POLÍTICA E PROCEDIMENTOS DE PROTEÇÃO DE DADOS PESSOAIS

Rua Beato Miguel de Carvalho 242
4710-356 Braga Portugal
t (+351) 253 617 607
www.casadeinvestimentos.com

Índice

I. POLÍTICA E PROCEDIMENTOS DE PROTEÇÃO DE DADOS PESSOAIS

1.1. Âmbito e Objetivos

O presente documento estabelece a Política e os Procedimentos de Proteção de Dados Pessoais da Casa de Investimentos - Gestão de Patrimónios e Fundos de Investimento, S.A. (doravante "Casa de Investimentos") (doravante "Política"), tendo em conta o disposto na alínea l) do n.º 2 do artigo 12.º da Lei n.º 83/2017[1], bem como no Regulamento (UE) 2016/679[2], em especial no seu artigo 24.º, nos termos dos quais a Casa de Investimentos tem o dever de desenvolver políticas e procedimentos em matéria de proteção de dados pessoais[3].

A presente Política é aplicável a todo o tratamento[4] de dados pessoais levado a cabo pela Casa de Investimentos, designadamente o que respeita aos seguintes titulares dos dados[5]:

a) Clientes;

b) Colaboradores;

c) Contrapartes contratuais;

d) Participantes em eventos organizados pela Casa de Investimentos;

e) Utilizadores do website da Casa de Investimentos e subscritores da newsletter.

[1] Lei n.º 83/2017, de 18 de agosto, que estabelece medidas de combate ao branqueamento de capitais e ao financiamento do terrorismo (doravante "Lei do Branqueamento").
[2] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.
[3] **Definição de Dados Pessoais**: informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»), sendo considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular (artigo 4.º, ponto 1) do Regulamento (UE) 2016/679).
[4] **Definição de Tratamento**: uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou a alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição. (artigo 4.º, ponto 2) do Regulamento (UE) 2016/679).
[5] **Definição de Titular dos Dados**: pessoa singular identificada ou identificável, sendo considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular (artigo 4.º, ponto 1) do Regulamento (UE) 2016/679).

1.2. Tratamento de Dados Pessoais pela Casa de Investimentos

A atividade da Casa de Investimentos consiste na prestação dos seguintes serviços, para os quais se encontra autorizada e registada junto da CMVM:

a) Gestão de organismos de investimento coletivo em valores mobiliários;

b) Gestão de organismos de investimento alternativo em valores mobiliários;

c) Gestão de carteiras por conta de outrem;

d) Consultoria para investimento;

No decurso da sua atividade, a Casa de Investimentos, por regra, trata dados pessoais ao abrigo das alíneas b) e c) do n.º 1 do artigo 6.º do Regulamento (UE) 2016/679, ou seja, quando o tratamento dos dados pessoais é necessário para:

a) A execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

b) O cumprimento de uma obrigação jurídica a que a Casa de Investimentos esteja sujeita.

Pese embora com menos expressão do que os anteriores, a Casa de Investimentos também leva a cabo o tratamento de dados pessoais ao abrigo da alínea a) do n.º 1 do artigo 6.º do Regulamento (UE) 2016/679, ou seja, com fundamento no consentimento do titular dos dados para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas.

O tratamento de dados pessoais com fundamento na execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados, é realizado pela Casa de Investimentos no âmbito dos seguintes contratos:

a) Contrato de Gestão de Carteiras;

b) Contrato de Consultoria para Investimento;

c) Contratos de Trabalho;

d) Outro tipo de contratos celebrados com colaboradores da Casa de Investimentos;

e) Contratos celebrados com fornecedores, designadamente na subcontratação de suporte informático, apoio jurídico, contabilidade e auditoria.

No âmbito do tratamento de dados pessoais com fundamento na execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados, além dos dados recolhidos nos contratos supramencionados, são ainda tratados pela Casa de Investimentos os dados pessoais constantes dos seguintes documentos:

a) Documentos de comunicação de ordens de subscrição e de resgate de fundos;

b) Formulário para envio de extratos por correio eletrónico;

c) Documentos de recolha de dados pessoais de outras pessoas que não os clientes, designadamente os colaboradores e os fornecedores da Casa de Investimentos, com base na execução de contratos.

O tratamento de dados pessoais com fundamento no cumprimento de uma obrigação jurídica a que a Casa de Investimentos esteja sujeita, é realizado pela Casa de Investimentos no âmbito dos seguintes documentos e dos procedimentos com eles relacionados:

a) Ficha de Informação de Cliente;

b) Ficha de Informação da Empresa;

c) Ficha de Informação de Sócio/Procurador;

d) Ficha de Abertura de Conta;

e) Ficha de Abertura de Conta Empresas;

f) Ficha de Cliente;

g) Perfil de Cliente;

h) Formulários FATCA e CRS;

i) Registo de Atividade de Consultoria;

j) Manutenção de registos internos;

k) Política de Investimentos. Instrumentos Financeiros e Operações;

l) Informações;

m) Eventuais documentos de recolha de dados pessoais de outras pessoas que não os clientes, designadamente os colaboradores e fornecedores da Casa de Investimentos, cuja recolha se baseie em obrigações legais.

O tratamento de dados pessoais com fundamento no consentimento do titular dos dados para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas é realizado pela Casa de Investimentos no seguinte âmbito:

a) Criação e manutenção de *mailing lists*;

b) Criação e manutenção de bases de dados telefónicos;

c) Envio de artigos de opinião;

d) Envio de *newsletters* e de outros documentos informativos;

e) Envio de convites para as iniciativas promovidas pela Casa de Investimentos;

f) Envio de informação publicitária;

O facto de o tratamento de dados pessoais pela Casa de Investimentos ser normalmente realizado com os fundamentos acima referidos não prejudica a possibilidade de tratamento de dados pessoais, pela Casa de Investimentos, com outros fundamentos, nos termos do disposto na presente Política e na legislação e regulamentação aplicáveis.

1.3. Princípios Aplicados ao Tratamento de Dados Pessoais

A Casa de Investimentos assegura que os dados pessoais por si recolhidos são (artigo 5.º do Regulamento (UE) 2016/679):

a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados ("licitude, lealdade e transparência);

b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades ("limitação das finalidades");

c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados ("minimização dos dados");

d) Exatos e atualizados sempre que necessário, sendo adotadas pela Casa de Investimentos as medidas adequadas a assegurar que os dados inexatos, tendo em conta as finalidades para que são tratados, são apagados ou retificados sem demora ("exatidão");

e) Conservados de uma forma que permite a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados, ("limitação da conservação");

f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, sendo adotadas pela Casa de Investimentos as medidas técnicas ou organizativas adequadas ("integridade e confidencialidade");

g) Protegidos desde a conceção, sendo adotadas pela Casa de Investimentos, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento de dados, as medidas técnicas e organizativas adequadas para garantir a aplicação dos princípios de proteção de dados, identificados nas alíneas anteriores, como a pseudonimização, bem como para incluir as garantias necessárias no tratamento, de forma a proteger os direitos dos titulares dos dados, tendo em conta as técnicas mais avançadas, os custos da sua aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento de dados, bem como os riscos decorrentes do tratamento para os direitos e as liberdades

das pessoas singulares (“proteção de dados desde a conceção”) (artigo 25.º, n.º 1 do Regulamento (UE) 2016/679);

h) Protegidos por defeito, sendo aplicadas pela Casa de Investimentos as medidas técnicas e organizativas necessárias para assegurar que só são tratados os dados pessoais que sejam necessários para cada finalidade específica de tratamento, no que respeita à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade, sendo assegurado pela Casa de Investimentos que os dados recolhidos não são disponibilizados, sem intervenção humana, a um número indeterminado de pessoas singulares (“proteção de dados por defeito”) (artigo 25.º, n.º 1 do Regulamento (UE) 2016/679).

A Casa de Investimentos impõe as necessárias restrições, contratuais ou outras, para assegurar que as pessoas que, agindo sob a autoridade da Casa de Investimentos ou sendo seus subcontratados, tenham acesso a dados pessoais, não procedem ao tratamento desses dados sem instruções da Casa de Investimentos nesse sentido, salvo se forem obrigados a fazê-lo por força da legislação e da regulamentação aplicáveis (artigo 29.º do Regulamento (UE) 2016/679).

Caso os colaboradores da Casa de Investimentos ou os seus subcontratados incumpram o disposto no parágrafo anterior, a Casa de Investimentos adotará as medidas disciplinares, contratuais, penais e cíveis que sejam aplicáveis ao caso concreto (artigos 29.º e 32.º, n.º 4 do Regulamento (UE) 2016/679).

1.4. Segurança do Tratamento de Dados Pessoais

A Casa de Investimentos aplica medidas técnicas e organizativas, que considera adequadas, para assegurar a segurança do tratamento de dados pessoais, num nível adequado ao seu risco, tendo em conta as técnicas mais avançadas, os custos da sua aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento de dados, bem como os riscos, de probabilidade e de gravidade variáveis, para os direitos e as liberdades das pessoas singulares, incluindo, consoante o que se mostre adequado em face do caso concreto, as seguintes medidas (artigo 32.º, n.º 1 do Regulamento (UE) 2016/679):

a) A pseudonimização e a cifragem dos dados pessoais;

b) A capacidade de assegurar a confidencialidade, a integridade, a disponibilidade e a resiliência permanentes dos sistemas e dos serviços de tratamento;

c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada em caso de incidente físico ou técnico;

d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Ao avaliar o nível de segurança adequado, a Casa de Investimentos tem em conta, designadamente, os riscos apresentados pelo tratamento, em particular em caso de destruição, perda e alteração acidentais ou ilícitas, bem como em caso de divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, pela Casa de Investimentos (artigo 32.º, n.º 2 do Regulamento (UE) 2016/679).

No âmbito do exercício dos direitos dos titulares dos dados previstos na presente Política, bem como na legislação e na regulamentação aplicáveis, o Responsável pelo Compliance confirma a identidade do titular dos dados antes de dar seguimento aos seus pedidos, através de solicitação de apresentação de um documento de identificação (página 16 das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre o direito à portabilidade dos dados - WP 242 rev. 01).

1.5. Fundamento Jurídico para o Tratamento de Dados Pessoais e Finalidade do Tratamento

A Casa de Investimentos apenas trata dados pessoais se e na medida em que se verifique pelo menos uma das seguintes situações (artigo 6.º, n.º 1 do Regulamento (UE) 2016/679):

a) O titular dos dados, ter dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;

b) O tratamento ser necessário para a execução de um contrato do qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

c) O tratamento ser necessário para o cumprimento de uma obrigação jurídica a que a Casa de Investimentos esteja sujeita;

d) O tratamento ser necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

e) O tratamento ser necessário para efeito dos interesses legítimos prosseguidos pela Casa de Investimentos ou por terceiros, exceto se prevalecerem os interesses ou os direitos e as liberdades fundamentais do titular dos dados que exijam a proteção dos dados pessoais, em especial se o titular dos dados for uma criança.

A finalidade do tratamento dos dados pessoais é determinada com o respetivo fundamento jurídico (artigo 6.º, n.º 3 do Regulamento (UE) 2016/679).

Na eventualidade de a Casa de Investimentos vir a tratar os dados pessoais para outros fins que não aqueles para os quais os dados pessoais foram recolhidos e caso o tratamento não seja realizado com base no consentimento do titular dos dados pessoais, nem em disposição legal ou regulamentar aplicável que constitua uma medida necessária e proporcionada para salvaguardar os objetivos referidos no n.º 1 do artigo 23.º do Regulamento (UE) 2016/679[6], a Casa de Investimentos, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem, nomeadamente, em conta (artigo 6.º, n.º 4 do Regulamento (UE) 2016/679):

a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;

b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e a Casa de Investimentos;

[6] O n.º 1 do artigo 23.º do Regulamento (UE) 2016/679 dispõe o seguinte:
"*1. O direito da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento ou o seu subcontratante pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 12.º a 22.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar, designadamente:*
a) A segurança do Estado;
b) A defesa;
c) A segurança pública;
d) A prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública;
e) Outros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social;
f) A defesa da independência judiciária e dos processos judiciais;
g) A prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas;
h) Uma missão de controlo, de inspeção ou de regulamentação associada, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas a) a e) e g);
i) A defesa do titular dos dados ou dos direitos e liberdades de outrem;
j) A execução de ações cíveis".

c) A natureza dos dados pessoais, em especial se estiver em causa o tratamento de dados pessoais relacionados com condenações penais e infrações nos termos do artigo 10.º do Regulamento (UE) 2016/679[7];

d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;

e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

1.5.1. Tratamento Baseado no Consentimento do Titular dos Dados Pessoais

Sempre que o tratamento seja realizado com base no consentimento do titular dos dados pessoais, a Casa de Investimentos conserva os documentos necessários para poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais (artigo 7.º, n.º 1 do Regulamento (UE) 2016/679).

Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento é apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples, não sendo vinculativa qualquer parte dessa declaração que constitua violação do disposto no Regulamento (UE) 2016/679 (artigo 7.º, n.º 2 do Regulamento (UE) 2016/679).

O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento, pese embora a retirada do consentimento não comprometa a licitude do tratamento efetuado com base no consentimento previamente dado, facto do qual o titular dos dados é informado antes de dar o seu consentimento (artigo 7.º, n.º 3 do Regulamento (UE) 2016/679).

A Casa de Investimentos aplica os procedimentos adequados para assegurar que o consentimento seja tão fácil de retirar quanto de dar (artigo 7.º, n.º 3 do Regulamento (UE) 2016/679).

O consentimento não é considerado livre caso a execução de um contrato, *inclusive* a prestação de um serviço, se encontre subordinada ao consentimento para o tratamento de dados pessoais que não seja necessário para a execução desse contrato (artigo 7.º, n.º 4 e considerando (43) do Regulamento (UE) 2016/679).

[7] O artigo 10.º do Regulamento (UE) 2016/679 dispõe o seguinte:
"*O tratamento de dados pessoais relacionados com condenações penais e infrações ou com medidas de segurança conexas com base no artigo 6.º, n.º 1, só é efetuado sob o controlo de uma autoridade pública ou se o tratamento for autorizado por disposições do direito da União ou de um Estado-Membro que prevejam garantias adequadas para os direitos e liberdades dos titulares dos dados. Os registos completos das condenações penais só são conservados sob o controlo das autoridades públicas*."

Na avaliação da validade do consentimento do titular dos dados pessoais a Casa de Investimentos tem em conta o disposto nas Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre o consentimento ao abrigo do Regulamento (UE) 2016/679 – WP 259 rev.01 (conferir o Anexo I).

1.6. Tratamento de Categorias Especiais de Dados Pessoais

A Casa de Investimentos não trata dados pessoais que revelem a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, ou filiação sindical, nem dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa (artigo 9.º do Regulamento (UE) 2016/679).

A Casa de Investimentos não trata dados pessoais relacionados com condenações penais e infrações, a não ser que o seu tratamento seja exigido e, nessa medida, autorizado, pela legislação ou regulamentação aplicáveis (artigo 10.º do Regulamento (UE) 2016/679).

1.7. Tratamento que Não Exige Identificação do Titular dos Dados Pessoais

Caso as finalidades para as quais a Casa de Investimentos procede ao tratamento de dados pessoais, no caso concreto, não exigirem, ou tiverem deixado de exigir, a identificação do titular dos dados, a Casa de Investimentos não é obrigada a manter, a obter ou a tratar informações suplementares para identificar o titular dos dados com o único objetivo de dar cumprimento ao Regulamento (UE) 2016/679 (artigo 11.º, n.º 1 do Regulamento (UE) 2016/679).

Quando a Casa de Investimentos possa demonstrar que não está em condições de identificar o titular dos dados, informa-o, se possível, desse facto (artigo 11.º, n.º 2 do Regulamento (UE) 2016/679).

Nesses casos, não é aplicável o disposto nos pontos 1.10. a 1.14. da Política, exceto se o titular dos dados, com a finalidade de exercer os seus direitos ao abrigo dos referidos artigos, fornecer informações adicionais que permitam a sua identificação (artigo 11.º, n.º 2 do Regulamento (UE) 2016/679).

1.8. Transparência das Informações, das Comunicações e das Regras para o Exercício dos Direitos dos Titulares dos Dados Pessoais

A Casa de Investimentos fornece aos titulares dos dados pessoais as informações devidas no âmbito da recolha de dados pessoais e do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, sendo as informações prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos. As informações referidas podem ainda ser prestadas oralmente, a pedido do titular dos dados pessoais, desde que a sua identidade seja comprovada por outros meios (artigo 12.º, n.º 1 do Regulamento (UE) 2016/679).

A Casa de Investimentos facilita o exercício dos direitos de acesso, de retificação, ao apagamento, à limitação do tratamento, de portabilidade, de oposição e de não ficar sujeito a decisões individuais automatizadas, bem como o direito a pedir informação sobre os eventuais destinatários a quem os dados tenham sido transmitidos, pelo titular dos dados, sempre que a eles haja lugar, não se recusando a dar seguimento aos pedidos de exercício dos direitos mencionados, a não ser que possa demonstrar não estar em condições de identificar o titular dos dados (artigo 12.º, n.º 2 do Regulamento (UE) 2016/679).

A Casa de Investimentos fornece ao titular dos dados pessoais, mediante pedido, as informações sobre as medidas tomadas nos termos do disposto *infra* quanto aos direitos de acesso, de retificação, ao apagamento, à limitação do tratamento e de portabilidade, bem como no âmbito da notificação da retificação, do apagamento dos dados pessoais ou da limitação do tratamento, sem demora injustificada e no prazo de um mês a contar da data de receção do pedido, podendo este prazo ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. Nesse caso, a Casa de Investimentos informa o titular dos dados pessoais sobre a prorrogação e os motivos da demora, no prazo de um mês a contar da data da receção do pedido. Se o titular dos dados pessoais apresentar o pedido por meios eletrónicos, a informação é, sempre que possível, fornecida por meios eletrónicos, salvo pedido em contrário do titular dos dados pessoais (artigo 12.º, n.º 3 do Regulamento (UE) 2016/679).

Caso a Casa de Investimentos não dê seguimento ao pedido apresentado pelo titular dos dados pessoais, informa-o sem demora e, o mais tardar, no prazo de um mês a contar da data de receção do pedido, das razões que a levaram a não tomar medidas, bem como da possibilidade de apresentar reclamação à Comissão Nacional de Proteção de Dados e de intentar ação judicial (artigo 12.º, n.º 4 do Regulamento (UE) 2016/679).

As informações fornecidas no âmbito da recolha de dados pessoais, tratadas no ponto 1.9. abaixo, bem como quaisquer comunicações e medidas tomadas no âmbito dos direitos de acesso, de retificação, ao apagamento, à limitação do tratamento, de portabilidade, de oposição, de não ficar sujeito a decisões individuais automatizadas, bem como no âmbito da notificação da retificação, do

apagamento dos dados pessoais ou da limitação do tratamento e da comunicação de violações de dados pessoais ao titular dos dados pessoais, são fornecidas/ levadas a cabo a título gratuito, a não ser que os pedidos apresentados pelo titular dos dados pessoais sejam manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo, podendo nesse caso a Casa de Investimentos , pese embora lhe caiba demonstrar o caráter manifestamente infundado ou excessivo do pedido (artigo 12.º, n.º 5 do Regulamento (UE) 2016/679):

a) Exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas; ou

b) Recusar-se a dar seguimento ao pedido.

Sem prejuízo do disposto no ponto 1.7. da Política, quando a Casa de Investimentos tiver dúvidas razoáveis quanto à identidade da pessoa singular que apresenta o pedido relativo aos direitos de acesso, de retificação, ao apagamento, à limitação do tratamento, de portabilidade, de oposição, bem como o pedido de fornecimento de informação sobre os eventuais destinatários a quem os dados tenham sido transmitidos, pode solicitar que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade do titular dos dados pessoais (artigo 12.º, n.º 6 do Regulamento (UE) 2016/679).

As informações a fornecer aos titulares dos dados pessoais no âmbito da recolha dos dados pessoais podem ser dadas pela Casa de Investimentos em combinação com ícones normalizados, a fim de dar, de uma forma facilmente visível, inteligível e claramente legível, uma perspetiva geral significativa do tratamento previsto. Se forem apresentados por via eletrónica, os ícones devem ser de leitura automática (artigo 12.º, n.º 7 do Regulamento (UE) 2016/679).

No âmbito das informações e das comunicações feitas de acordo com a presente Política, a Casa de Investimentos tem em conta o disposto nas Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre transparência ao abrigo do Regulamento (UE) 2016/679 – WP 260 rev.01 (conferir o Anexo II).

1.9. Informação a Fornecer no Âmbito da Recolha de Dados Pessoais

Quando os dados pessoais são recolhidos junto do titular dos dados, o que acontece por regra, tendo em conta o tratamento de dados pessoais levado a cabo pela Casa de Investimentos, melhor descrito

no ponto 1.2. da Política, a Casa de Investimentos faculta-lhe, aquando da recolha desses dados pessoais, as seguintes informações (artigo 13.º, n.º 1 do Regulamento (UE) 2016/679):

a) A identidade e os contactos da Casa de Investimentos, enquanto responsável pelo tratamento e, se for caso disso, do seu representante;

b) Os contactos do encarregado da proteção de dados da Casa de Investimentos;

c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;

d) Se o tratamento dos dados se basear nos interesses legítimos prosseguidos pela Casa de Investimentos, enquanto responsável pelo tratamento, ou por terceiros, o interesse legítimo em causa;

e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;

f) Se for caso disso, o facto de a Casa de Investimentos tencionar transferir dados pessoais para um país terceiro ou para uma organização internacional, bem como a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.º, 47.º e 49, n.º 1, segundo parágrafo do Regulamento (UE) 2016/679 (conferir o ponto 1.25. da Política), a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.

Para além das informações supramencionadas, aquando da recolha dos dados pessoais, a Casa de Investimentos fornece ao titular dos dados pessoais as seguintes informações adicionais, na medida do aplicável (artigos 13.º, n.º 2 e 22.º, n.ºs 1 e 4 do Regulamento (UE) 2016/679):

a) O prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;

b) A existência do direito de solicitar à Casa de Investimentos o acesso aos dados pessoais que lhe digam respeito, a sua retificação ou o seu apagamento, bem como a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;

c) Se o tratamento dos dados se basear no consentimento do titular dos dados, a existência do direito de retirar o consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;

d) O direito de apresentar reclamação à Comissão Nacional de Proteção de Dados;

e) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular dos dados está obrigado a fornecer os dados pessoais e as eventuais consequências do não fornecimento;

f) A existência de decisões exclusivamente automatizadas, incluindo a definição de perfis, caso a Casa de Investimentos as venha a admitir e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Nos casos em que a Casa de Investimentos tenha a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, antes desse tratamento, fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes, nos termos do disposto nas alíneas anteriores, relativas às informações adicionais fornecidas aquando da recolha dos dados pessoais (artigo 13.º, n.º 3 do Regulamento (UE) 2016/679).

Os procedimentos supramencionados, no presente ponto da Política, não são aplicados quando e na medida em que o titular dos dados já tenha conhecimento das informações em questão (artigo 13.º, n.º 4 do Regulamento (UE) 2016/679).

Quando os dados pessoais não são recolhidos junto do seu titular, o que por regra não acontece, atendendo ao tratamento de dados pessoais levado a cabo pela Casa de Investimentos, melhor descrito no ponto 1.2. da Política, a Casa de Investimentos fornece as seguintes informações ao titular dos dados pessoais (artigo 14.º, n.º 1 do Regulamento (UE) 2016/679):

a) A identidade e os contactos da Casa de Investimentos, enquanto responsável pelo tratamento e, se for caso disso, do seu representante;

b) Os contactos do encarregado da proteção de dados da Casa de Investimentos;

c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;

d) As categorias dos dados pessoais em questão;

e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;

f) Se for caso disso, o facto de a Casa de Investimentos tencionar transferir dados pessoais para um país terceiro ou para uma organização internacional, bem como a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.º, 47.º e 49, n.º 1, segundo parágrafo do Regulamento (UE) 2016/679 (conferir o ponto 1.25. *infra)*, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.

Para além das informações supramencionadas, quando os dados não são recolhidos junto do seu titular, a Casa de Investimentos fornece ao titular dos dados pessoais as seguintes informações adicionais, na medida do aplicável (artigos 14.º, n.º 2 e 22.º, n.ºs 1 e 4 do Regulamento (UE) 2016/679):

a) O prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo;

b) Se o tratamento dos dados se basear nos interesses legítimos prosseguidos pela Casa de Investimentos, enquanto responsável pelo tratamento, ou por terceiros, o interesse legítimo em causa;

c) A existência do direito de solicitar à Casa de Investimentos o acesso aos dados pessoais que lhe digam respeito, a sua retificação ou o seu apagamento, bem como a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;

d) Se o tratamento dos dados se basear no consentimento do titular dos dados, a existência do direito de retirar o consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;

e) O direito de apresentar reclamação à Comissão Nacional de Proteção de Dados;

f) A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público;

g) A existência de decisões exclusivamente automatizadas, incluindo a definição de perfis, caso a Casa de Investimentos as venha a admitir e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

As informações comunicadas quando os dados pessoais não são recolhidos junto do seu titular, nos termos supramencionados, são comunicadas pela Casa de Investimentos ao titular dos dados (artigo 14.º, n.º 3 do Regulamento (UE) 2016/679):

a) Num prazo razoável após a obtenção dos dados pessoais, o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que os dados sejam tratados;

b) Se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados; ou

c) Se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados.

Nos casos em que a Casa de Investimentos tenha a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, antes desse tratamento, fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes, nos termos do disposto nas alíneas *supra*, relativas às informações adicionais fornecidas quando os dados não são recolhidos junto do seu titular (artigo 14.º, n.º 4 do Regulamento (UE) 2016/679).

Os procedimentos supramencionados, relativos às informações fornecidas quando os dados pessoais não são recolhidos junto do seu titular, não são aplicados quando e na medida em que (artigo 14.º, n.º 5 do Regulamento (UE) 2016/679):

a) O titular dos dados já tenha conhecimento das informações em questão;

b) Se comprove a impossibilidade de disponibilizar a informação, ou caso o esforço envolvido seja desproporcionado, na medida em que a obrigação de disponibilizar as informações (principais) supramencionadas ao titular dos dados seja suscetível de tornar impossível ou de prejudicar gravemente a obtenção dos objetivos desse tratamento. Nesses casos, a Casa

de Investimentos toma as medidas adequadas para defender os direitos, liberdades e interesses legítimos do titular dos dados, *inclusive* através da divulgação da informação ao público;

c) A obtenção ou a divulgação dos dados esteja expressamente prevista na legislação e na regulamentação aplicáveis, sendo previstas medidas adequadas para proteger os legítimos interesses do titular dos dados; ou

d) Os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional ou de confidencialidade, regulamentada pela legislação e regulamentação aplicáveis.

Ao prestar informação aos titulares dos dados sobre os seus direitos, nos termos supramencionados, a Casa de Investimentos explica claramente a diferença entre os tipos de dados que um titular de dados pode receber no âmbito dos direitos de acesso e de portabilidade dos dados (página 15 das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre o direito à portabilidade dos dados - WP 242 rev. 01).

1.10. Direito de Acesso

A pedido do titular dos dados pessoais, a Casa de Investimentos confirma se os dados pessoais que lhe dizem respeito são ou não objeto de tratamento e, em caso afirmativo, assegura ao titular dos dados o direito de aceder aos seus dados pessoais e às informações seguintes (artigo 15.º, n.º 1 do Regulamento (UE) 2016/679):

a) As finalidades do tratamento dos dados;

b) As categorias dos dados pessoais em questão;

c) Os destinatários ou as categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;

d) Quando possível, o prazo previsto para a conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo;

e) A existência do direito de solicitar à Casa de Investimentos a retificação, o apagamento ou a limitação do tratamento dos seus dados pessoais, ou do direito de se opor a esse tratamento;

f) O direito de apresentar reclamação à Comissão Nacional de Proteção de Dados;

g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;

h) A existência de decisões automatizadas, incluindo a definição de perfis, caso a Casa de Investimentos as venha a admitir e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Caso a Casa de Investimentos venha a transferir os dados pessoais para um país terceiro ou para uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas relativas à transferência de dados, nos termos do disposto no artigo 46.º do Regulamento (UE) 2016/679 (conferir o ponto 1.25. da Política) (artigo 15.º, n.º 2 do Regulamento (UE) 2016/679).

A Casa de Investimentos fornece, gratuitamente, uma cópia dos dados pessoais em fase de tratamento, mediante pedido do titular dos dados, podendo exigir o pagamento de um montante razoável para a disponibilização de cópias adicionais, tendo em conta os custos administrativos (artigo 15.º, n.º 3 do Regulamento (UE) 2016/679).

Sempre que o titular dos dados apresenta o pedido de acesso aos seus dados pessoais por meios eletrónicos, a Casa de Investimentos fornece a informação correspondente num formato eletrónico de uso corrente, salvo indicação em contrário do titular dos dados (artigo 15.º, n.º 3 do Regulamento (UE) 2016/679).

O direito de o titular dos dados obter uma cópia dos dados pessoais em fase de tratamento, nos termos supramencionados, não prejudica os direitos e as liberdades de terceiros (artigo 15.º, n.º 4 do Regulamento (UE) 2016/679).

1.11. Direito de Retificação

A Casa de Investimentos retifica os dados pessoais que se encontrem inexatos, sem demora injustificada, mediante pedido do titular dos dados em questão (artigo 16.º do Regulamento (UE) 2016/679).

Tendo em conta as finalidades do tratamento, a Casa de Investimentos assegura a possibilidade de o titular dos dados exercer o seu direito a completar os seus dados pessoais que se encontrem incompletos, designadamente por meio de uma declaração adicional (artigo 16.º do Regulamento (UE) 2016/679).

A Casa de Investimentos comunica a cada destinatário a quem os dados pessoais tenham eventualmente sido transmitidos qualquer retificação dos dados pessoais a que tenha procedido, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado. A Casa de Investimentos fornece ao titular dos dados informações sobre os destinatários suprarreferidos, mediante pedido (artigo 19.º do Regulamento (UE) 2016/679).

1.12. Direito ao Apagamento

A Casa de Investimentos apaga os dados pessoais, sem demora injustificada, independentemente da existência ou não de pedido do titular dos dados nesse sentido, sempre que (artigo 17.º, n.º 1 do Regulamento (UE) 2016/679):

a) Os dados pessoais deixem de ser necessários para a finalidade que motivou a sua recolha ou o seu tratamento;

b) O titular retire o consentimento no qual se baseia o tratamento dos dados, caso não exista outro fundamento jurídico para o referido tratamento;

c) O titular dos dados se oponha ao seu tratamento, nos termos previstos no ponto 1.15. da Política, não existindo interesses legítimos prevalecentes que justifiquem o tratamento;

d) Os dados pessoais tenham sido tratados ilicitamente;

e) Os dados pessoais tenham de ser apagados para o cumprimento de uma obrigação legal ou regulamentar a que a Casa de Investimentos esteja sujeita.

Caso a Casa de Investimentos tenha tornado públicos os dados pessoais e seja obrigada a apagá-los nos termos supramencionados, a Casa de Investimentos toma as medidas que se mostrem razoáveis, incluindo medidas de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhe solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos (artigo 17.º, n.º 2 do Regulamento (UE) 2016/679).

Os procedimentos supramencionados não são aplicados pela Casa de Investimentos na medida em que o tratamento dos dados em questão se revele necessário (artigo 17.º, n.º 3 do Regulamento (UE) 2016/679):

a) Ao exercício da liberdade de expressão e de informação;

b) Ao cumprimento de uma obrigação legal da Casa de Investimentos que exija o tratamento, prevista na legislação ou na regulamentação aplicáveis; ou

c) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

A Casa de Investimentos comunica a cada destinatário a quem os dados pessoais tenham eventualmente sido transmitidos qualquer apagamento dos dados pessoais a que tenha procedido, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado, fornecendo ao titular dos dados informações sobre os referidos destinatários, mediante pedido (artigo 19.º do Regulamento (UE) 2016/679).

1.13. Direito à Limitação do Tratamento

A Casa de Investimentos procede à limitação do tratamento dos dados pessoais, mediante pedido do titular dos dados, sempre que se verifique uma das seguintes situações (artigo 18.º, n.º 1 do Regulamento (UE) 2016/679):

a) O titular dos dados tenha contestado a exatidão dos dados pessoais, durante um período que permita à Casa de Investimentos verificar a sua exatidão;

b) O tratamento dos dados seja ilícito e o titular dos dados se tenha oposto ao apagamento dos dados pessoais, solicitando, em contrapartida, a limitação da sua utilização;

c) A Casa de Investimentos já não precise dos dados pessoais para fins de tratamento, mas esses dados tenham sido requeridos pelo titular dos dados para efeitos de declaração, exercício ou defesa de um direito num processo judicial;

d) O titular dos dados se tenha oposto ao tratamento, nos termos do disposto no ponto 1.15. da Política, sendo a limitação do tratamento dos dados pessoais colocada em prática até que seja verificada a prevalência dos motivos legítimos da Casa de Investimentos sobre os do titular dos dados.

Sempre que o tratamento seja limitado, nos termos supramencionados, os dados pessoais em questão só são tratados pela Casa de Investimentos, exceto no que diz respeito à sua conservação, com o consentimento do titular dos dados, bem como para efeitos de declaração, de exercício ou de defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos ponderosos de interesse público (artigo 18.º, n.º 2 do Regulamento (UE) 2016/679).

Sempre que a Casa de Investimentos tenha procedido à limitação do tratamento dos dados, nos termos supramencionados, informa o titular dos dados da anulação da limitação ao referido tratamento, antes de a mesma ter lugar (artigo 18.º, n.º 3 do Regulamento (UE) 2016/679).

A Casa de Investimentos comunica a cada destinatário a quem os dados pessoais tenham eventualmente sido transmitidos qualquer limitação do tratamento dos dados pessoais a que tenha procedido, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado, fornecendo ao titular dos dados informações sobre os referidos destinatários, mediante pedido (artigo 19.º do Regulamento (UE) 2016/679).

1.14. Direito de Portabilidade dos Dados

A Casa de Investimentos disponibiliza os dados pessoais ao seu titular, mediante pedido e caso os dados pessoais lhe tenham sido fornecidos pelo seu titular[8], num formato estruturado, de uso

[8] Segundo as Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre o direito à portabilidade dos dados - WP 242 rev. 01, consideram-se dados fornecidos pelo seu titular não apenas os dados pessoais fornecidos por aquele de forma ativa e consciente, mas também aqueles que sejam observados a partir das atividades dos utilizadores, tais como os dados brutos tratados por um contador inteligente ou por outros tipos de objetos conectados, os registos das atividades e os históricos da utilização de um sítio na Internet ou das pesquisas realizadas, não incluindo os dados inferidos ou derivados, designadamente os que sejam criados pelo responsável pelo tratamento com base nos dados observados ou diretamente inseridos pelo titular dos dados, por exemplo um perfil de utilizador criado através de uma análise dos dados brutos de contagem inteligente recolhidos.

corrente e de leitura automática[9], não criando obstáculos a que o titular dos dados os transmita a outro responsável pelo tratamento, sempre que (artigo 20.º, n.º 1 do Regulamento (UE) 2016/679):

a) O tratamento seja baseado no consentimento do titular dos dados, ou num contrato cuja execução ou realização de diligências pré-contratuais, tenha fundamentado o fornecimento dos dados pessoais; e

b) O tratamento seja realizado por meios automatizados.

Os formatos utilizado pela Casa de Investimentos neste contexto são, nos termos das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre o direito à portabilidade dos dados - WP 242 rev. 01, quando não existem formatos de utilização comum em determinado setor ou contexto, formatos abertos comummente utilizados (p. ex., XML, JSON, CSV, etc.) juntamente com metadados úteis no melhor nível possível de granularidade, sem, com isso, deixar de preservar um elevado nível de abstração.

Quando o direito de portabilidade dos dados seja exercido pelo titular dos dados, nos termos supramencionados, a Casa de Investimentos transmite diretamente os dados ao novo responsável pelo tratamento, mediante pedido do titular dos dados, sempre que tal seja tecnicamente possível (artigo 20.º, n.º 2 do Regulamento (UE) 2016/679).

Neste contexto, entende-se que a transmissão é tecnicamente possível sempre que a comunicação entre o sistema da Casa de Investimentos e o sistema do novo responsável pelo tratamento seja possível, de forma segura, através de uma comunicação autenticada com o nível necessário de cifragem dos dados, sendo necessário que o sistema recetor tenha condições técnicas para receber os dados de entrada. Em caso de entraves técnicos que impeçam a transmissão direta dos dados, a Casa de Investimentos explica esses entraves ao titular dos dados, nos termos aplicáveis às situações de recusa de dar seguimento a um pedido do titular dos dados (página 18 das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre o direito à portabilidade dos dados - WP 242 rev. 01).

[9] Nos termos das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre o direito à portabilidade dos dados - WP 242 rev. 01, a utilização de um formato estruturado, de uso corrente e de leitura automática corresponde ao cumprimento dos requisitos mínimos para possibilitar a interoperabilidade que se pretende existir no âmbito da portabilidade dos dados, a qual é definida como a capacidade de organizações díspares e diversas interagirem com vista à consecução de objetivos comuns com benefícios mútuos, definidos de comum acordo e implicando a partilha de informações e de conhecimentos entre as organizações, no âmbito dos processos administrativos a que dão apoio, mediante o intercâmbio de dados entre os respetivos sistemas TIC, nos termos do artigo 2.º da Decisão n.º 922/2009/CE do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, sobre soluções de interoperabilidade para as administrações públicas europeias.

À recusa da portabilidade dos dados é aplicável o disposto no ponto 1.8. da Política, não podendo a Casa de Investimentos deixar os titulares dos dados sem resposta no âmbito de um pedido de portabilidade dos seus dados (artigo 12.º, n.º 4 do Regulamento (UE) 2016/679 e página 17 das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre o direito à portabilidade dos dados - WP 242 rev. 01).

No plano técnico, a Casa de Investimentos dispõe de mecanismos diferentes e complementares para disponibilizar os dados abrangidos pelo direito de portabilidade aos titulares dos dados, os quais permitem, por um lado, uma transmissão direta do conjunto global desses dados ou de várias partes extraídas do conjunto global desses dados e, por outro lado, a extração dos dados relevantes, dando prevalência à utilização do segundo mecanismo, sempre que possível (página 18 das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre o direito à portabilidade dos dados - WP 242 rev. 01).

O exercício do direito de portabilidade dos dados aplica-se sem prejuízo do direito ao seu apagamento, pese embora não o implique necessariamente (artigo 20.º, n.º 3 do Regulamento (UE) 2016/679 e página 8 das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre o direito à portabilidade dos dados - WP 242 rev. 01).

O direito de o titular dos dados solicitar a sua portabilidade não prejudica os direitos e as liberdades de terceiros (artigo 20.º, n.º 4 do Regulamento (UE) 2016/679).

Sempre que se verifique a existência do direito de portabilidade dos dados, a Casa de Investimentos fornece aos titulares dos dados informação sobre o direito de portabilidade dos dados antes de os titulares dos dados cessarem qualquer contrato com a Casa de Investimentos, de forma a permitir que os titulares dos dados possam obter um balanço dos seus dados pessoais e transmiti-los facilmente para os seus próprios dispositivos ou para outro responsável pelo tratamento antes da cessação do contrato (página 15 das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre o direito à portabilidade dos dados - WP 242 rev. 01).

A portabilidade dos dados pessoais implica um patamar suplementar de tratamento dos dados por parte da Casa de Investimentos, de forma a extrair os dados da sua base de dados e a filtrar os dados pessoais que não se encontram no âmbito da portabilidade, sendo considerada auxiliar relativamente ao tratamento de dados principal (página 20 das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre o direito à portabilidade dos dados - WP 242 rev. 01).

1.15. Direito de Oposição

A Casa de Investimentos cessa o tratamento dos dados pessoais caso o titular dos dados se oponha ao seu tratamento, o que pode fazer por motivos relacionados com a sua situação particular, quando o tratamento seja feito com base em interesses legítimos prosseguidos pela Casa de Investimentos ou por terceiros, bem como quando o tratamento seja feito para fins que não sejam aqueles para os quais os dados foram recolhidos, incluindo a definição de perfis, nos termos do disposto no ponto 1.5. da Política (artigo 21.º, n.º 1 do Regulamento (UE) 2016/679).

Nos casos identificados no parágrafo anterior, mesmo existindo oposição do titular dos dados, a Casa de Investimentos pode não cessar o tratamento dos dados pessoais caso tenha razões imperiosas e legítimas para esse tratamento, que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, bem como caso o tratamento dos dados seja necessário para efeitos de declaração, de exercício ou de defesa de um direito num processo judicial (artigo 21.º, n.º 1 do Regulamento (UE) 2016/679).

A Casa de Investimentos não trata dados pessoais para efeitos de comercialização direta.

O titular dos dados tem o direito de se opor, a qualquer momento, ao tratamento dos dados pessoais que lhe digam respeito para efeitos de comercialização direta, o que abrange a definição de perfis na medida em que esteja relacionada com a referida comercialização (artigo 21.º, n.º 2 do Regulamento (UE) 2016/679).

Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais não podem ser tratados para esse fim (artigo 21.º, n.º 3 do Regulamento (UE) 2016/679).

A Casa de Investimentos não trata dados pessoais para fins de investigação científica ou histórica nem para fins estatísticos (artigo 21.º, n.º 6 do Regulamento (UE) 2016/679).

1.16. Decisões Individuais Automatizadas

A Casa de Investimentos não sujeita os titulares dos dados pessoais a quaisquer decisões tomadas exclusivamente com base em tratamento automatizado, incluindo a definição de perfis, que produza efeitos nas suas esferas jurídicas ou que os afetem significativamente de forma similar (artigo 22.º do Regulamento (UE) 2016/679).

1.17. Subcontratação

A Casa de Investimentos não recorre atualmente a quaisquer entidades subcontratadas para prestação de serviços relacionados com o tratamento de dados pessoais.

Caso a Casa de Investimentos venha, no futuro, a subcontratar outras entidades para a prestação de serviços relacionados com o tratamento de dados pessoais, a Casa de Investimentos encontra-se ciente da necessidade de recorrer apenas a entidades que apresentem garantias suficientes relativamente à aplicação de medidas técnicas e organizativas adequadas a garantir que o tratamento satisfaz os requisitos legais e regulamentares aplicáveis e assegura a defesa dos direitos dos titulares dos dados (artigo 28.º, n.º 1 do Regulamento (UE) 2016/679).

A Casa de Investimentos encontra-se ainda ciente de que, caso venha a recorrer à subcontratação dos serviços supramencionados, a subcontratação tem de ser regida por contrato escrito que vincule a entidade subcontratada à Casa de Investimentos, que estabeleça o objeto e a duração do tratamento, a sua natureza e a sua finalidade, o tipo de dados pessoais e as categorias dos titulares dos dados, bem como as obrigações e os direitos da Casa de Investimentos, enquanto responsável pelo tratamento[10], não podendo a entidade subcontratada voltar a subcontratar sem autorização

[10] O contrato celebrado entre a Casa de Investimentos e eventuais entidades subcontratantes, ou outro ato normativo que venha a ser previsto para o mesmo efeito nos termos da legislação e regulamentação aplicáveis, estipula, designadamente, que a entidade subcontratada:

a) Trata os dados pessoais apenas mediante instruções documentadas da Casa de Investimentos, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pela legislação e regulamentação aplicáveis, informando nesse caso a Casa de Investimentos desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;

b) Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;

c) Adota todas as medidas exigidas nos termos do artigo 32.º do Regulamento (UE) 2016/679;

d) Respeita as condições a que se referem os n.ºs 2 e 4 do artigo 28.º do Regulamento (UE) 2016/679 para contratar outro subcontratado;

e) Toma em conta a natureza do tratamento, e na medida do possível, presta assistência à Casa de Investimentos através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos previstos no capítulo III do Regulamento (UE) 2016/679;

f) Presta assistência à Casa de Investimentos no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32.º a 36.º do Regulamento (UE) 2016/679, tendo em conta a natureza do tratamento e a informação ao dispor do subcontratado;

g) Consoante a escolha da Casa de Investimentos, apaga ou devolve-lhe todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo da legislação e regulamentação aplicáveis; e

h) Disponibiliza à Casa de Investimentos todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no artigo 28.º do Regulamento (UE) 2016/679 e facilita e contribui para as auditorias, *inclusive* as inspeções, conduzidas pela Casa de Investimentos ou por um auditor por esta mandatado.

No que diz respeito à alínea h), o subcontratado informa imediatamente a Casa de Investimentos se, no seu entender, alguma instrução violar o Regulamento (UE) 2016/679 ou outras disposições legais ou regulamentares aplicáveis em matéria de proteção de dados.

Se o subcontratado contratar outra entidade para a realização de operações específicas de tratamento de dados por conta da Casa de Investimentos, são impostas a esse outro subcontratado, por contrato ou outro ato

prévia e por escrito da Casa de Investimentos, a qual pode ser específica ou geral, sendo necessário, neste último caso, que a entidade subcontratada informe a Casa de Investimentos sobre quaisquer alterações que pretenda efetuar relativamente ao aumento do número ou à substituição das outras entidades subcontratantes, podendo a Casa de Investimentos opor-se a tais alterações (artigo 28.º, n.ºs 2 e 3 do Regulamento (UE) 2016/679).

As entidades subcontratadas, bem como qualquer pessoa que tenha acesso aos dados pessoais agindo sob a sua autoridade, não procede ao tratamento desses dados exceto por instrução da Casa de Investimentos, salvo nos casos em que o tratamento seja obrigatório por força da legislação e da regulamentação aplicáveis (artigo 29.º do Regulamento (UE) 2016/679).

1.18. Outras Informações a Fornecer ao Titular dos Dados

A Casa de Investimentos informa o titular dos dados sobre o direito de se opor ao tratamento, nos termos do disposto no ponto 1.15. da Política, sempre que a ele haja lugar, de modo claro e distinto, o mais tardar no momento da primeira comunicação ao titular dos dados (artigo 21.º, n.º 4 do Regulamento (UE) 2016/679).

1.19. Conservação de Documentos

A Casa de Investimentos e, sendo caso disso, o seu representante, conserva um registo de todas as atividades de tratamento realizadas sob a sua responsabilidade, do qual constam todas as seguintes informações (artigo 30.º, n.º 1 do Regulamento (UE) 2016/679):

---

normativo ao abrigo da legislação e regulamentação aplicáveis, as mesmas obrigações em matéria de proteção de dados que as estabelecidas no contrato ou outro ato normativo entre a Casa de Investimentos e o subcontratado inicial, referidas acima, em particular a obrigação de apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas a assegurar que o tratamento seja conforme com os requisitos do Regulamento (UE) 2016/679.
Se esse outro subcontratado não cumprir as suas obrigações em matéria de proteção de dados, o subcontratado inicial continua a ser plenamente responsável, perante o responsável pelo tratamento, pelo cumprimento das obrigações desse outro subcontratado.
O facto de o subcontratado cumprir um código de conduta aprovado conforme referido no artigo 40.º do Regulamento (UE) 2016/679, ou um procedimento de certificação aprovado conforme referido no artigo 42.º do mesmo diploma, pode ser utilizado como elemento para demonstrar as garantias suficientes supramencionadas.
Sem prejuízo de um eventual contrato individual entre a Casa de Investimentos e o subcontratado, o contrato ou outro ato normativo referido acima podem ser baseados, totalmente ou em parte, em cláusulas contratuais-tipo que venham a ser definidas pela Comissão Europeia ou pela Comissão Nacional de Proteção de Dados, inclusivamente quando façam parte de uma certificação concedida à Casa de Investimentos ou ao subcontratado por força dos artigos 42.º e 43.º do Regulamento (UE) 2016/679.
O contrato ou outro ato normativo devem ser feitos por escrito, incluindo em formato eletrónico.
(artigo 28.º do Regulamento (UE) 2016/679)

a) O nome e os contactos da Casa de Investimentos e, sendo caso disso, de qualquer responsável conjunto pelo tratamento, do representante da Casa de Investimentos e do seu encarregado da proteção de dados;

b) As finalidades do tratamento dos dados;

c) A descrição das categorias de titulares de dados e das categorias de dados pessoais;

d) As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou as organizações internacionais;

e) Se aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou dessas organizações internacionais e, no caso das transferências referidas no artigo 49.º, n.º 1, segundo parágrafo do Regulamento (UE) 2016/679 (conferir o ponto 1.25. da Política), a documentação que comprove a existência das garantias adequadas;

f) Se possível, os prazos previstos para o apagamento das diferentes categorias de dados;

g) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.º, n.º 1 do Regulamento (UE) 2016/679[11].

Os registos referidos são efetuados por escrito, incluindo em formato eletrónico (artigo 30.º, n.º 3 do Regulamento (UE) 2016/679).

A Casa de Investimentos e, sendo caso disso, as eventuais entidades subcontratadas, o representante da Casa de Investimentos ou da entidade subcontratada, disponibilizam, mediante

[11] O artigo 32.º, n.º 1 do Regulamento (UE) 2016/679 dispõe o seguinte:
"*1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:*
a) A pseudonimização e a cifragem dos dados pessoais;
b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.".

pedido, o registo supramencionado à Comissão Nacional de Proteção de Dados (artigo 30.º, n.º 4 do Regulamento (UE) 2016/679).

A Casa de Investimentos conserva os documentos relacionados com o tratamento de dados pessoais, de forma a poder comprovar o cumprimento do disposto na presente Política e na legislação e regulamentação aplicáveis, durante um período de sete anos a contar do termo da relação de negócio no que respeita aos dados pessoais de clientes, nos termos do disposto no ponto 1.9. da Política e dos Procedimentos de Prevenção e de Repressão do Branqueamento de Capitais e do Financiamento do Terrorismo, e durante um período de dez anos a contar da cessação da relação no âmbito da qual se originou o tratamento no que respeita aos restantes dados pessoais (artigo 24.º, n.º 1 do Regulamento (UE) 2016/679 e artigo 51.º da Lei do Branqueamento).

As versões revogadas da presente Política são conservadas por um período de sete anos a contar da respetiva alteração ou revogação, nos termos do disposto no ponto 1.9. da Política e dos Procedimentos de Prevenção e de Repressão do Branqueamento de Capitais e do Financiamento do Terrorismo, sendo colocada, em permanência, à disposição das autoridades competentes (artigos 12.º, n.º 4 e 51.º da Lei do Branqueamento).

O Responsável pelo Compliance assegura a conservação dos documentos nos termos supramencionados.

1.20. Notificação de Violações de Dados Pessoais à Comissão Nacional de Proteção de Dados

Caso qualquer colaborador da Casa de Investimentos tenha conhecimento de uma violação de dados pessoais[12], comunica-a de imediato ao encarregado da proteção de dados, o qual notifica a Comissão Nacional de Proteção de Dados, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e as liberdades das pessoas singulares (artigo 33.º, n.º 1 do Regulamento (UE) 2016/679).

Caso a notificação supramencionada não seja transmitida no prazo de 72 horas, deverá ser devidamente acompanhada da descrição dos motivos do atraso (artigo 33.º, n.º 1 do Regulamento (UE) 2016/679).

[12] **Definição de Violação de Dados Pessoais**: uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, pela Casa de Investimentos (artigo 4.º, ponto 12) do Regulamento (UE) 2016/679).

A notificação supramencionada inclui, pelo menos, os seguintes elementos:

a) A descrição da natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;

b) O nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;

c) As consequências prováveis da violação de dados pessoais;

d) A descrição das medidas adotadas ou propostas pela Casa de Investimentos para reparar a violação de dados pessoais, *inclusive*, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

Caso as informações supramencionadas não possam ser todas fornecidas ao mesmo tempo, o encarregado da proteção de dados fornece-as faseadamente, sem demora injustificada (artigo 33.º, n.º 4 do Regulamento (UE) 2016/679).

A Casa de Investimentos documenta quaisquer violações de dados pessoais, o que é assegurado pelo Responsável pelo Compliance compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada, de forma que permita às autoridades competentes a verificação do cumprimento do disposto no presente ponto da Política (artigo 33.º, n.º 5 do Regulamento (UE) 2016/679).

No âmbito da notificação de violações de dados pessoais à Comissão Nacional de Proteção de Dados a Casa de Investimentos tem ainda em conta o disposto nas Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre as notificações de violações de dados ao abrigo do Regulamento (UE) 2016/679 - WP 250 rev.01 (conferir o Anexo III).

1.21. Comunicação de Violações de Dados Pessoais ao Titular dos Dados

O Responsável pelo Compliance da Casa de Investimentos comunica ao titular dos dados, sem demora injustificada, qualquer violação de dados pessoais que seja suscetível de implicar um elevado risco para os seus direitos e liberdades (artigo 34.º, n.º 1 do Regulamento (UE) 2016/679).

A comunicação supramencionada descreve em linguagem clara e simples a natureza da violação dos dados pessoais e fornece, pelo menos, as seguintes informações (artigo 34.º, n.º 2 do Regulamento (UE) 2016/679):

a) O nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;

b) A descrição das consequências prováveis da violação de dados pessoais;

c) A descrição das medidas adotadas ou propostas pela Casa de Investimentos para reparar a violação de dados pessoais, *inclusive*, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

A Casa de Investimentos não realiza a comunicação suprarreferida, ao titular dos dados, sempre que se encontre verificada uma das seguintes situações (artigo 34.º, n.º 3 do Regulamento (UE) 2016/679):

a) A Casa de Investimentos tenha aplicado medidas de proteção adequadas, tanto técnicas como organizativas, tendo essas medidas sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, nomeadamente a cifragem;

b) A Casa de Investimentos tenha tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados, supramencionado, já não é suscetível de se concretizar; ou

c) A realização da referida comunicação implicar um esforço desproporcionado, sendo neste caso feita pela Casa de Investimentos uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados sejam informados de forma igualmente eficaz.

Se a Casa de Investimentos não tiver comunicado a violação de dados pessoais ao titular dos dados, a Comissão Nacional de Proteção de Dados, tendo considerado a probabilidade de a violação de dados pessoais resultar num elevado risco, pode exigir-lhe que proceda a essa notificação ou pode constatar que se encontram preenchidas as condições suprarreferidas para que a comunicação não tenha de ser realizada (artigo 34.º, n.º 4 do Regulamento (UE) 2016/679).

No âmbito da comunicação de violações de dados pessoais ao titular dos dados a Casa de Investimentos tem ainda em conta o disposto nas Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre as notificações de violações de dados ao abrigo do Regulamento (UE) 2016/679 - WP 250 rev.01 (conferir o Anexo III).

1.22. Avaliação de Impacto Sobre a Proteção de Dados e Consulta Prévia

Atendendo ao tipo de dados recolhidos pela Casa de Investimentos e ao contexto do tratamento de dados levado a cabo pela Casa de Investimentos, realizado no âmbito do estabelecimento de relações contratuais e do cumprimento dos deveres legais a que a Casa de Investimentos se encontra obrigada, a Casa de Investimentos considera que o tipo de tratamento de dados pessoais por si realizado não é suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos dados pessoais.

Neste contexto, a Casa de Investimentos justifica e documenta as razões que a levam a não realizar a avaliação de impacto sobre a proteção de dados, registando os pontos de vista do encarregado da proteção de dados sobre o tema (página 14 das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679 – WP 248 ver.01).

Sem prejuízo, caso venha a realizar tipos diversos de tratamento de dados, suscetíveis de implicar um elevado risco para os direitos e as liberdades dos titulares dos dados, a Casa de Investimentos encontra-se ciente da necessidade de realização de uma avaliação de impacto sobre a proteção de dados e de consulta prévia da Comissão Nacional de Proteção de Dados, pelo encarregado da proteção de dados, caso conclua pela existência de um elevado risco no seguimento da referida avaliação de impacto, nos termos do disposto nos artigos 35.º e 36.º do Regulamento (UE) 2016/679.

1.23. Nomeação do Encarregado da Proteção de Dados

A Casa de Investimentos dispõe de um encarregado da proteção de dados, designado pelo Conselho de Administração (artigo 37.º, n.º 1, alínea b) do Regulamento (UE) 2016/679 e ponto 2.1. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

O encarregado da proteção de dados não exerce funções no âmbito de grupo empresarial, exercendo-as exclusivamente na Casa de Investimentos (artigo 37.º, n.º 2 do Regulamento (UE) 2016/679).

O encarregado da proteção de dados é nomeado pelo Conselho de Administração da Casa de Investimentos com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no ponto seguinte da Política (artigo 37.º, n.º 5 do Regulamento (UE) 2016/679).

O encarregado da proteção de dados nomeado pela Casa de Investimentos tem, designadamente, competências no domínio das legislações e das práticas nacionais e europeias em matéria de proteção de dados e um conhecimento profundo do Regulamento (UE) 2016/679**,** bem como da demais legislação e regulamentação aplicáveis nesta sede (ponto 2.5. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

O encarregado da proteção de dados nomeado pela Casa de Investimentos tem ainda um bom conhecimento das operações de tratamento efetuadas pela Casa de Investimentos, bem como dos sistemas de informação, da segurança dos dados e das necessidades de proteção de dados da Casa de Investimentos, conhecendo o setor empresarial e a organização da Casa de Investimentos (ponto 2.5. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

O encarregado da proteção de dados nomeado pela Casa de Investimentos é um colaborador seu (artigo 37.º, n.º 6 do Regulamento (UE) 2016/679).

A Casa de Investimentos publica os contactos do encarregado da proteção de dados no seu sítio na Internet e comunica-os à autoridade de controlo (artigo 37.º, n.º 7 do Regulamento (UE) 2016/679).

A Casa de Investimentos divulga internamente o nome e os contactos do encarregado da proteção de dados a todos os seus colaboradores, disponibilizando-os na sua intranet (ponto 2.6. e 3.2. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

1.24. Funções do Encarregado da Proteção de Dados

O encarregado da proteção de dados da Casa de Investimentos é envolvido, de forma adequada e em tempo útil, em todas as questões da Casa de Investimentos relacionadas com a proteção de dados pessoais (artigo 38.º, n.º 1 do Regulamento (UE) 2016/679).

O encarregado da proteção de dados da Casa de Investimentos é, designadamente, convidado a participar nas reuniões em que sejam discutidas questões com implicações na proteção de dados pessoais, sendo o seu parecer devidamente ponderado e, em caso de desacordo, enunciados os motivos para que o mesmo não seja seguido (artigo 38.º, n.º 1 do Regulamento (UE) 2016/679 e ponto 3.1. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

O encarregado da proteção de dados da Casa de Investimentos tem, designadamente, as seguintes funções (artigo 39.º, n.º 1 do Regulamento (UE) 2016/679):

a) Informar e aconselhar a Casa de Investimentos, bem como os seus colaboradores envolvidos no tratamento dos dados pessoais, a respeito das suas obrigações resultantes da legislação e da regulamentação aplicáveis em matéria de proteção de dados pessoais;

b) Controlar a conformidade com a legislação e a regulamentação aplicáveis em matéria de proteção de dados pessoais, bem como com a presente Política, incluindo a repartição de responsabilidades, a sensibilização e a formação dos colaboradores implicados nas operações de tratamento de dados, e as auditorias correspondentes;

c) Prestar aconselhamento, quando tal lhe for solicitado, no que respeita a eventuais avaliações de impacto sobre a proteção de dados realizadas pela Casa de Investimentos e controlar a sua realização;

d) Cooperar com a Comissão Nacional de Proteção de Dados;

e) Ser o ponto de contacto para a Comissão Nacional de Proteção de Dados quanto a questões relacionadas com o tratamento de dados pessoais, incluindo a consulta prévia a que se refere o artigo 36.º do Regulamento (UE) 2016/679, caso a mesma se venha a verificar, consultando a referida autoridade sobre qualquer outro assunto relevante.

Para o efeito da alínea b), o encarregado da proteção de dados pode, nomeadamente, recolher informações para identificar as atividades de tratamento, analisar e verificar a conformidade das atividades de tratamento, prestar informações e aconselhamento e dirigir recomendações à Casa de

Investimentos (ponto 4. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento realizadas pela Casa de Investimentos, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento (artigo 39.º, n.º 2 do Regulamento (UE) 2016/679).

O encarregado da proteção de dados é imediatamente consultado após a ocorrência de uma violação de dados ou de outro incidente relacionado com a proteção de dados (ponto 3.1. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

O Conselho de Administração da Casa de Investimentos apoia o encarregado da proteção de dados no exercício das suas funções, fornecendo-lhe os recursos necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento (artigo 38.º, n.º 2 do Regulamento (UE) 2016/679 e ponto 3.2. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

A Casa de Investimentos não transmite instruções relativamente ao exercício das suas funções ao encarregado da proteção de dados, designadamente, instruções quanto à forma de tratar uma questão, ao resultado que deve ser obtido, à forma de investigar uma queixa ou à necessidade de consultar a Comissão Nacional de Proteção de Dados, bem como instruções no sentido de adotar determinada perspetiva sobre uma questão relacionada com as normas de proteção de dados, por exemplo determinada interpretação da legislação (artigo 38.º, n.º 3 do Regulamento (UE) 2016/679 e ponto 3.3. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

A Casa de Investimentos não destitui nem penaliza o encarregado da proteção de dados pelo facto de exercer corretamente as suas funções (artigo 38.º, n.º 3 do Regulamento (UE) 2016/679 e ponto 3.4. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

O encarregado da proteção de dados transmite a informação relacionada com as suas funções, designadamente os seus pareceres e as suas recomendações, diretamente ao Conselho de Administração da Casa de Investimentos (artigo 38.º, n.º 3 do Regulamento (UE) 2016/679 e ponto

3.3. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

Os titulares dos dados pessoais tratados pela Casa de Investimentos podem contactar o encarregado da proteção de dados sobre todas as questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos que lhe são conferidos pelo Regulamento (UE) 2016/679 (artigo 38.º, n.º 4 do Regulamento (UE) 2016/679).

O encarregado da proteção de dados está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com a legislação e a regulamentação aplicáveis (artigo 38.º, n.º 5 do Regulamento (UE) 2016/679).

O encarregado da proteção de dados pode exercer outras funções e atribuições, sendo assegurado pelo Conselho de Administração da Casa de Investimentos que essas funções e atribuições não resultam num conflito de interesses (artigo 38.º, n.º 6 do Regulamento (UE) 2016/679).

O encarregado da proteção de dados não exerce na Casa de Investimentos qualquer cargo que o leve a determinar as finalidades e os meios do tratamento de dados pessoais (ponto 3.5. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

Neste contexto, a Casa de Investimentos considera o cargo de encarregado da proteção de dados incompatível com as funções de membro do Conselho de Administração (ponto 3.5. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

Sempre que aplicável, a Casa de Investimentos assegura que o anúncio de vaga para o lugar de encarregado da proteção de dados é suficientemente preciso e pormenorizado, com vista a evitar conflitos de interesses (ponto 3.5. das Orientações do Grupo de Trabalho do Artigo 29.º para a Proteção de Dados sobre os encarregados da proteção de dados (EPD) - WP 243 ver.01).

1.25. Transferências de Dados Pessoais para Países Terceiros ou Organizações Internacionais

Atendendo ao tipo de tratamento de dados pessoais levado a cabo pela Casa de Investimentos, realizado no âmbito do estabelecimento de relações contratuais e do cumprimento dos deveres legais a que a Casa de Investimentos se encontra obrigada, a Casa de Investimentos não procede,

habitualmente, a transferências de dados pessoais para países terceiros ou para organizações internacionais (artigo 44.º do Regulamento (UE) 2016/679).

Sem prejuízo, a Casa de Investimentos encontra-se ciente do teor das normas aplicáveis caso venha a realizar transferências de dados pessoais para países terceiros ou para organizações internacionais (Capítulo V do Regulamento (UE) 2016/679).

Designadamente, a Casa de Investimentos encontra-se ciente da possibilidade de transferência de dados pessoais, sem necessidade de autorização específica, para países terceiros ou para organizações internacionais, caso a Comissão Europeia tenha decidido que o país terceiro, o território em causa ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado, nos termos do artigo 45.º do Regulamento (UE) 2016/679, transcrito no Anexo IV (artigo 44.º do Regulamento (UE) 2016/679).

Caso não tenha sido adotada qualquer decisão da Comissão Europeia, nos termos referidos no parágrafo anterior, a Casa de Investimentos encontra-se ciente de que só pode transferir dados pessoais para um país terceiro ou para uma organização internacional caso tenham apresentado garantias adequadas, na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes, nos termos previstos nos artigos 46.º e 47.º do Regulamento (UE) 2016/679, transcritos no Anexo IV (artigo 46.º, n.º 1 do Regulamento (UE) 2016/679).

Na falta de uma decisão de adequação ou de garantias adequadas nos termos supramencionados, a Casa de Investimentos encontra-se ciente da possibilidade de transferência de dados pessoais para países terceiros ou para organizações internacionais apenas quando verificada uma das seguintes condições (artigo 49.º, n.ºs 1 e 4 do Regulamento (UE) 2016/679):

a) O titular dos dados ter explicitamente dado o seu consentimento à transferência prevista, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas;

b) A transferência ser necessária para a execução de um contrato entre o titular dos dados e a Casa de Investimentos ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados;

c) A transferência ser necessária para a celebração ou a execução de um contrato, celebrado no interesse do titular dos dados, entre a Casa de Investimentos e outra pessoa singular ou coletiva;

d) A transferência ser necessária por importantes razões de interesse público, reconhecido nos termos da legislação e da regulamentação aplicáveis;

e) A transferência ser necessária à declaração, ao exercício ou à defesa de um direito num processo judicial;

f) A transferência ser necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento;

g) A transferência ser realizada a partir de um registo que, nos termos da legislação e na regulamentação aplicáveis, se destine a informar o público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar nela ter um interesse legítimo, mas apenas na medida em que as condições de consulta estabelecidas na legislação e na regulamentação aplicáveis se encontrem preenchidas nesse caso concreto.

Quando uma transferência não puder basear-se na existência de uma decisão da Comissão Europeia ou de garantias adequadas, nos termos supramencionados, não se encontrando verificada nenhuma das condições previstas nas alíneas acima, a transferência para um país terceiro ou para uma organização internacional só pode ser efetuada se não for repetitiva, apenas disser respeito a um número limitado de titulares dos dados, for necessária para efeitos dos interesses legítimos visados pela Casa de Investimentos , desde que a tais interesses não se sobreponham os interesses ou os direitos e liberdades do titular dos dados e a Casa de Investimentos tenha ponderado todas as circunstâncias relativas à transferência de dados e, com base nessa avaliação, tenha apresentado garantias adequadas no que respeita à proteção de dados pessoais (artigo 49.º, n.º 1 do Regulamento (UE) 2016/679).

A avaliação referida no parágrafo anterior e as garantias adequadas no que respeita à proteção de dados pessoais, apresentadas pela Casa de Investimentos nos termos do parágrafo anterior, são documentadas nos registos a que se refere o ponto 1.19. (artigo 49.º, n.º 6 do Regulamento (UE) 2016/679).

Neste último caso, a Casa de Investimentos informa da transferência a Comissão Nacional de Proteção de Dados e presta informação ao titular dos dados sobre a transferência e os interesses legítimos visados, além de fornecer a informação referida no ponto 1.9. da Política (artigo 49.º, n.º 1 do Regulamento (UE) 2016/679).

Caso a Casa de Investimentos realize transferências de dados pessoais com fundamento no disposto na alínea g) *supra*, estas não podem envolver a totalidade dos dados pessoais nem as categorias completas de dados pessoais constantes do registo referido e caso o registo se destine a ser consultado por pessoas com um interesse legítimo, as transferências só podem ser efetuadas a pedido dessas pessoas ou se forem elas os seus destinatários (artigo 49.º, n.º 2 do Regulamento (UE) 2016/679).

A Casa de Investimentos tem ainda em conta que as decisões judiciais e as decisões de autoridades administrativas de um país terceiro que exijam que a Casa de Investimentos transfira ou divulgue dados pessoais, só são reconhecidas ou executadas se tiverem como base um acordo internacional, como um acordo de assistência judiciária mútua, em vigor entre o país terceiro em causa e a União Europeia ou Portugal, sem prejuízo de outros motivos de transferência nos termos do Capítulo V do Regulamento (UE) 2016/679 (artigo 48.º do Regulamento (UE) 2016/679).

A Casa de Investimentos encontra-se ciente da necessidade de cumprimento da demais legislação e regulamentação aplicável às transferências de dados pessoais para países terceiros ou para organizações internacionais, caso as venha a realizar, atendendo, designadamente, às regras vinculativas aplicáveis às empresas aprovadas pela Comissão Nacional de Proteção de Dados (artigo 47.º do Regulamento (UE) 2016/679).

1.26. Aprovação, Divulgação e Avaliação da Política de Proteção de Dados Pessoais

A presente Política foi aprovada pelo Conselho de Administração da Casa de Investimentos.

Esta Política é divulgada a todos os colaboradores da Casa de Investimentos.

Cabe ao Responsável pelo Compliance da Casa de Investimentos, ao encarregado da proteção de dados e ao Conselho de Administração a avaliação da boa e efetiva aplicação da Política.

A presente Política é revista sempre que necessário e, pelo menos, com periodicidade anual.

17/EN
WP259 rev.01

Article 29 Working Party
Guidelines on consent under Regulation 2016/679

Adopted on 28 November 2017
As last Revised and Adopted on 10 April 2018

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE

PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

Contents

1. Introduction

These Guidelines provide a thorough analysis of the notion of consent in Regulation 2016/679, the General Data Protection Regulation (hereafter: GDPR). The concept of consent as used in the Data Protection Directive (hereafter: Directive 95/46/EC) and in the e-Privacy Directive to date, has evolved. The GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent. These Guidelines focus on these changes, providing practical guidance to ensure compliance with the GDPR and building upon Opinion 15/2011 on consent. The obligation is on controllers to innovate to find new solutions that operate within the parameters of the law and better support the protection of personal data and the interests of data subjects.

Consent remains one of six lawful bases to process personal data, as listed in Article 6 of the GDPR.[1] When initiating activities that involve processing of personal data, a controller must always take time to consider what would be the appropriate lawful ground for the envisaged processing.

Generally, consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful.[2]

The existing Article 29 Working Party (WP29) Opinions on consent[3] remain relevant, where consistent with the new legal framework, as the GDPR codifies existing WP29 guidance and general good practice and most of the key elements of consent remain the same under the GDPR. Therefore, in this document, WP29 expands upon and completes earlier Opinions on specific topics that include reference to consent under Directive 95/46/EC, rather than replacing them.

As stated in Opinion 15/2011 on the definition on consent, inviting people to accept a data processing operation should be subject to rigorous requirements, since it concerns the fundamental rights of data subjects and the controller wishes to engage in a processing operation that would be unlawful without the data subject's consent.[4] The crucial role of consent is underlined by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Furthermore, obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 of the GDPR with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data is

[1] Article 9 GDPR provides a list of possible exemptions to the ban on processing special categories of data. One of the exemptions listed is the situation where the data subject provides explicit consent to the use of this data.
[2] See also Opinion 15/2011 on the definition of consent (WP 187), pp. 6-8, and/or Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), pp. 9, 10, 13 and 14.
[3] Most notably, Opinion 15/2011 on the definition of consent (WP 187).
[4] Opinion 15/2011, page on the definition of consent (WP 187), p. 8

based on consent of the data subject, this would not legitimise collection of data which is not necessary in relation to a specified purpose of processing and be fundamentally unfair.[5]

Meanwhile, WP29 is aware of the review of the ePrivacy Directive (2002/58/EC). The notion of consent in the draft ePrivacy Regulation remains linked to the notion of consent in the GDPR.[6] Organisations are likely to need consent under the ePrivacy instrument for most online marketing messages or marketing calls, and online tracking methods including by the use of cookies or apps or other software. WP29 has already provided recommendations and guidance to the European legislator on the Proposal for a Regulation on ePrivacy.[7]

With regard to the existing e-Privacy Directive, WP29 notes that references to the repealed Directive 95/46/EC shall be construed as references to the GDPR.[8] This also applies to references to consent in the current Directive 2002/58/EC, as the ePrivacy Regulation will not (yet) be in force from 25 May 2018. According to Article 95 GDPR, additional obligations in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks shall not be imposed insofar the e-Privacy Directive imposes specific obligations with the same objective. WP29 notes that the requirements for consent under the GDPR are not considered to be an 'additional obligation', but rather as preconditions for lawful processing. Therefore, the GDPR conditions for obtaining valid consent are applicable in situations falling within the scope of the e-Privacy Directive.

2. Consent in Article 4(11) of the GDPR

Article 4(11) of the GDPR defines consent as: "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*"

The basic concept of consent remains similar to that under the Directive 95/46/EC and consent is one of the lawful grounds on which personal data processing has to be based, pursuant to Article 6 of the GDPR.[9] Besides the amended definition in Article 4(11), the GDPR provides additional

[5] See also Opinion 15/2011 on the definition of consent (WP 187), and Article 5 GDPR.
[6] According to Article 9 of the proposed ePrivacy Regulation, the definition of and the conditions for consent provided for in Articles 4(11) and Article 7 of the GDPR apply.
[7] See Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (WP 240).
[8] See Article 94 GDPR.
[9] Consent was defined in Directive 95/46/EC as "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*" which must be '*unambiguously given*' in order to make the processing of personal data legitimate (Article 7(a) of Directive 95/46/EC)). See WP29 Opinion 15/2011 on the definition of consent (WP 187) for examples on the appropriateness of consent as lawful basis. In this Opinion, WP29 has provided guidance to distinguish where consent is an appropriate lawful basis from those where relying on the legitimate interest ground (perhaps with an opportunity to opt out) is sufficient or a contractual relation would be recommended. See also WP29 Opinion 06/2014, paragraph III.1.2, p. 14 and further. Explicit consent is also one of the exemptions to the prohibition on the processing of special categories of data: See Article 9 GDPR.

guidance in Article 7 and in recitals 32, 33, 42, and 43 as to how the controller must act to comply with the main elements of the consent requirement.

Finally, the inclusion of specific provisions and recitals on the withdrawal of consent confirms that consent should be a reversible decision and that there remains a degree of control on the side of the data subject.

3. Elements of valid consent

Article 4(11) of the GDPR stipulates that consent of the data subject means any:

- freely given,
- specific,
- informed and
- unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

In the sections below, it is analysed to what extent the wording of Article 4(11) requires controllers to change their consent requests/forms, in order to ensure compliance with the GDPR.[10]

3.1. Free / freely given[11]

The element “free” implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.[12] If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment.[13] The notion of imbalance between the controller and the data subject is also taken into consideration by the GDPR.

When assessing whether consent is freely given, one should also take into account the specific situation of tying consent into contracts or the provision of a service as described in Article 7(4). Article 7(4) has been drafted in a non-exhaustive fashion by the words “inter alia”, meaning that there may be a range of other situations which are caught by this provision. In general terms, any

[10] For guidance with regard to ongoing processing activities based on consent in Directive 95/46, see chapter 7 of this document and recital 171 of the GDPR.
[11] In several opinions, the Article 29 Working Party has explored the limits of consent in situations where it cannot be freely given. This was notably the case in its Opinion 15/2011 on the definition of consent (WP 187), Working Document on the processing of personal data relating to health in electronic health records (WP 131), Opinion 8/2001 on the processing of personal data in the employment context (WP48), and Second opinion 4/2009 on processing of data by the World Anti-Doping Agency (WADA) (International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations (WP 162).
[12] See Opinion 15/2011 on the definition of consent (WP187), p. 12
[13] See Recitals 42, 43 GDPR and WP29 Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, (WP 187), p. 12.

element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid.

> [Example 1]
> A mobile app for photo editing asks its users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes. Neither geo-localisation or online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.

3.1.1. Imbalance of power

Recital 43[14] clearly indicates that it is unlikely that **public authorities** can rely on consent for processing as whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. WP29 considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities.[15]

Without prejudice to these general considerations, the use of consent as a lawful basis for data processing by public authorities is not totally excluded under the legal framework of the GDPR. The following examples show that the use of consent can be appropriate under certain circumstances.

> [Example 2] A local municipality is planning road maintenance works. As the road works may disrupt traffic for a long time, the municipality offers its citizens the opportunity to subscribe to an email list to receive updates on the progress of the works and on expected delays. The municipality makes clear that there is no obligation to participate and asks for consent to use email addresses for this (exclusive) purpose. Citizens that do not consent will not miss out on any core service of the municipality or the exercise of any right, so they are able to give or refuse their consent to this use of data freely. All information on the road works will also be available on the municipality's website.

> [Example 3] An individual who owns land needs certain permits from both her local municipality and from the provincial government under which the municipality resides. Both public bodies require the same information for issuing their permit, but are not accessing each other's databases. Therefore, both ask for the same information and the land owner sends out her details to both public bodies. The municipality and the provincial authority ask for her consent to merge the files, to avoid duplicate procedures and correspondence. Both public bodies ensure that this is optional and that the permit requests will still be processed separately if she decides not to consent to the merger of her data. The land owner is able to give consent to the authorities for the purpose of merging the files freely.

[14] Recital 43 GDPR states: *"In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. (…)"*
[15] See Article 6 GDPR, notably paragraphs (1c) and (1e).

[Example 4] A public school asks students for consent to use their photographs in a printed student magazine. Consent in these situations would be a genuine choice as long as students will not be denied education or services and could refuse the use of these photographs without any detriment.[16]

An imbalance of power also occurs in the **employment** context.[17] Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera-observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent.[18] Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee.[19]

However this does not mean that employers can never rely on consent as a lawful basis for processing. There may be situations when it is possible for the employer to demonstrate that consent actually is freely given. Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent.[20]

[Example 5]
A film crew is going to be filming in a certain part of an office. The employer asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penalised in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming.

Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will.

3.1.2. Conditionality

[16] For the purposes of this example, a public school means a publically funded school or any educational facility that qualifies as a public authority or body by national law.
[17] See also Article 88 GDPR, where the need for protection of the specific interests of employees is emphasized and a possibility for derogations in Member State law is created. See also Recital 155.
[18] See Opinion 15/2011 on the definition of consent (WP 187), pp. 12-14 , Opinion 8/2001 on the processing of personal data in the employment context (WP 48), Chapter 10, Working document on the surveillance of electronic communications in the workplace (WP 55), paragraph 4.2 and Opinion 2/2017 on data processing at work (WP 249), paragraph 6.2.
[19] See Opinion 2/2017 on data processing at work, page 6-7
[20] See also Opinion 2/2017 on data processing at work (WP249), paragraph 6.2.

To assess whether consent is freely given, Article 7(4) GDPR plays an important role.[21]
Article 7(4) GDPR indicates that, inter alia, the situation of "bundling" consent with acceptance of terms or conditions, or "tying" the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given (recital 43). Article 7(4) seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract of a service for which these personal data are not necessary. In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract. The two lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged and blurred.

Compulsion to agree with the use of personal data additional to what is strictly necessary limits data subject's choices and stands in the way of free consent. As data protection law is aiming at the protection of fundamental rights, an individual's control over their personal data is essential and there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service.

Hence, whenever a request for consent is tied to the performance of a contract by the controller, a data subject that does not wish to make his/her personal data available for processing by the controller runs the risk to be denied services they have requested.

To assess whether such a situation of bundling or tying occurs, it is important to determine what the scope of the contract is and what data would be necessary for the performance of that contract.
According to Opinion 06/2014 of WP29, the term "necessary for the performance of a contract" needs to be interpreted strictly. The processing must be necessary to fulfil the contract with each individual data subject. This may include, for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to facilitate payment. In the employment context, this ground may allow, for example, the processing of salary information and bank account details so that wages can be paid.[22] There needs to be a direct and objective link between the processing of the data and the purpose of the execution of the contract.

If a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis.[23]

---

[21] Article 7(4) GDPR: "*When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*" See also Recital 43 GDPR, that states: "*[…] Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent, despite such consent not being necessary for such performance.*"
[22] For more information and examples, see Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, adopted by WP29 on 9 April 2014, p. 16-17. (WP 217).
[23] The appropriate lawful basis could then be Article 6(1)(b) (contract).

Article 7(4) is only relevant where the requested data are **not** necessary for the performance of the contract, (including the provision of a service), and the performance of that contract is made conditional on the obtaining of these data on the basis of consent. Conversely, if processing **is** necessary to perform the contract (including to provide a service), then Article 7(4) does not apply.

> [Example 6]
> A bank asks customers for consent to allow third parties to use their payment details for direct marketing purposes. This processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services. If the customer's refusal to consent to this processing purpose would lead to the denial of banking services, closure of the bank account, or, depending on the case, an increase of the fee, consent cannot be freely given.

The choice of the legislator to highlight conditionality, amongst others, as a presumption of a lack of freedom to consent, demonstrates that the occurrence of conditionality must be carefully scrutinized. The term "utmost account" in Article 7(4) suggests that special caution is needed from the controller when a contract (which could include the provision of a service) has a request for consent to process personal data tied to it.

As the wording of Article 7(4) is not construed in an absolute manner, there might be very limited space for cases where this conditionality would not render the consent invalid. However, the word "presumed" in Recital 43 clearly indicates that such cases will be highly exceptional.

In any event, the burden of proof in Article 7(4) is on the controller.[24] This specific rule reflects the general principle of accountability which runs throughout the GDPR. However, when Article 7(4) applies, it will be more difficult for the controller to prove that consent was given freely by the data subject.[25]

The controller could argue that his organisation offers data subjects genuine choice if they were able to choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by the same controller that does not involve consenting to data use for additional purposes on the other hand. As long as there is a possibility to have the contract performed or the contracted service delivered by this controller without consenting to the other or additional data use in question, this means there is no longer a conditional service. However, both services need to be genuinely equivalent.

The WP29 considers that consent cannot be considered as freely given if a controller argues that a choice exists between its service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by a different controller on the other

[24] See also Article 7(1) GDPR, which states that the controller needs to demonstrate that the data subject's agreement was freely given.
[25] To some extent, the introduction of this paragraph is a codification of existing WP29 guidance. As described in Opinion 15/2011, when a data subject is in a situation of dependence on the data controller – due to the nature of the relationship or to special circumstances – there may be a strong presumption that freedom to consent is limited in such contexts (e.g. in an employment relationship or if the collection of data is performed by a public authority). With Article 7(4) in force, it will be more difficult for the controller to prove that consent was given freely by the data subject. See: Opinion 15/2011 on the definition of consent (WP 187), pp. 12-17.

hand. In such a case, the freedom of choice would be made dependant on what other market players do and whether an individual data subject would find the other controller's services genuinely equivalent. It would furthermore imply an obligation for controllers to monitor market developments to ensure the continued validity of consent for their data processing activities, as a competitor may alter its service at a later stage. Hence, using this argument means this consent fails to comply with the GDPR.

3.1.3. Granularity

A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR.

Recital 43 clarifies that consent is presumed not to be freely given if the process/procedure for obtaining consent does not allow data subjects to give separate consent for personal data processing operations respectively (e.g. only for some processing operations and not for others) despite it being appropriate in the individual case. Recital 32 states "*Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them*".

If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. This granularity is closely related to the need of consent to be specific, as discussed in section 3.2 further below. When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose.

> [Example 7]
> Within the same consent request a retailer asks its customers for consent to use their data to send them marketing by email and also to share their details with other companies within their group. This consent is not granular as there is no separate consents for these two separate purposes, therefore the consent will not be valid. In this case, a specific consent should be collected to send the contact details to commercial partners. Such specific consent will be deemed valid for each partner (see also section 3.3.1), whose identity has been provided to the data subject at the time of the collection of his or her consent, insofar as it is sent to them for the same purpose (in this example: a marketing purpose).

3.1.4. Detriment

The controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment (recital 42). For example, the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and thus no clear disadvantage for those withdrawing consent.

Other examples of detriment are deception, intimidation, coercion or significant negative consequences if a data subject does not consent. The controller should be able to prove that the data subject had a free or genuine choice about whether to consent and that it was possible to withdraw consent without detriment.

If a controller is able to show that a service includes the possibility to withdraw consent without any negative consequences e.g. without the performance of the service being downgraded to the detriment of the user, this may serve to show that the consent was given freely. The GDPR does not preclude all incentives but the onus would be on the controller to demonstrate that consent was still freely given in all the circumstances.

> [Example 8]
> When downloading a lifestyle mobile app, the app asks for consent to access the phone's accelerometer. This is not necessary for the app to work, but it is useful for the controller who wishes to learn more about the movements and activity levels of its users. When the user later revokes that consent, she finds out that the app now only works to a limited extent. This is an example of detriment as meant in Recital 42, which means that consent was never validly obtained (and thus, the controller needs to delete all personal data about users' movements collected this way).

> [Example 9]
> A data subject subscribes to a fashion retailer's newsletter with general discounts. The retailer asks the data subject for consent to collect more data on shopping preferences to tailor the offers to his or her preferences based on shopping history or a questionnaire that is voluntary to fill out. When the data subject later revokes consent, he or she will receive non-personalised fashion discounts again. This does not amount to detriment as only the permissible incentive was lost.

> [Example: 10]
> A fashion magazine offers readers access to buy new make-up products before the official launch.
> The products will shortly be made available for sale, but readers of this magazine are offered an exclusive preview of these products. In order to enjoy this benefit, people must give their postal address and agree to subscription on the mailing list of the magazine. The postal address is necessary for shipping and the mailing list is used for sending commercial offers for products such as cosmetics or t-shirts year round.
> The company explains that the data on the mailing list will only be used for sending merchandise and paper advertising by the magazine itself and is not to be shared with any other organisation.
> In case the reader does not want to disclose their address for this reason, there is no detriment, as the products will be available to them anyway.

3.2. Specific

Article 6(1)(a) confirms that the consent of the data subject must be given in relation to "one or more specific" purposes and that a data subject has a choice in relation to each of them.[26] The requirement that consent must be '*specific*' aims to ensure a degree of user control and transparency for the data subject. This requirement has not been changed by the GDPR and remains closely linked to the requirement of 'informed' consent. At the same time it must be interpreted in line with the requirement for 'granularity' to obtain 'free' consent.[27] In sum, to comply with the element of 'specific' the controller must apply:

(i) Purpose specification as a safeguard against function creep,
(ii) Granularity in consent requests, and
(iii) Clear separation of information related to obtaining consent for data processing activities from information about other matters.

[26] Further guidance on the determination of 'purposes' can be found in Opinion 3/2013 on purpose limitation (WP 203).
[27] Recital 43 GDPR states that separate consent for different processing operations will be needed wherever appropriate. Granular consent options should be provided to allow data subjects to consent separately to separate purposes.

Ad. (i): Pursuant to Article 5(1)(b) GDPR, obtaining valid consent is always preceded by the determination of a specific, explicit and legitimate purpose for the intended processing activity.[28] The need for specific consent in combination with the notion of purpose limitation in Article 5(1)(b) functions as a safeguard against the gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection of the data. This phenomenon, also known as function creep, is a risk for data subjects, as it may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control.

If the controller is relying on Article 6(1)(a), data subjects must always give consent for a specific processing purpose.[29] In line with the concept of *purpose limitation*, Article 5(1)(b) and recital 32, consent may cover different operations, as long as these operations serve the same purpose. It goes without saying that specific consent can only be obtained when data subjects are specifically informed about the intended purposes of data use concerning them.

Notwithstanding the provisions on compatibility of purposes, consent must be specific to the purpose. Data subjects will give their consent with the understanding that they are in control and their data will only be processed for those specified purposes. If a controller processes data based on consent and wishes to process the data for another purpose, too, that controller needs to seek additional consent for this other purpose unless there is another lawful basis which better reflects the situation.

> [Example 11] A cable TV network collects subscribers' personal data, based on their consent, to present them with personal suggestions for new movies they might be interested in based on their viewing habits. After a while, the TV network decides it would like to enable third parties to send (or display) targeted advertising on the basis of the subscriber's viewing habits. Given this new purpose, new consent is needed.

Ad. (ii): Consent mechanisms must not only be granular to meet the requirement of 'free', but also to meet the element of 'specific'. This means, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes.

Ad. (iii): Lastly, controllers should provide specific information with each separate consent request about the data that are processed for each purpose, in order to make data subjects aware of the impact of the different choices they have. Thus, data subjects are enabled to give specific consent. This issue overlaps with the requirement that controllers must provide clear information, as discussed in paragraph 3.3. below.

3.3. Informed

The GDPR reinforces the requirement that consent must be informed. Based on Article 5 of the GDPR, the requirement for transparency is one of the fundamental principles, closely related to the

[28] See WP 29 Opinion 3/2013 on purpose limitation (WP 203), p. 16, : "*For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'.*"
[29] This is consistent with WP29 Opinion 15/2011 on the definition of consent (WP 187), for example on p. 17.

principles of fairness and lawfulness. Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.

The consequence of not complying with the requirements for informed consent is that consent will be invalid and the controller may be in breach of Article 6 of the GDPR.

3.3.1. Minimum content requirements for consent to be 'informed'

For consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. Therefore, WP29 is of the opinion that at least the following information is required for obtaining valid consent:

(i) the controller's identity, [30]
(ii) the purpose of each of the processing operations for which consent is sought,[31]
(iii) what (type of) data will be collected and used, [32]
(iv) the existence of the right to withdraw consent,[33]
(v) information about the use of the data for automated decision-making in accordance with Article 22 (2)(c)[34] where relevant, and
(vi) on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46.[35]

With regard to item (i) and (iii), WP29 notes that in a case where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named. Processors do not need to be named as part of the consent requirements, although to comply with Articles 13 and 14 of the GDPR, controllers will need to provide a full list of recipients or categories of recipients including processors. To conclude, WP29 notes that depending on the circumstances and context of a case, more information may be needed to allow the data subject to genuinely understand the processing operations at hand.

3.3.2. How to provide information

The GDPR does not prescribe the form or shape in which information must be provided in order to fulfil the requirement of informed consent. This means valid information may be presented in various ways, such as written or oral statements, or audio or video messages. However, the GDPR

[30] See also Recital 42 GDPR: " *[…]For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.[…]."*
[31] Again, see Recital 42 GDPR
[32] See also WP29 Opinion 15/2011 on the definition of consent (WP 187) pp.19-20
[33] See Article 7(3) GDPR
[34] See also WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), paragraph IV.B, p. 20 onwards.
[35] Pursuant to Article 49 (1)(a), specific information is required about the absence of safeguards described in Article 46, when explicit consent is sought. See also WP29 Opinion 15/2011 on the definition of consent (WP 187)p. 19

puts several requirements for informed consent in place, predominantly in Article 7(2) and Recital 32. This leads to a higher standard for the clarity and accessibility of the information.

When seeking consent, controllers should ensure that they use clear and plain language in all cases. This means a message should be easily understandable for the average person and not only for lawyers. Controllers cannot use long privacy policies that are difficult to understand or statements full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form. This requirement essentially means that information relevant for making informed decisions on whether or not to consent may not be hidden in general terms and conditions.[36]

A controller must ensure that consent is provided on the basis of information that allows the data subjects to easily identify who the controller is and to understand what they are agreeing to. The controller must clearly describe the purpose for data processing for which consent is requested.[37]

Other specific guidance on the accessibility has been provided in the WP29 guidelines on transparency. If consent is to be given by electronic means, the request must be clear and concise. Layered and granular information can be an appropriate way to deal with the two-fold obligation of being precise and complete on the one hand and understandable on the other hand.

A controller must assess what kind of audience it is that provides personal data to their organisation. For example, in case the targeted audience includes data subjects that are underage, the controller is expected to make sure information is understandable for minors.[38] After identifying their audience, controllers must determine what information they should provide and, subsequently how they will present the information to data subjects.

Article 7(2) addresses pre-formulated written declarations of consent which also concern other matters. When consent is requested as part of a (paper) contract, the request for consent should be clearly distinguishable from the other matters. If the paper contract includes many aspects that are unrelated to the question of consent to the use of personal data, the issue of consent should be dealt with in a way that clearly stands out, or in a separate document. Likewise, if consent is requested by electronic means, the consent request has to be separate and distinct, it cannot simply be a paragraph within terms and conditions, pursuant to Recital 32.[39] To accommodate for small screens or situations with restricted room for information, a layered way of presenting information can be considered, where appropriate, to avoid excessive disturbance of user experience or product design.

[36] The declaration of consent must be named as such. Drafting, such as "I know that…" does not meet the requirement of clear language.
[37] See Articles 4(11) and 7(2) GDPR.
[38] See also Recital 58 regarding information understandable for children.
[39] See also Recital 42 and Directive 93/13/EC, notably Article 5 (plain intelligible language and in case of doubt, the interpretation will be in favour of consumer) and Article 6 (invalidity of unfair terms, contract continues to exist without these terms only if still sensible, otherwise the whole contract is invalid).

A controller that relies on consent of the data subject must also deal with the separate information duties laid down in Articles 13 and 14 in order to be compliant with the GDPR. In practice, compliance with the information duties and compliance with the requirement of informed consent may lead to an integrated approach in many cases. However, this section is written in the understanding that valid "informed" consent can exist, even when not all elements of Articles 13 and/or 14 are mentioned in the process of obtaining consent (these points should of course be mentioned in other places, such as the privacy notice of a company). WP29 has issued separate guidelines on the requirement of transparency.

[Example 12]
Company X is a controller that received complaints that it is unclear to data subjects for what purposes of data use they are asked to consent to. The company sees the need to verify whether its information in the consent request is understandable for data subjects. X organises voluntary test panels of specific categories of its customers and presents new updates of its consent information to these test audiences before communicating it externally. The selection of the panel respects the principle of independence and is made on the basis of standards ensuring a representative, non-biased outcome. The panel receives a questionnaire and indicates what they understood of the information and how they would score it in terms of understandable and relevant information. The controller continues testing until the panels indicate that the information is understandable. X draws up a report of the test and keeps this available for future reference. This example shows a possible way for X to demonstrate that data subjects were receiving clear information before consenting to personal data processing by X.

[Example 13]
A company engages in data processing on the basis of consent. The company uses a layered privacy notice that includes a consent request. The company discloses all basic details of the controller and the data processing activities envisaged.[40] However, the company does not indicate how their data protection officer can be contacted in the first information layer of the notice. For the purposes of having a valid lawful basis as meant in Article 6, this controller obtained valid "informed" consent, even when the contact details of the data protection officer have not been communicated to the data subject (in the first information layer), pursuant to Article 13(1)(b) or 14(1)(b) GDPR.

3.4. Unambiguous indication of wishes

The GDPR is clear that consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing.

Article 2(h) of Directive 95/46/EC described consent as an "indication of wishes by which the data subject signifies his agreement to personal data relating to him being processed". Article 4(11) GDPR builds on this definition, by clarifying that valid consent requires an *unambiguous* indication by means of a *statement or by a clear affirmative action*, in line with previous guidance issued by the WP29.

[40] Note that when the identity of the controller or the purpose of the processing is not apparent from the first information layer of the layered privacy notice (and are located in further sub-layers), it will be difficult for the data controller to demonstrate that the data subject has given informed consent, unless the data controller can show that the data subject in question accessed that information prior to giving consent.

A “clear affirmative act” means that the data subject must have taken a deliberate action to consent to the particular processing.[41] Recital 32 sets out additional guidance on this. Consent can be collected through a written or (a recorded) oral statement, including by electronic means.

Perhaps the most literal way to fulfil the criterion of a “written statement” is to make sure a data subject writes in a letter or types an email to the controller explaining what exactly he/she agrees to. However, this is often not realistic. Written statements can come in many shapes and sizes that could be compliant with the GDPR.

Without prejudice to existing (national) contract law, consent can be obtained through a recorded oral statement, although due note must be taken of the information available to the data subject, prior to the indication of consent. The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice.

> [Example 14]
> When installing software, the application asks the data subject for consent to use non-anonymised crash reports to improve the software. A layered privacy notice providing the necessary information accompanies the request for consent. By actively ticking the optional box stating, “I consent”, the user is able to validly perform a ´clear affirmative act´ to consent to the processing.

A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data. The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example ‘opt-out boxes’).[42]

When consent is to be given following a request by electronic means, the request for consent should not be *unnecessarily* disruptive to the use of the service for which the consent is provided.[43] An active affirmative motion by which the data subject indicates consent can be necessary when a less infringing or disturbing modus would result in ambiguity. Thus, it may be necessary that a consent request interrupts the use experience to some extent to make that request effective.

---

[41] See Commission Staff Working Paper, Impact Assessment, Annex 2, p. 20 and also pp. 105-106: “*As also pointed out in the opinion adopted by WP29 on consent, it seems essential to clarify that valid consent requires the use of mechanisms that leave no doubt of the data subject’s intention to consent, while making clear that – in the context of the on-line environment – the use of default options which the data subject is required to modify in order to reject the processing ('consent based on silence') does not in itself constitute unambiguous consent. This would give individuals more control over their own data, whenever processing is based on his/her consent. As regards impact on data controllers, this would not have a major impact as it solely clarifies and better spells out the implications of the current Directive in relation to the conditions for a valid and meaningful consent from the data subject. In particular, to the extent that 'explicit' consent would clarify – by replacing "unambiguous" – the modalities and quality of consent and that it is not intended to extend the cases and situations where (explicit) consent should be used as a ground for processing, the impact of this measure on data controllers is not expected to be major*.”

[42] See Article 7(2). See also Working Document 02/2013 on obtaining consent for cookies (WP 208), pp. 3-6.

[43] See Recital 32 GDPR.

However, within the requirements of the GDPR, controllers have the liberty to develop a consent flow that suits their organisation. In this regard, physical motions can be qualified as a clear affirmative action in compliance with the GDPR.

Controllers should design consent mechanisms in ways that are clear to data subjects. Controllers must avoid ambiguity and must ensure that the action by which consent is given can be distinguished from other actions. Therefore, merely continuing the ordinary use of a website is not conduct from which one can infer an indication of wishes by the data subject to signify his or her agreement to a proposed processing operation.

> **[**Example 15]
> Swiping a bar on a screen, waiving in front of a smart camera, turning a smartphone around clockwise, or in a figure eight motion may be options to indicate agreement, as long as clear information is provided, and it is clear that the motion in question signifies agreement to a specific request (e.g. if you swipe this bar to the left, you agree to the use of information X for purpose Y. Repeat the motion to confirm). The controller must be able to demonstrate that consent was obtained this way and data subjects must be able to withdraw consent as easily as it was given.
>
> [Example 16]
> Scrolling down or swiping through a website will not satisfy the requirement of a clear and affirmative action. This is because the alert that continuing to scroll will constitute consent may be difficult to distinguish and/or may be missed when a data subject is quickly scrolling through large amounts of text and such an action is not sufficiently unambiguous.

In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing.

This results in a situation where consent questions are no longer read. This is a particular risk to data subjects, as, typically, consent is asked for actions that are in principle unlawful without their consent. The GDPR places upon controllers the obligation to develop ways to tackle this issue.

An often-mentioned example to do this in the online context is to obtain consent of Internet users via their browser settings. Such settings should be developed in line with the conditions for valid consent in the GDPR, as for instance that the consent shall be granular for each of the envisaged purposes and that the information to be provided, should name the controllers.

In any event, consent must always be obtained before the controller starts processing personal data for which consent is needed. WP29 has consistently held in previous opinions that consent should be given prior to the processing activity.[44] Although the GDPR does not literally prescribe in Article 4(11) that consent must be given prior to the processing activity, this is clearly implied. The heading of Article 6(1) and the wording "has given" in Article 6(1)(a) support this interpretation. It follows logically from Article 6 and Recital 40 that a valid lawful basis must be present before

[44] WP29 has consistently held this position since Opinion 15/2011 on the definition of consent (WP 187), pp. 30-31.

starting a data processing. Therefore, consent should be given prior to the processing activity. In principle, it can be sufficient to ask for a data subject's consent once. However, controllers do need to obtain a new and specific consent if purposes for data processing change after consent was obtained or if an additional purpose is envisaged.

4. Obtaining explicit consent

Explicit consent is required in certain situations where serious data protection risk emerge, hence, where a high level of individual control over personal data is deemed appropriate. Under the GDPR, explicit consent plays a role in Article 9 on the processing of special categories of data, the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards in Article 49[45], and in Article 22 on automated individual decision-making, including profiling.[46]

The GDPR prescribes that a "statement or clear affirmative action" is a prerequisite for 'regular' consent. As the 'regular' consent requirement in the GDPR is already raised to a higher standard compared to the consent requirement in Directive 95/46/EC, it needs to be clarified what extra efforts a controller should undertake in order to obtain the *explicit* consent of a data subject in line with the GDPR.

The term *explicit* refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.[47]

However, such a signed statement is not the only way to obtain explicit consent and, it cannot be said that the GDPR prescribes written and signed statements in all circumstances that require valid explicit consent. For example, in the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature. In theory, the use of oral statements can also be sufficiently express to obtain valid explicit consent, however, it may be difficult to prove for the controller that all conditions for valid explicit consent were met when the statement was recorded.

---

[45] According to Article 49 (1)(a) GDPR, explicit consent can lift the ban on data transfers to countries without adequate levels of data protection law. Also note Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP 114), p. 11, where WP29 has indicated that consent for data transfers that occur periodically or on an on-going basis is inappropriate.

[46] In Article 22, the GDPR introduces provisions to protect data subjects against decision-making based solely on automated processing, including profiling. Decisions made on this basis are allowed under certain legal conditions. Consent plays a key role in this protection mechanism, as Article 22(2)(c) GDPR makes clear that a controller may proceed with automated decision making, including profiling, that may significantly affect the individual, with the data subject's explicit consent. WP29 have produced separate guidelines on this issue: WP29 Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2017 (WP 251).

[47] See also WP29 Opinion 15/2011, on the definition of consent (WP 187), p. 25.

An organisation may also obtain explicit consent through a telephone conversation, provided that the information about the choice is fair, intelligible and clear, and it asks for a specific confirmation from the data subject (e.g. pressing a button or providing oral confirmation).

> [Example 17] A data controller may also obtain explicit consent from a visitor to its website by offering an explicit consent screen that contains Yes and No check boxes, provided that the text clearly indicates the consent, for instance "I, hereby, consent to the processing of my data", and not for instance, "It is clear to me that my data will be processed". It goes without saying that the conditions for informed consent as well as the other conditions for obtaining valid consent should be met.

> [Example 18] A clinic for cosmetic surgery seeks explicit consent from a patient to transfer his medical record to an expert whose second opinion is asked on the condition of the patient. The medical record is a digital file. Given the specific nature of the information concerned, the clinic asks for an electronic signature of the data subject to obtain valid explicit consent and to be able to demonstrate that explicit consent was obtained.[48]

Two stage verification of consent can also be a way to make sure explicit consent is valid. For example, a data subject receives an email notifying them of the controller's intent to process a record containing medical data. The controller explains in the email that he asks for consent for the use of a specific set of information for a specific purpose. If the data subjects agrees to the use of this data, the controller asks him or her for an email reply containing the statement 'I agree'. After the reply is sent, the data subject receives a verification link that must be clicked, or an SMS message with a verification code, to confirm agreement.

Article 9(2) does not recognize "necessary for the performance of a contract" as an exception to the general prohibition to process special categories of data. Therefore controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) subparagraphs (b) to (j). Should none of the exceptions (b) to (j) apply, obtaining explicit consent in accordance with the conditions for valid consent in the GDPR remains the only possible lawful exception to process such data.

> [Example 19]
> An airline company, Holiday Airways, offers an assisted travelling service for passengers that cannot travel unassisted, for example due to a disability. A customer books a flight from Amsterdam to Budapest and requests travel assistance to be able to board the plane. Holiday Airways requires her to provide information on her health condition to be able to arrange the appropriate services for her (hence, there are many possibilities e.g. wheelchair on the arrival gate, or an assistant travelling with her from A to B.) Holiday Airways asks for explicit consent to process the health data of this customer for the purpose of arranging the requested travel assistance. -The data processed on the basis of consent should be necessary for the requested service. Moreover, flights to Budapest remain available without travel assistance. Please note that since that data are necessary for the provision of the requested service, Article 7 (4) does not apply.

> [Example 20]
> A successful company is specialised in providing custom-made ski- and snowboard goggles, and other types of customised eyewear for outdoors sports. The idea is that people could wear these without their own glasses on. The company receives orders at a central point and delivers products from a single location all across the EU.

[48] This example is without prejudice to EU Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

In order to be able to provide its customised products to customers who are short-sighted, this controller requests consent for the use of information on customers' eye condition. Customers provide the necessary health data, such as their prescription data online when they place their order. Without this, it is not possible to provide the requested customized eyewear. The company also offers series of goggles with standardized correctional values. Customers that do not wish to share health data could opt for the standard versions. Therefore, an explicit consent under Article 9 is required and consent can be considered to be freely given.

5. Additional conditions for obtaining valid consent

The GDPR introduces requirements for controllers to make additional arrangements to ensure they obtain, and maintain and are able to demonstrate, valid consent. Article 7 of the GDPR sets out these additional conditions for valid consent, with specific provisions on keeping records of consent and the right to easily withdraw consent. Article 7 also applies to consent referred to in other articles of GDPR, e.g. Articles 8 and 9. Guidance on the additional requirement to demonstrate valid consent and on withdrawal of consent is provided below.

5.1. Demonstrate consent

In Article 7(1), the GDPR clearly outlines the explicit obligation of the controller to demonstrate a data subject's consent. The burden of proof will be on the controller, according to Article 7(1).

Recital 42 states: "*Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation.*"

Controllers are free to develop methods to comply with this provision in a way that is fitting in their daily operations. At the same time, the duty to demonstrate that valid consent has been obtained by a controller, should not in itself lead to excessive amounts of additional data processing. This means that controllers should have enough data to show a link to the processing (to show consent was obtained) but they shouldn't be collecting any more information than necessary.

It is up to the controller to prove that valid consent was obtained from the data subject. The GDPR does not prescribe exactly how this must be done. However, the controller must be able to prove that a data subject in a given case has consented. As long as a data processing activity in question lasts, the obligation to demonstrate consent exists. After the processing activity ends, proof of consent should be kept no longer then strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims, in accordance with Article 17(3)(b) and (e).

For instance, the controller may keep a record of consent statements received, so he can show how consent was obtained, when consent was obtained and the information provided to the data subject at the time shall be demonstrable. The controller shall also be able to show that the data subject was informed and the controller´s workflow met all relevant criteria for a valid consent. The rationale behind this obligation in the GDPR is that controllers must be accountable with regard to obtaining valid consent from data subjects and the consent mechanisms they have put in place. For example, in an online context, a controller could retain information on the session in which consent was expressed, together with documentation of the consent workflow at the time of the session, and a

copy of the information that was presented to the data subject at that time. It would not be sufficient to merely refer to a correct configuration of the respective website.

> [Example 21] A hospital sets up a scientific research programme, called project X, for which dental records of real patients are necessary. Participants are recruited via telephone calls to patients that voluntarily agreed to be on a list of candidates that may be approached for this purpose. The controller seeks explicit consent from the data subjects for the use of their dental record. Consent is obtained during a phone call by recording an oral statement of the data subject in which the data subject confirms that they agree to the use of their data for the purposes of project X.

There is no specific time limit in the GDPR for how long consent will last. How long consent lasts will depend on the context, the scope of the original consent and the expectations of the data subject. If the processing operations change or evolve considerably then the original consent is no longer valid. If this is the case, then new consent needs to be obtained.

WP29 recommends as a best practice that consent should be refreshed at appropriate intervals. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and how to exercise their rights.[49]

5.2. Withdrawal of consent

Withdrawal of consent is given a prominent place in the GDPR. The provisions and recitals on withdrawal of consent in the GDPR can be regarded as codification of the existing interpretation of this matter in WP29 Opinions.[50]

Article 7(3) of the GDPR prescribes that the controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time. The GDPR does not say that giving and withdrawing consent must always be done through the same action.

However, when consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily. Where consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Furthermore, the data subject should be able to withdraw his/her consent without detriment. This means, inter alia, that a controller must make withdrawal of consent possible free of charge or without lowering service levels.[51]

---

[49] See WP29 guidelines on transparency. [Citation to be finalized when available]

[50] WP29 has discussed this subject in their Opinion on consent (see Opinion 15/2011 on the definition of consent (WP 187), pp. 9, 13, 20, 27 and 32-33) and, inter alia, their Opinion on the use of location data. (see Opinion 5/2005 on the use of location data with a view to providing value-added services (WP 115), p. 7).

[51] See also opinion WP29 Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing (WP 174) and the Opinion on the use of location data with a view to providing value-added services (WP 115).

[Example 22] A music festival sells tickets through an online ticket agent. With each online ticket sale, consent is requested in order to use contact details for marketing purposes. To indicate consent for this purpose, customers can select either No or Yes. The controller informs customers that they have the possibility to withdraw consent. To do this, they could contact a call centre on business days between 8am and 5pm, free of charge. The controller in this example does not comply with article 7(3) of the GDPR. Withdrawing consent in this case requires a telephone call during business hours, this is more burdensome than the one mouse-click needed for giving consent through the online ticket vendor, which is open 24/7.

The requirement of an easy withdrawal is described as a necessary aspect of valid consent in the GDPR. If the withdrawal right does not meet the GDPR requirements, then the consent mechanism of the controller does not comply with the GDPR. As mentioned in section 3.1 on the condition of *informed* consent, the controller must inform the data subject of the right to withdraw consent prior to actually giving consent, pursuant to Article 7(3) of the GDPR. Additionally, the controller must as part of the transparency obligation inform the data subjects on how to exercise their rights.[52]

As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent - and in accordance with the GDPR - remain lawful, however, the controller must stop the processing actions concerned. If there is no other lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted by the controller.[53]

As mentioned earlier in these guidelines, it is very important that controllers assess the purposes for which data is actually processed and the lawful grounds on which it is based prior to collecting the data. Often companies need personal data for several purposes, and the processing is based on more than one lawful basis, e.g. customer data may be based on contract and consent. Hence, a withdrawal of consent does not mean a controller must erase data that are processed for a purpose that is based on the performance of the contract with the data subject. Controllers should therefore be clear from the outset about which purpose applies to each element of data and which lawful basis is being relied upon.

Controllers have an obligation to delete data that was processed on the basis of consent once that consent is withdrawn, assuming that there is no other purpose justifying the continued retention.[54] Besides this situation, covered in Article 17 (1)(b), an individual data subject may request erasure of other data concerning him that is processed on another lawful basis, e.g. on the basis of Article 6(1)(b).[55] Controllers are obliged to assess whether continued processing of the data in question is appropriate, even in the absence of an erasure request by the data subject.[56]

[52] Recital 39 GDPR, which refers to Articles 13 and 14 of that Regulation, states that *"natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.*
[53] See Article 17(1)(b) and (3) GDPR.
[54] In that case, the other purpose justifying the processing must have its own separate legal basis. This does not mean the controller can swap from consent to another lawful basis, see section 6 below.
[55] See Article 17, including exceptions that may apply, and Recital 65 GDPR
[56] See also Article 5 (1)(e) GDPR

In cases where the data subject withdraws his/her consent and the controller wishes to continue to process the personal data on another lawful basis, they cannot silently migrate from consent (which is withdrawn) to this other lawful basis. Any change in the lawful basis for processing must be notified to a data subject in accordance with the information requirements in Articles 13 and 14 and under the general principle of transparency.

6. Interaction between consent and other lawful grounds in Article 6 GDPR

Article 6 sets the conditions for a lawful personal data processing and describes six lawful bases on which a controller can rely. The application of one of these six bases must be established prior to the processing activity and in relation to a specific purpose.[57]

It is important to note here that if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent. Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals.

In other words, the controller cannot swap from consent to other lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. Because of the requirement to disclose the lawful basis which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is.

7. Specific areas of concern in the GDPR

7.1. Children (Article 8)

Compared to the current directive, the GDPR creates an additional layer of protection where personal data of vulnerable natural persons, especially children, are processed. Article 8 introduces additional obligations to ensure an enhanced level of data protection of children in relation to information society services. The reasons for the enhanced protection are specified in Recital 38: *" [...] they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data [...]"* Recital 38 also states that *"Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child."* The words 'in particular' indicate that the specific protection is not confined to marketing or profiling but includes the wider 'collection of personal data with regard to children'.

Article 8(1) states that where consent applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful

[57] Pursuant to Articles 13 (1)(c) and/or 14(1)(c), the controller must inform the data subject thereof.

only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.[58] Regarding the age limit of valid consent the GDPR provides flexibility, Member States can provide by law a lower age, but this age cannot be below 13 years.

As mentioned in section 3.1. on informed consent, the information shall be understandable to the audience addressed by the controller, paying particular attention to the position of children. In order to obtain "informed consent" from a child, the controller must explain in language that is clear and plain for children how it intends to process the data it collects.[59] If it is the parent that is supposed to consent, then a set of information may be required that allows adults to make an informed decision.

It is clear from the foregoing that Article 8 shall only apply when the following conditions are met:

- The processing is related to the offer of information society services directly to a child.[60, 61]
- The processing is based on consent.

7.1.1. Information society service

To determine the scope of the term 'information society service" in the GDPR, reference is made in Article 4(25) GDPR to Directive 2015/1535.

While assessing the scope of this definition, WP29 also refers to case law of the ECJ.[62] The ECJ held that *information society services* cover contracts and other services that are concluded or transmitted on-line. Where a service has two economically independent components, one being the online component, such as the offer and the acceptance of an offer in the context of the conclusion of a contract or the information relating to products or services, including marketing activities, this component is defined as an information society service, the other component being the physical delivery or distribution of goods is not covered by the notion of an information society service. The online delivery of a service would fall within the scope of the term *information society service* in Article 8 GDPR.

---

[58] Without prejudice to the possibility of Member State law to derogate from the age limit, see Article 8(1).

[59] Recital 58 GDPR re-affirms this obligation, in stating that, where appropriate, a controller should make sure the information provided is understandable for children.

[60] According to Article 4(25) GDPR an information society service means a service as defined in point (b) of Article 1(1) of Directive 2015/1535: "*(b) 'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request."* An indicative list of services not covered by this definition is set out in Annex I of the said Directive. See also Recital 18 of Directive 2000/31.

[61] According to the UN Convention on the Protection of the Child, Article 1, *"[…] a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier,"* see United Nations, General Assembly Resolution 44/25 of 20 November 1989 (Convention on the Rights of the Child).

[62] See European Court of Justice, 2 December 2010 Case C-108/09, (*Ker-Optika),* paragraphs 22 and 28. In relation to 'composite services', WP29 also refers to Case C-434/15 *(Asociacion Profesional Elite Taxi v Uber Systems Spain SL),* para 40, which states that an information society service forming an integral part of an overall service whose main component is not an information society service (in this case a transport service), must not be qualified as 'an information society service'.

7.1.2. Offered directly to a child

The inclusion of the wording 'offered directly to a child' indicates that Article 8 is intended to apply to some, not all information society services. In this respect, if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be 'offered directly to a child' and Article 8 will not apply.

7.1.3. Age

The GDPR specifies that *"Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."* The controller must be aware of those different national laws, by taking into account the public targeted by its services. In particular it should be noted that a controller providing a cross-border service cannot always rely on complying with only the law of the Member State in which it has its main establishment but may need to comply with the respective national laws of each Member State in which it offers the information society service(s). This depends on whether a Member State chooses to use the place of main establishment of the controller as a point of reference in its national law, or the residence of the data subject. First of all the Member States shall consider the best interests of the child during making their choice. The Working Group encourages the Member States to search for a harmonized solution in this matter.

When providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities.

If the users state that they are over the age of digital consent then the controller can carry out appropriate checks to verify that this statement is true. Although the need to undertake reasonable efforts to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful.

If the user states that he/she is below the age of digital consent then the controller can accept this statement without further checks, but will need to go on to obtain parental authorisation and verify that the person providing that consent is a holder of parental responsibility.

Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor.[63] If doubts arise the controller

[63] Although this may not be a watertight solution in all cases, it is an example to deal with this provision

should review their age verification mechanisms in a given case and consider whether alternative checks are required.[64]

7.1.4. Children's consent and parental responsibility

Regarding the authorisation of a holder of parental responsibility, the GDPR does not specify practical ways to gather the parent's consent or to establish that someone is entitled to perform this action.[65] Therefore, the WP29 recommends the adoption of a proportionate approach, in line with Article 8(2) GDPR and Article 5(1)(c) GDPR (data minimisation). A proportionate approach may be to focus on obtaining a limited amount of information, such as contact details of a parent or guardian.

What is reasonable, both in terms of verifying that a user is old enough to provide their own consent, and in terms of verifying that a person providing consent on behalf of a child is a holder of parental responsibility, may depend upon the risks inherent in the processing as well as the available technology. In low-risk cases, verification of parental responsibility via email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information pursuant to Article 7(1) GDPR.[66] Trusted third party verification services may offer solutions which minimise the amount of personal data the controller has to process itself.

> [Example 23] An online gaming platform wants to make sure underage customers only subscribe to its services with the consent of their parents or guardians. The controller follows these steps:
> Step 1: ask the user to state whether they are under or over the age of 16 (or alternative age of digital consent)
> If the user states that they are under the age of digital consent:
> Step 2: service informs the child that a parent or guardian needs to consent or authorise the processing before the service is provided to the child. The user is requested to disclose the email address of a parent or guardian.
> Step 3: service contacts the parent or guardian and obtains their consent via email for processing and take reasonable steps to confirm that the adult has parental responsibility.
> Step 4: in case of complaints, the platform takes additional steps to verify the age of the subscriber.
> If the platform has met the other consent requirements, the platform can comply with the additional criteria of Article 8 GDPR by following these steps.

The example shows that the controller can put itself in a position to show that reasonable efforts have been made to ensure that valid consent has been obtained, in relation to the services provided to a child. Article 8(2) particularly adds that "*The controller shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.*"

---

[64] See WP29 Opinion 5/2009 on social networking services (WP 163).
[65] WP 29 notes that it not always the case that the holder of parental responsibility is the natural parent of the child and that parental responsibility can be held by multiple parties which may include legal as well as natural persons.
[66] For example, a parent or guardian could be asked to make a payment of €0,01 to the controller via a bank transaction, including a brief confirmation in the description line of the transaction that the bank account holder is a holder of parental responsibility over the user. Where appropriate, an alternative method of verification should be provided to prevent undue discriminatory treatment of persons that do not have a bank account.

It is up to the controller to determine what measures are appropriate in a specific case. As a general rule, controllers should avoid verification solutions which themselves involve excessive collection of personal data.

WP29 acknowledges that there may be cases where verification is challenging (for example where children providing their own consent have not yet established an 'identity footprint', or where parental responsibility is not easily checked. This can be taken into account when deciding what efforts are reasonable, but controllers will also be expected to keep their processes and the available technology under constant review.

With regard to the data subject's autonomy to consent to the processing of their personal data and have full control over the processing, consent by a holder of parental responsibility or authorized by a holder of parental responsibility for the processing of personal data of children can be confirmed, modified or withdrawn, once the data subject reaches the age of digital consent.

In practice, this means that if the child does not take any action, consent given by a holder of parental responsibility or authorized by a holder of parental responsibility for the processing of personal data given prior to the age of digital consent, will remain a valid ground for processing.

After reaching the age of digital consent, the child will have the possibility to withdraw the consent himself, in line with Article 7(3). In accordance with the principles of fairness and accountability, the controller must inform the child about this possibility.[67]

It is important to point out that in accordance with Recital 38, consent by a parent or guardian is not required in the context of preventive or counselling services offered directly to a child. For example the provision of child protection services offered online to a child by means of an online chat service do not require prior parental authorisation.

Finally, the GDPR states that the rules concerning parental authorization requirements vis-à-vis minors shall not interfere with "the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child". Therefore, the requirements for valid consent for the use of data about children are part of a legal framework that must be regarded as separate from national contract law. Therefore, this guidance paper does not deal with the question whether it is lawful for a minor to conclude online contracts. Both legal regimes may apply simultaneously, and, the scope of the GDPR does not include harmonization of national provisions of contract law.

7.2. Scientific research

The definition of scientific research purposes has substantial ramifications for the range of data processing activities a controller may undertake. The term *'scientific research'* is not defined in the GDPR. Recital 159 states "(…) *For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner.* (…)", however the WP29

[67] Also, data subjects should be aware of the right to be forgotten as laid down in Article 17, which is in particular relevant for consent given when the data subject was still a child, see recital 63.

considers the notion may not be stretched beyond its common meaning and understands that '*scientific research'* in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice.

When consent is the legal basis for conducting research in accordance with the GDPR, this consent for the use of personal data should be distinguished from other consent requirements that serve as an ethical standard or procedural obligation. An example of such a procedural obligation, where the processing is based not on consent but on another legal basis, is to be found in the Clinical Trials Regulation. In the context of data protection law, the latter form of consent could be considered as an additional safeguard.[68] At the same time, the GDPR does not restrict the application of Article 6 to consent alone, with regard to processing data for research purposes. As long as appropriate safeguards are in place, such as the requirements under Article 89(1), and the processing is fair, lawful, transparent and accords with data minimisation standards and individual rights, other lawful bases such as Article 6(1)(e) or (f) may be available.[69] This also applies to special categories of data pursuant to the derogation of Article 9(2)(j).[70]

Recital 33 seems to bring some flexibility to the degree of specification and granularity of consent in the context of scientific research. Recital 33 states: "*It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose*."

First, it should be noted that Recital 33 does not disapply the obligations with regard to the requirement of specific consent. This means that, in principle, scientific research projects can only include personal data on the basis of consent if they have a well-described purpose. For the cases where purposes for data processing within a scientific research project cannot be specified at the outset, Recital 33 allows as an exception that the purpose may be described at a more general level.

Considering the strict conditions stated by Article 9 GDPR regarding the processing of special categories of data, WP29 notes that when special categories of data are processed on the basis of explicit consent, applying the flexible approach of Recital 33 will be subject to a stricter interpretation and requires a high degree of scrutiny.

When regarded as a whole, the GDPR cannot be interpreted to allow for a controller to navigate around the key principle of specifying purposes for which consent of the data subject is asked.

---

[68] See also Recital 161 of the GDPR.

[69] Article 6(1)(c) may also be applicable for parts of the processing operations specifically required by law, such as gathering reliable and robust data following the protocol as approved by the Member State under the Clinical Trial Regulation.

[70] Specific testing of medicinal products may take place on the basis of an EU or national law pursuant to Article 9(2)(i).

When research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset. As the research advances, consent for subsequent steps in the project can be obtained before that next stage begins. Yet, such a consent should still be in line with the applicable ethical standards for scientific research.

Moreover, the controller may apply further safeguards in such cases. Article 89(1), for example, highlights the need for safeguards in data processing activities for scientific or historical or statistical purposes. These purposes "*shall be subject to appropriate safeguards, in accordance with this regulation, for the rights and freedoms of data subject*." Data minimization, anonymisation and data security are mentioned as possible safeguards.[71] Anonymisation is the preferred solution as soon as the purpose of the research can be achieved without the processing of personal data.

Transparency is an additional safeguard when the circumstances of the research do not allow for a specific consent. A lack of purpose specification may be offset by information on the development of the purpose being provided regularly by controllers as the research project progresses so that, over time, the consent will be as specific as possible. When doing so, the data subject has at least a basic understanding of the state of play, allowing him/her to assess whether or not to use, for example, the right to withdraw consent pursuant to Article 7(3).[72]

Also, having a comprehensive research plan available for data subjects to take note of, before they consent could help to compensate a lack of purpose specification.[73] This research plan should specify the research questions and working methods envisaged as clearly as possible. The research plan could also contribute to compliance with Article 7(1), as controllers need to show what information was available to data subjects at the time of consent in order to be able to demonstrate that consent is valid.

It is important to recall that where consent is being used as the lawful basis for processing there must be a possibility for a data subject to withdraw that consent. WP29 notes that withdrawal of consent could undermine types scientific research that require data that can be linked to individuals, however the GDPR is clear that consent can be withdrawn and controllers must act upon this – there

[71] See for example Recital 156. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials, see Recital 156, mentioning Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use. See also WP29 Opinion 15/2011 on the definition of consent (WP 187), p. 7: "*Moreover, obtaining consent does not negate the controller's obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality. For instance, even if the processing of personal data is based on the consent of the user, this would not legitimise the collection of data which is excessive in relation to a particular purpose.*" *[…] As a principle, consent should not be seen as an exemption from the other data protection principles, but as a safeguard. It is primarily a ground for lawfulness, and it does not waive the application of other principles."*

[72] Other transparency measures may also be relevant. When controllers engage in data processing for scientific purposes, while full information cannot be provided at the outset, they could designate a specific contact person for data subjects to address with questions.

[73] Such a possibility can be found in Article 14(1) of the current Personal Data Act of Finland (*Henkilötietolaki*, 523/1999)

is no exemption to this requirement for scientific research. If a controller receives a withdrawal request, it must in principle delete the personal data straight away if it wishes to continue to use the data for the purposes of the research.[74]

7.3. Data subject's rights

If a data processing activity is based on a data subject's consent, this will affect that individual's rights. Data subjects may have the right to data portability (Article 20) when processing is based on consent. At the same time, the right to object (Article 21) does not apply when processing is based on consent, although the right to withdraw consent at any time may provide a similar outcome.

Articles 16 to 20 of the GDPR indicate that (when data processing is based on consent), data subjects have the right to erasure when consent has been withdrawn and the rights to restriction, rectification and access.[75]

8. Consent obtained under Directive 95/46/EC

Controllers that currently process data on the basis of consent in compliance with national data protection law are not automatically required to completely refresh all existing consent relations with data subjects in preparation for the GDPR. Consent which has been obtained to date continues to be valid in so far as it is in line with the conditions laid down in the GDPR.

It is important for controllers to review current work processes and records in detail, before 25 May 2018, to be sure existing consents meet the GDPR standard (see Recital 171 of the GDPR[76]). In practice, the GDPR raises the bar with regard to implementing consent mechanisms and introduces several new requirements that require controllers to alter consent mechanisms, rather than rewriting privacy policies alone.[77]

For example, as the GDPR requires that a controller must be able to demonstrate that valid consent was obtained, all presumed consents of which no references are kept will automatically be below the consent standard of the GDPR and will need to be renewed. Likewise as the GDPR requires a "statement or a clear affirmative action", all presumed consents that were based on a more implied form of action by the data subject (e.g. a pre-ticked opt-in box) will also not be apt to the GDPR standard of consent.

---

[74] See also WP29 Opinion 05/2014 on "Anonymisation Techniques" (WP216).

[75] In cases where certain data processing activities are restricted in accordance with Article 18, GDPR, consent of the data subject may be needed to lift restrictions.

[76] Recital 171 GDPR states: "*Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.*"

[77] As indicated in the introduction, the GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent. Many of the new requirements build upon Opinion 15/2011 on consent.

Furthermore, to be able to demonstrate that consent was obtained or to allow for more granular indications of the data subject's wishes, operations and IT systems may need revision. Also, mechanisms for data subjects to withdraw their consent easily must be available and information about how to withdraw consent must be provided. If existing procedures for obtaining and managing consent do not meet the GDPR's standards, controllers will need to obtain fresh GDPR-compliant consent.

On the other hand, as not all elements named in Articles 13 and 14 must always be present as a condition for informed consent, the extended information obligations under the GDPR do not necessarily oppose the continuity of consent which has been granted before the GDPR enters into force (see page 15 above). Under Directive 95/46/EC, there was no requirement to inform data subjects of the basis upon which the processing was being conducted.

If a controller finds that the consent previously obtained under the old legislation will not meet the standard of GDPR consent, then controllers must undertake action to comply with these standards, for example by refreshing consent in a GDPR-compliant way. Under the GDPR, it is not possible to swap between one lawful basis and another. If a controller is unable to renew consent in a compliant way and is also unable –as a one off situation- to make the transition to GDPR compliance by basing data processing on a different lawful basis while ensuring that continued processing is fair and accounted for, the processing activities must be stopped. In any event the controller needs to observe the principles of lawful, fair and transparent processing.

-*-*-*-*-*-*-*-*-*-*-*-* END OF DOCUMENT *-*

17/EN

WP260 rev.01

Article 29 Working Party

Guidelines on transparency under Regulation 2016/679

Adopted on 29 November 2017

As last Revised and Adopted on 11 April 2018

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

Table of Contents

Introduction

1. These guidelines provide practical guidance and interpretative assistance from the Article 29 Working Party (WP29) on the new obligation of transparency concerning the processing of personal data under the General Data Protection Regulation[1] (the "**GDPR**"). Transparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights[2]. Insofar as compliance with transparency is required in relation to data processing under Directive (EU) 2016/680[3], these guidelines also apply to the interpretation of that principle.[4] These guidelines are, like all WP29 guidelines, intended to be generally applicable and relevant to controllers irrespective of the sectoral, industry or regulatory specifications particular to any given data controller. As such, these guidelines cannot address the nuances and many variables which may arise in the context of the transparency obligations of a specific sector, industry or regulated area. However, these guidelines are intended to enable controllers to understand, at a high level, WP29's interpretation of what the transparency obligations entail in practice and to indicate the approach which WP29 considers controllers should take to being transparent while embedding fairness and accountability into their transparency measures.

2. Transparency is a long established feature of the law of the EU[5]. It is about engendering trust in the processes which affect the citizen by enabling them to understand, and if necessary, challenge those processes. It is also an expression of the principle of fairness in relation to the

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[2] These guidelines set out general principles in relation to the exercise of data subjects' rights rather than considering specific modalities for each of the individual data subject rights under the GDPR.

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[4] While transparency is not one of the principles relating to processing of personal data set out in Article 4 of Directive (EU) 2016/680, Recital 26 states that any processing of personal data must be "lawful, fair and transparent" in relation to the natural persons concerned.

[5] Article 1 of the TEU refers to decisions being taken "*as openly as possible and as close to the citizen as possible*"; Article 11(2) states that "*The institutions shall maintain an open, transparent and regular dialogue with representative associations and civil society";* and Article 15 of the TFEU refers amongst other things to citizens of the Union having a right of access to documents of Union institutions, bodies, offices and agencies and the requirements of those Union institutions, bodies, offices and agencies to ensure that their proceedings are transparent.

processing of personal data expressed in Article 8 of the Charter of Fundamental Rights of the European Union. Under the GDPR (Article 5(1)(a)[6]), in addition to the requirements that data must be processed lawfully and fairly, transparency is now included as a fundamental aspect of these principles.[7] Transparency is intrinsically linked to fairness and the new principle of accountability under the GDPR. It also follows from Article 5.2 that the controller must always be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject.[8] Connected to this, the accountability principle requires transparency of processing operations in order that data controllers are able to demonstrate compliance with their obligations under the GDPR[9].

3. In accordance with Recital 171 of the GDPR, where processing is already under way prior to 25 May 2018, a data controller should ensure that it is compliant with its transparency obligations as of 25 May 2018 (along with all other obligations under the GDPR). This means that prior to 25 May 2018, data controllers should revisit all information provided to data subjects on processing of their personal data (for example in privacy statements/ notices etc.) to ensure that they adhere to the requirements in relation to transparency which are discussed in these guidelines. Where changes or additions are made to such information, controllers should make it clear to data subjects that these changes have been effected in order to comply with the GDPR. WP29 recommends that such changes or additions be actively brought to the attention of data subjects but at a minimum controllers should make this information publically available (e.g. on their website). However, if the changes or additions are material or substantive, then in line with paragraphs 29 to 32 below, such changes should be actively brought to the attention of the data subject.

4. Transparency, when adhered to by data controllers, empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights[10]. The concept of transparency in the GDPR is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles. The practical (information) requirements are outlined in Articles 12 - 14 of the GDPR. However, the quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information, which must be provided to data subjects.

---

[6] "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject".

[7] In Directive 95/46/EC, transparency was only alluded to in Recital 38 by way of a requirement for processing of data to be fair, but not expressly referenced in the equivalent Article 6(1)(a).

[8] Article 5.2 of the GDPR obliges a data controller to demonstrate transparency (together with the five other principles relating to data processing set out in Article 5.1) under the principle of accountability.

[9] The obligation upon data controllers to implement technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR is set out in Article 24.1.

[10] See, for example, the Opinion of Advocate General Cruz Villalon (9 July 2015) in the Bara case (Case C-201/14) at paragraph 74: *"the requirement to inform the data subjects about the processing of their personal data, which guarantees transparency of all processing, is all the more important since it affects the exercise by the data subjects of their right of access to the data being processed, referred to in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive".*

5. The transparency requirements in the GDPR apply irrespective of the legal basis for processing and throughout the life cycle of processing. This is clear from Article 12 which provides that transparency applies at the following stages of the data processing cycle:

- before or at the start of the data processing cycle, i.e. when the personal data is being collected either from the data subject or otherwise obtained;
- throughout the whole processing period, i.e. when communicating with data subjects about their rights; and
- at specific points while processing is ongoing, for example when data breaches occur or in the case of material changes to the processing.

The meaning of transparency

6. Transparency is not defined in the GDPR. Recital 39 of the GDPR is informative as to the meaning and effect of the principle of transparency in the context of data processing:

> *"It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed…"*

Elements of transparency under the GDPR

7. The key articles in relation to transparency in the GDPR, as they apply to the rights of the data subject, are found in Chapter III (Rights of the Data Subject). Article 12 sets out the general rules which apply to: the provision of information to data subjects (under Articles 13 - 14); communications with data subjects concerning the exercise of their rights (under Articles 15 - 22); and communications in relation to data breaches (Article 34). In particular Article 12 requires that the information or communication in question must comply with the following rules:

- it must be concise, transparent, intelligible and easily accessible (Article 12.1);
- clear and plain language must be used (Article 12.1);
- the requirement for clear and plain language is of particular importance when providing information to children (Article 12.1);
- it must be in writing *"or by other means, including where appropriate, by electronic means"* (Article 12.1);
- where requested by the data subject it may be provided orally (Article 12.1) ; and

- it generally must be provided free of charge (Article 12.5).

"*Concise, transparent, intelligible and easily accessible"*

8. The requirement that the provision of information to, and communication with, data subjects is done in a "concise and transparent" manner means that data controllers should present the information/ communication efficiently and succinctly in order to avoid information fatigue. This information should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use. In an online context, the use of a layered privacy statement/ notice will enable a data subject to navigate to the particular section of the privacy statement/ notice which they want to immediately access rather than having to scroll through large amounts of text searching for particular issues.

9. The requirement that information is "intelligible" means that it should be understood by an average member of the intended audience. Intelligibility is closely linked to the requirement to use clear and plain language. An accountable data controller will have knowledge about the people they collect information about and it can use this knowledge to determine what that audience would likely understand. For example, a controller collecting the personal data of working professionals can assume its audience has a higher level of understanding than a controller that obtains the personal data of children. If controllers are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/ notices/ policies etc., they can test these, for example, through mechanisms such as user panels, readability testing, formal and informal interactions and dialogue with industry groups, consumer advocacy groups and regulatory bodies, where appropriate, amongst other things.

10. A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used. This is also an important aspect of the principle of fairness under Article 5.1 of the GDPR and indeed is linked to Recital 39 which states that *"[n]atural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data…"* In particular, for complex, technical or unexpected data processing, WP29's position is that, as well as providing the prescribed information under Articles 13 and 14 (dealt with later in these guidelines), controllers should also separately spell out in unambiguous language what the most important *consequences* of the processing will be: in other words, what kind of effect will the specific processing described in a privacy statement/ notice actually have on a data subject? In accordance with the principle of accountability and in line with Recital 39, data controllers should assess whether there are particular risks for natural persons involved in this type of processing which should be brought to the attention of data subjects. This can help to provide an overview of the types of processing that could have the highest impact on the fundamental rights and freedoms of data subjects in relation to the protection of their personal data.

11. The "easily accessible" element means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question (for example in an online layered privacy statement/ notice, in FAQs, by way of contextual pop-ups which activate when a data subject fills in an online form, or in an interactive digital context through a chatbot interface, etc. These mechanisms are further considered below, including at paragraphs 33 to 40).

Example

Every organisation that maintains a website should publish a privacy statement/ notice on the website. A direct link to this privacy statement/ notice should be clearly visible on each page of this website under a commonly used term (such as "Privacy", "Privacy Policy" or "Data Protection Notice"). Positioning or colour schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible.

For apps, the necessary information should also be made available from an online store prior to download. Once the app is installed, the information still needs to be easily accessible from within the app. One way to meet this requirement is to ensure that the information is never more than "two taps away" (e.g. by including a "Privacy"/ "Data Protection" option in the menu functionality of the app). Additionally, the privacy information in question should be specific to the particular app and should not merely be the generic privacy policy of the company that owns the app or makes it available to the public.

WP29 recommends as a best practice that at the point of collection of the personal data in an online context a link to the privacy statement/ notice is provided or that this information is made available on the same page on which the personal data is collected.

"*Clear and plain language*"

12. With *written* information (and where written information is delivered orally, or by audio/ audiovisual methods, including for vision-impaired data subjects), best practices for clear writing should be followed.[11] A similar language requirement (for "plain, intelligible language") has previously been used by the EU legislator[12] and is also explicitly referred to in the context of consent in Recital 42 of the GDPR[13]. The requirement for clear and plain language means that information should be provided in as simple a manner as possible, avoiding complex sentence and language structures. The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different

[11] See How to Write Clearly by the European Commission (2011), to be found at: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5.

[12] Article 5 of Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts

[13] Recital 42 states that a declaration of consent pre-formulated by a data controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.

interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear.

Poor Practice Examples

The following phrases are not sufficiently clear as to the purposes of processing:

- "*We may use your personal data to develop new services"* (as it is unclear what the "services" are or how the data will help develop them);
- "*We may use your personal data for research purposes* (as it is unclear what kind of "research" this refers to); and
- "*We may use your personal data to offer personalised services"* (as it is unclear what the "personalisation" entails).

Good Practice Examples[14]

- *"We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in "* (it is clear that what types of data will be processed, that the data subject will be subject to targeted advertisements for products and that their data will be used to enable this);
- *"We will retain and evaluate information on your recent visits to our website and how you move around different sections of our website for analytics purposes to understand how people use our website so that we can make it more intuitive"* (it is clear what type of data will be processed and the type of analysis which the controller is going to undertake); and
- "*We will keep a record of the articles on our website that you have clicked on and use that information to target advertising on this website to you that is relevant to your interests, which we have identified based on articles you have read"* (it is clear what the personalisation entails and how the interests attributed to the data subject have been identified).

13. Language qualifiers such as "may", "might", "some", "often" and "possible" should also be avoided. Where data controllers opt to use indefinite language, they should be able, in accordance with the principle of accountability, to demonstrate why the use of such language could not be avoided and how it does not undermine the fairness of processing. Paragraphs and sentences should be well structured, utilising bullets and indents to signal hierarchical

[14] The requirement for transparency exists entirely independently of the requirement upon data controllers to ensure that there is an appropriate legal basis for the processing under Article 6.

relationships. Writing should be in the active instead of the passive form and excess nouns should be avoided. The information provided to a data subject should not contain overly legalistic, technical or specialist language or terminology. Where the information is translated into one or more other languages, the data controller should ensure that all the translations are accurate and that the phraseology and syntax makes sense in the second language(s) so that the translated text does not have to be deciphered or re-interpreted. (A translation in one or more other languages should be provided where the controller targets[15] data subjects speaking those languages.)

Providing information to children and other vulnerable people

14. Where a data controller is targeting children[16] or is, or should be, aware that their goods/ services are particularly utilised by children (including where the controller is relying on the consent of the child)[17], it should ensure that the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognises that the message/ information is being directed at them.[18] A useful example of child-centred language used as an alternative to the original legal language can be found in the "UN Convention on the Rights of the Child in Child Friendly Language".[19]

15. WP29's position is that transparency is a free-standing right which applies as much to children as it does to adults. WP29 emphasises in particular that children do not lose their rights as data subjects to transparency simply because consent has been given/ authorised by the holder of parental responsibility in a situation to which Article 8 of the GDPR applies. While such consent will, in many cases, be given or authorised on a once-off basis by the holder of parental responsibility, a child (like any other data subject) has an ongoing right to transparency throughout the continuum of their engagement with a data controller. This is consistent with Article 13 of the UN Convention on the Rights of the Child which states that a child has a right to freedom of expression which includes the right to seek, receive and impart information and ideas of all kinds.[20] It is important to point out that, while providing for consent to be given on behalf of a child when under a particular age,[21] Article 8 *does not provide* for transparency measures to be directed at the holder of parental responsibility who

[15] For example, where the controller operates a website in the language in question and/or offers specific country options and/or facilitates the payment for goods or services in the currency of a particular member state then these may be indicative of a data controller targeting data subjects of a particular member state.

[16] The term "child" is not defined under the GDPR, however WP29 recognises that, in accordance with the UN Convention on the Rights of the Child, which all EU Member States have ratified, a child is a person under the age of 18 years.

[17] i.e. children of 16 years or older (or, where in accordance with Article 8.1 of the GDPR Member State national law has set the age of consent at a specific age between 13 and 16 years for children to consent to an offer for the provision of information society services, children who meet that national age of consent).

[18] Recital 38 states that "Children merit special protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data". Recital 58 states that "Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand".

[19] https://www.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf

[20] Article 13 of the UN Convention on the Rights of the Child states that: "The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice."

[21] See footnote 17 above.

gives such consent. Therefore, data controllers have an obligation in accordance with the specific mentions of transparency measures addressed to children in Article 12.1 (supported by Recitals 38 and 58) to ensure that where they target children or are aware that their goods or services are particularly utilised by children of a literate age, that any information and communication should be conveyed in clear and plain language or in a medium that children can easily understand. For the avoidance of doubt however, WP29 recognises that with very young or pre-literate children, transparency measures may also be addressed to holders of parental responsibility given that such children will, in most cases, be unlikely to understand even the most basic written or non-written messages concerning transparency.

16. Equally, if a data controller is aware that their goods/ services are availed of by (or targeted at) other vulnerable members of society, including people with disabilities or people who may have difficulties accessing information, the vulnerabilities of such data subjects should be taken into account by the data controller in its assessment of how to ensure that it complies with its transparency obligations in relation to such data subjects.[22] This relates to the need for a data controller to assess its audience's likely level of understanding, as discussed above at paragraph 9.

"In writing or by other means"

17. Under Article 12.1, the default position for the provision of information to, or communications with, data subjects is that the information is in writing.[23] (Article 12.7 also provides for information to be provided in combination with standardised icons and this issue is considered in the section on visualisation tools at paragraphs 49 to 53). However, the GDPR also allows for other, unspecified "means" including electronic means to be used. WP29's position with regard to written electronic means is that where a data controller maintains (or operates, in part or in full, through) a website, WP29 recommends the use of layered privacy statements/ notices, which allow website visitors to navigate to particular aspects of the relevant privacy statement/ notice that are of most interest to them (see more on layered privacy statements/ notices at paragraph 35 to 37).[24] However, the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (whether in a digital or paper format) which can be easily accessed by a data subject should they wish to consult the entirety of the information addressed to them. Importantly, the use of a layered approach is not confined only to written electronic means for providing information to data subjects. As discussed at paragraphs 35 to 36 and 38 below, a layered approach to the provision of information to data subjects may also be utilised by employing a combination of *methods* to ensure transparency in relation to processing.

[22] For example, the UN Convention on the Rights of Persons with Disabilities requires that appropriate forms of assistance and support are provided to persons with disabilities to ensure their access to information.

[23] Article 12.1 refers to "language" and states that the information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

[24] The WP29's recognition of the benefits of layered notices has already been noted in Opinion 10/2004 on More Harmonised Information Provisions and Opinion 02/2013 on apps on smart devices.

18. Of course, the use of digital layered privacy statements/ notices is not the only written electronic means that can be deployed by controllers. Other electronic means include "just-in-time" contextual pop-up notices, 3D touch or hover-over notices, and privacy dashboards. Non-written electronic means which may be used *in addition* to a layered privacy statement/ notice might include videos and smartphone or IoT voice alerts.[25] "Other means", which are not necessarily electronic, might include, for example, cartoons, infographics or flowcharts. Where transparency information is directed at children specifically, controllers should consider what types of measures may be particularly accessible to children (e.g. these might be comics/ cartoons, pictograms, animations, etc. amongst other measures).

19. It is critical that the method(s) chosen to provide the information is/are appropriate to the particular circumstances, i.e. the manner in which the data controller and data subject interact or the manner in which the data subject's information is collected. For example, only providing the information in electronic written format, such as in an online privacy statement/ notice may not be appropriate/ workable where a device that captures personal data does not have a screen (e.g. IoT devices/ smart devices) to access the website/ display such written information. In such cases, appropriate alternative *additional* means should be considered, for example providing the privacy statement/ notice in hard copy instruction manuals or providing the URL website address (i.e. the specific page on the website) at which the online privacy statement/ notice can be found in the hard copy instructions or in the packaging. Audio (oral) delivery of the information could also be additionally provided if the screenless device has audio capabilities. WP29 has previously made recommendations around transparency and provision of information to data subjects in its Opinion on Recent Developments in the Internet of Things[26] (such as the use of QR codes printed on internet of things objects, so that when scanned, the QR code will display the required transparency information). These recommendations remain applicable under the GDPR.

"*..the information may be provided orally"*

20. Article 12.1 specifically contemplates that information may be provided orally to a data subject on request, provided that their identity is proven by other means. In other words, the means employed should be more than reliance on a mere assertion by the individual that they are a specific named person and the means should enable the controller to verify a data subject's identity with sufficient assurance. The requirement to verify the identity of the data subject before providing information orally only applies to information relating to the exercise by a specific data subject of their rights under Articles 15 to 22 and 34. This precondition to the provision of oral information cannot apply to the provision of general privacy information as outlined in Articles 13 and 14, since information required under Articles 13 and 14 must also be made accessible to *future* users/ customers (whose identity a data controller would not be in a position to verify). Hence, information to be provided under

[25] These examples of electronic means are indicative only and data controllers may develop new innovative methods to comply with Article 12.

[26] WP29 Opinion 8/2014 adopted on 16 September 2014

Articles 13 and 14 may be provided by oral means without the controller requiring a data subject's identity to be proven.

21. The oral provision of information required under Articles 13 and 14 does not necessarily mean oral information provided on a person-to-person basis (i.e. in person or by telephone). Automated oral information may be provided in addition to written means. For example, this may apply in the context of persons who are visually impaired when interacting with information society service providers, or in the context of screenless smart devices, as referred to above at paragraph 19. Where a data controller has chosen to provide information to a data subject orally, or a data subject requests the provision of oral information or communications, WP29's position is that the data controller should allow the data subject to re-listen to pre-recorded messages. This is imperative where the request for oral information relates to visually impaired data subjects or other data subjects who may have difficulty in accessing or understanding information in written format. The data controller should also ensure that it has a record of, and can demonstrate (for the purposes of complying with the accountability requirement): (i) the request for the information by oral means, (ii) the method by which the data subject's identity was verified (where applicable – see above at paragraph 20) and (iii) the fact that information was provided to the data subject.

"Free of charge"

22. Under Article 12.5,[27] data controllers cannot generally charge data subjects for the provision of information under Articles 13 and 14, or for communications and actions taken under Articles 15 - 22 (on the rights of data subjects) and Article 34 (communication of personal data breaches to data subjects).[28] This aspect of transparency also means that any information provided under the transparency requirements cannot be made conditional upon financial transactions, for example the payment for, or purchase of, services or goods.[29]

Information to be provided to the data subject – Articles 13 & 14

Content

23. The GDPR lists the categories of information that must be provided to a data subject in relation to the processing of their personal data where it is collected from the data subject (Article 13) or obtained from another source (Article 14). The **table in the Annex** to these

[27] This states that "Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge."

[28] However, under Article 12.5 the controller may charge a reasonable fee where, for example, a request by a data subject in relation to the information under Article 13 and 14 or the rights under Articles 15 - 22 or Article 34 is excessive or manifestly unfounded. (Separately, in relation to the right of access under Article 15.3 a controller may charge a reasonable fee based on administrative costs for any further copy of the personal data which is requested by a data subject).

[29] By way of illustration, if a data subject's personal data is being collected in connection with a purchase, the information which is required to be provided under Article 13 should be provided prior to payment being made and at the point at which the information is being collected, rather than after the transaction has been concluded. Equally though, where free services are being provided to the data subject, the Article 13 information must be provided prior to, rather than after, sign-up given that Article 13.1 requires the provision of the information "at the time when the personal data are obtained".

guidelines summarises the categories of information that must be provided under Articles 13 and 14. It also considers the nature, scope and content of these requirements. For clarity, WP29's position is that there is no difference between the status of the information to be provided under sub-article 1 and 2 of Articles 13 and 14 respectively. All of the information across these sub-articles is of equal importance and must be provided to the data subject.

"Appropriate measures"

24. As well as content, the form and manner in which the information required under Articles 13 and 14 should be provided to the data subject is also important. The notice containing such information is frequently referred to as a data protection notice, privacy notice, privacy policy, privacy statement or fair processing notice. The GDPR does not prescribe the format or modality by which such information should be provided to the data subject but does make it clear that it is the data controller's responsibility to take "appropriate measures" in relation to the provision of the required information for transparency purposes. This means that the data controller should take into account all of the circumstances of the data collection and processing when deciding upon the appropriate modality and format of the information provision. In particular, appropriate measures will need to be assessed in light of the product/ service user experience. This means taking account of the device used (if applicable), the nature of the user interfaces/ interactions with the data controller (the user "journey") and the limitations that those factors entail. As noted above at paragraph 17, WP29 recommends that where a data controller has an online presence, an online layered privacy statement/ notice should be provided.

25. In order to help identify the most appropriate modality for providing the information, in advance of "going live", data controllers may wish to trial different modalities by way of user testing (e.g. hall tests, or other standardised tests of readability or accessibility) to seek feedback on how accessible, understandable and easy to use the proposed measure is for users. (See also further comments above on other mechanisms for carrying out user testing at paragraph 9). Documenting this approach should also assist data controllers with their accountability obligations by demonstrating how the tool/ approach chosen to convey the information is the most appropriate in the circumstances.

Timing for provision of information

26. Articles 13 and 14 set out information which must be provided to the data subject at the commencement phase of the processing cycle[30]. Article 13 applies to the scenario where the data is collected from the data subject. This includes personal data that:

[30] Pursuant to the principles of fairness and purpose limitation, the organisation which collects the personal data from the data subject should always specify the purposes of the processing at the time of collection. If the purpose includes the creation of inferred personal data, the intended purpose of creating and further processing such inferred personal data, as well as the categories of the inferred data processed, must always be communicated to the data subject at the time of collection, or prior to the further processing for a new purpose in compliance with Article 13.3 or Article 14.4.

- a data subject consciously provides to a data controller (e.g. when completing an online form); or
- a data controller collects from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras, network equipment, Wi-Fi tracking, RFID or other types of sensors).

Article 14 applies in the scenario where the data have not been obtained from the data subject. This includes personal data which a data controller has obtained from sources such as:

- third party data controllers;
- publicly available sources;
- data brokers; or
- other data subjects.

27. As regards timing of the provision of this information, providing it in a timely manner is a vital element of the transparency obligation and the obligation to process data fairly. Where Article 13 applies, under Article 13.1 the information must be provided *"at the time when personal data are obtained".* In the case of indirectly obtained personal data under Article 14, the timeframes within which the required information must be provided to the data subject are set out in Article 14.3 (a) to (c) as follows:

- The general requirement is that the information must be provided within a "reasonable period" after obtaining the personal data and no later than one month, *"having regard to the specific circumstances in which the personal data are processed"* (Article 14.3(a)).

- The general one-month time limit in Article 14.3(a) may be further curtailed under Article 14.3(b),[31] which provides for a situation where the data are being used for communication with the data subject. In such a case, the information must be provided at the latest at the time of the first communication with the data subject. If the first communication occurs prior to the one-month time limit after obtaining the personal data, then the information must be provided *at the latest* at the time of the first communication with the data subject notwithstanding that one month from the point of obtaining the data has not expired. If the first communication with a data subject occurs more than one month after obtaining the personal data then Article 14.3(a) continues to apply, so that the Article 14 information must be provided to the data subject at the latest within one month after it was obtained.

[31] The use of the words *"if the personal data are to be used for.."* in Article 14.3(b) indicates a specification to the general position with regard to the maximum time limit set out in Article 14.3(a) but does not replace it.

- The general one-month time limit in Article 14.3(a) can also be curtailed under Article 14.3(c)[32] which provides for a situation where the data are being disclosed to another recipient (whether a third party or not)[33]. In such a case, the information must be provided at the latest at the time of the first disclosure. In this scenario, if the disclosure occurs prior to the one-month time limit, then the information must be provided *at the latest* at the time of that first disclosure, notwithstanding that one month from the point of obtaining the data has not expired. Similar to the position with Article 14.3(b), if any disclosure of the personal data occurs more than one month after obtaining the personal data, then Article 14.3(a) again continues to apply, so that the Article 14 information must be provided to the data subject at the latest within one month after it was obtained.

28. Therefore, in any case, the maximum time limit within which Article 14 information must be provided to a data subject is one month. However, the principles of fairness and accountability under the GDPR require data controllers to always consider the reasonable expectations of data subjects, the effect that the processing may have on them and their ability to exercise their rights in relation to that processing, when deciding at what point to provide the Article 14 information. Accountability requires controllers to demonstrate the rationale for their decision and justify why the information was provided at the time it was. In practice, it may be difficult to meet these requirements when providing information at the 'last moment'. In this regard, Recital 39 stipulates, amongst other things, that data subjects should be *"made aware of the risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing".* Recital 60 also refers to the requirement that the data subject be informed of the existence of the processing operation and its purposes in the context of the principles of fair and transparent processing. For all of these reasons, WP29's position is that, wherever possible, data controllers should, in accordance with the principle of fairness, provide the information to data subjects well in advance of the stipulated time limits. Further comments on the appropriateness of the timeframe between notifying data subjects of the processing operations and such processing operations actually taking effect are set out in paragraphs 30 to 31 and 48.

Changes to Article 13 and Article 14 information

29. Being accountable as regards transparency applies not only at the point of collection of personal data but throughout the processing life cycle, irrespective of the information or communication being conveyed. This is the case, for example, when changing the contents of existing privacy statements/ notices. The controller should adhere to the same principles when communicating both the initial privacy statement/ notice and any subsequent substantive or material changes to this statement/ notice. Factors which controllers should consider in assessing what is a substantive or material change include the impact on data subjects (including their ability to exercise their rights), and how unexpected/ surprising the

[32] The use of the words *"if a disclosure to anther recipient is envisaged…"* in Article 14.3(c) likewise indicates a specification to the general position with regard to the maximum time limit set out in Article 14.3(a) but does not replace it.

[33] Article 4.9 defines "recipient" and clarifies that a recipient to whom personal data are disclosed does not have to be a third party. Therefore, a recipient may be a data controller, joint controller or processor.

change would be to data subjects. Changes to a privacy statement/ notice that should always be communicated to data subjects include inter alia: a change in processing purpose; a change to the identity of the controller; or a change as to how data subjects can exercise their rights in relation to the processing. Conversely, an example of changes to a privacy statement/ notice which are not considered by WP29 to be substantive or material include corrections of misspellings, or stylistic/ grammatical flaws. Since most existing customers or users will only glance over communications of changes to privacy statements/ notices, the controller should take all measures necessary to ensure that these changes are communicated in such a way that ensures that most recipients will actually notice them. This means, for example, that a notification of changes should always be communicated by way of an appropriate modality (e.g. email, hard copy letter, pop-up on a webpage or other modality which will effectively bring the changes to the attention of the data subject) specifically devoted to those changes (e.g. not together with direct marketing content), with such a communication meeting the Article 12 requirements of being concise, transparent, intelligible, easily accessible and using clear and plain language. References in the privacy statement/ notice to the effect that the data subject should regularly check the privacy statement/notice for changes or updates are considered not only insufficient but also unfair in the context of Article 5.1(a). Further guidance in relation to the timing for notification of changes to data subjects is considered below at paragraph 30 to 31.

Timing of notification of changes to Article 13 and Article 14 information

30. The GDPR is silent on the timing requirements (and indeed the methods) that apply for notifications of changes to information that has previously been provided to a data subject under Article 13 or 14 (excluding an intended further purpose for processing, in which case information on that further purpose must be notified prior to the commencement of that further processing as per Articles 13.3 and 14.4 – see below at paragraph 45). However, as noted above in the context of the timing for the provision of Article 14 information, the data controller must again have regard to the fairness and accountability principles in terms of any reasonable expectations of the data subject, or the potential impact of those changes upon the data subject. If the change to the information is indicative of a fundamental change to the nature of the processing (e.g. enlargement of the categories of recipients or introduction of transfers to a third country) or a change which may not be fundamental in terms of the processing operation but which may be relevant to and impact upon the data subject, then that information should be provided to the data subject well in advance of the change actually taking effect and the method used to bring the changes to the data subject's attention should be explicit and effective. This is to ensure the data subject does not "miss" the change and to allow the data subject a reasonable timeframe for them to (a) consider the nature and impact of the change and (b) exercise their rights under the GDPR in relation to the change (e.g. to withdraw consent or to object to the processing).

31. Data controllers should carefully consider the circumstances and context of each situation where an update to transparency information is required, including the potential impact of the changes upon the data subject and the modality used to communicate the changes, and be able to demonstrate how the timeframe between notification of the changes and the

change taking effect satisfies the principle of fairness to the data subject. Further, WP29's position is that, consistent with the principle of fairness, when notifying such changes to data subjects, a data controller should also explain what will be the likely impact of those changes on data subjects. However, compliance with transparency requirements does not "whitewash" a situation where the changes to the processing are so significant that the processing becomes completely different in nature to what it was before. WP29 emphasises that all of the other rules in the GDPR, including those relating to incompatible further processing, continue to apply irrespective of compliance with the transparency obligations.

32. Additionally, even when transparency information (e.g. contained in a privacy statement/ notice) does not materially change, it is likely that data subjects who have been using a service for a significant period of time will not recall the information provided to them at the outset under Articles 13 and/or 14. WP29 recommends that controllers facilitate data subjects to have continuing easy access to the information to re-acquaint themselves with the scope of the data processing. In accordance with the accountability principle, controllers should also consider whether, and at what intervals, it is appropriate for them to provide express reminders to data subjects as to the fact of the privacy statement/ notice and where they can find it.

Modalities - format of information provision

33. Both Articles 13 and 14 refer to the obligation on the data controller to *"provide the data subject with all of the following information…"* The operative word here is "provide". This means that the data controller must take active steps to furnish the information in question to the data subject or to actively direct the data subject to the location of it (e.g. by way of a direct link, use of a QR code, etc.). The data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app. The example at paragraph 11 illustrates this point. As noted above at paragraph 17, WP29 recommends that the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (e.g. whether in a digital form on a website or in paper format) which can be easily accessed should they wish to consult the entirety of the information.

34. There is an inherent tension in the GDPR between the requirements on the one hand to provide the comprehensive information to data subjects which is required under the GDPR, and on the other hand do so in a form that is concise, transparent, intelligible and easily accessible. As such, and bearing in mind the fundamental principles of accountability and fairness, controllers must undertake their own analysis of the nature, circumstances, scope and context of the processing of personal data which they carry out and decide, within the legal requirements of the GDPR and taking account of the recommendations in these Guidelines particularly at paragraph 36 below, how to prioritise information which must be provided to data subjects and what are the appropriate levels of detail and methods for conveying the information.

Layered approach in a digital environment and layered privacy statements/ notices

35. In the digital context, in light of the volume of information which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency. WP29 recommends in particular that layered privacy statements/ notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on the screen, in order to avoid information fatigue. Layered privacy statements/ notices can help resolve the tension between completeness and understanding, notably by allowing users to navigate directly to the section of the statement/ notice that they wish to read. It should be noted that layered privacy statements/ notices are not merely nested pages that require several clicks to get to the relevant information. The design and layout of the first layer of the privacy statement/ notice should be such that the data subject has a clear overview of the information available to them on the processing of their personal data and where/ how they can find that detailed information within the layers of the privacy statement/ notice. It is also important that the information contained within the different layers of a layered notice is consistent and that the layers do not provide conflicting information.

36. As regards the content of the first modality used by a controller to inform data subjects in a layered approach (in other words the primary way in which the controller first engages with a data subject), or the content of the first layer of a layered privacy statement/ notice, WP29 recommends that the first layer/ modality should include the details of the purposes of processing, the identity of controller and a description of the data subject's rights. (Furthermore this information should be directly brought to the attention of a data subject at the time of collection of the personal data e.g. displayed as a data subject fills in an online form.) The importance of providing this information upfront arises in particular from Recital 39.[34] While controllers must be able to demonstrate accountability as to what further information they decide to prioritise, WP29's position is that, in line with the fairness principle, in addition to the information detailed above in this paragraph, the first layer/ modality should also contain information on the processing which has the most impact on the data subject and processing which could surprise them. Therefore, the data subject should be able to understand from information contained in the first layer/ modality what the consequences of the processing in question will be for the data subject (see also above at paragraph 10).

37. In a digital context, aside from providing an online layered privacy statement/ notice, data controllers may also choose to use *additional* transparency tools (see further examples considered below) which provide tailored information to the individual data subject which is specific to the position of the individual data subject concerned and the goods/ services which that data subject is availing of. It should be noted however that while WP29 recommends the

[34] Recital 39 states, on the principle of transparency, that "That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed."

use of online layered privacy statements/ notices, this recommendation does not exclude the development and use of other innovative methods of compliance with transparency requirements.

Layered approach in a non-digital environment

38. A layered approach to the provision of transparency information to data subjects can also be deployed in an offline/ non-digital context (i.e. a real-world environment such as person-to-person engagement or telephone communications) where multiple modalities may be deployed by data controllers to facilitate the provision of information. (See also paragraphs 33 to 37 and 39 to 40 in relation to different modalities for providing the information.) This approach should not be confused with the separate issue of layered privacy statements/ notices. Whatever the formats that are used in this layered approach, WP29 recommends that the first "layer" (in other words the primary way in which the controller first engages with the data subject) should generally convey the most important information (as referred to at paragraph 36 above), namely the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impact of processing or processing which could surprise the data subject. For example, where the first point of contact with a data subject is by telephone, this information could be provided during the telephone call with the data subject and they could be provided with the balance of the information required under Article 13/ 14 by way of further, different means, such as by sending a copy of the privacy policy by email and/ or sending the data subject a link to the controller's layered online privacy statement/ notice.

"Push" and "pull" notices

39. Another possible way of providing transparency information is through the use of "push" and "pull" notices. Push notices involve the provision of "just-in-time" transparency information notices while "pull" notices facilitate access to information by methods such as permission management, privacy dashboards and "learn more" tutorials. These allow for a more user-centric transparency experience for the data subject.

- A privacy dashboard is a single point from which data subjects can view 'privacy information' and manage their privacy preferences by allowing or preventing their data from being used in certain ways by the service in question. This is particularly useful when the same service is used by data subjects on a variety of different devices as it gives them access to and control over their personal data no matter how they use the service. Allowing data subjects to manually adjust their privacy settings via a privacy dashboard can also make it easier for a privacy statement/ notice to be personalised by reflecting only the types of processing occurring for that particular data subject. Incorporating a privacy dashboard into the existing architecture of a service (e.g. by using the same design and branding as the rest of the service) is preferable because it will ensure that access and use of it will be intuitive and may help to encourage users to engage with this information, in the same way that they would with other aspects of the service. This can be an effective way of

demonstrating that 'privacy information' is a necessary and integral part of a service rather than a lengthy list of legalese.

- A just-in-time notice is used to provide specific 'privacy information' in an ad hoc manner, as and when it is most relevant for the data subject to read. This method is useful for providing information at various points throughout the process of data collection; it helps to spread the provision of information into easily digestible chunks and reduces the reliance on a single privacy statement/ notice containing information that is difficult to understand out of context. For example, if a data subject purchases a product online, brief explanatory information can be provided in pop-ups accompanying relevant fields of text. The information next to a field requesting the data subject's telephone number could explain for example that this data is only being collected for the purposes of contact regarding the purchase and that it will only be disclosed to the delivery service.

Other types of "appropriate measures"

40. Given the very high level of internet access in the EU and the fact that data subjects can go online at any time, from multiple locations and different devices, as stated above, WP29's position is that an "appropriate measure" for providing transparency information in the case of data controllers who maintain a digital/ online presence, is to do so through an electronic privacy statement/ notice. However, based on the circumstances of the data collection and processing, a data controller may need to additionally (or alternatively where the data controller does not have any digital/online presence) use other modalities and formats to provide the information. Other possible ways to convey the information to the data subject arising from the following different personal data environments may include the following modes applicable to the relevant environment which are listed below. As noted previously, a layered approach may be followed by controllers where they opt to use a combination of such methods while ensuring that the most important information (see paragraph 36 and 38) is always conveyed in the first modality used to communicate with the data subject.

a. Hard copy/ paper environment, for example when entering into contracts by postal means: written explanations, leaflets, information in contractual documentation, cartoons, infographics or flowcharts;
b. Telephonic environment: oral explanations by a real person to allow interaction and questions to be answered or automated or pre-recorded information with options to hear further more detailed information;
c. Screenless smart technology/ IoT environment such as Wi-Fi tracking analytics: icons, QR codes, voice alerts, written details incorporated into paper set-up instructions, videos incorporated into digital set-up instructions, written information on the smart device, messages sent by SMS or email, visible boards containing the information, public signage or public information campaigns;
d. Person to person environment, such as responding to opinion polls, registering in person for a service: oral explanations or written explanations provided in hard or soft copy format;

e. "Real-life" environment with CCTV/ drone recording: visible boards containing the information, public signage, public information campaigns or newspaper/ media notices.

Information on profiling and automated decision-making

41. Information on the existence of automated decision-making, including profiling, as referred to in Articles 22.1 and 22.4, together with meaningful information about the logic involved and the significant and envisaged consequences of the processing for the data subject, forms part of the obligatory information which must be provided to a data subject under Articles 13.2(f) and 14.2(g). WP29 has produced guidelines on automated individual decision-making and profiling[35] which should be referred to for further guidance on how transparency should be given effect in the particular circumstances of profiling. It should be noted that, aside from the specific transparency requirements applicable to automated decision-making under Articles 13.2(f) and 14.2(g), the comments in these guidelines relating to the importance of informing data subjects as to the consequences of processing of their personal data, and the general principle that data subjects should not be taken by surprise by the processing of their personal data, equally apply to profiling generally (not just profiling which is captured by Article 22[36]), as a type of processing.[37]

Other issues – risks, rules and safeguards

42. Recital 39 of the GDPR also refers to the provision of certain information which is not explicitly covered by Articles 13 and Article 14 (see recital text above at paragraph 28). The reference in this recital to making data subjects aware of the risks, rules and safeguards in relation to the processing of personal data is connected to a number of other issues. These include data protection impact assessments (DPIAs). As set out in the WP29 Guidelines on DPIAs,[38] data controllers may consider publication of the DPIA (or part of it), as a way of fostering trust in the processing operations and demonstrating transparency and accountability, although such publication is not obligatory. Furthermore, adherence to a code of conduct (provided for under Article 40) may go towards demonstrating transparency, as codes of conduct may be drawn up for the purpose of specifying the application of the GDPR with regard to: fair and transparent processing; information provided to the public and to data subjects; and information provided to, and the protection of, children, amongst other issues.

43. Another relevant issue relating to transparency is data protection by design and by default (as required under Article 25). These principles require data controllers to build data

[35] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251

[36] This applies to decision-making based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her.

[37] Recital 60, which is relevant here, states that "Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling".

[38] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.1

protection considerations into their processing operations and systems from the ground up, rather than taking account of data protection as a last-minute compliance issue. Recital 78 refers to data controllers implementing measures that meet the requirements of data protection by design and by default including measures consisting of transparency with regard to the functions and processing of personal data.

44. Separately, the issue of joint controllers is also related to making data subjects aware of the risks, rules and safeguards. Article 26.1 requires joint controllers to determine their respective responsibilities for complying with obligations under the GDPR in a transparent manner, in particular with regard to the exercise by data subjects of their rights and the duties to provide the information under Articles 13 and 14. Article 26.2 requires that the essence of the arrangement between the data controllers must be made available to the data subject. In other words, it must be completely clear to a data a subject as to which data controller he or she can approach where they intend to exercise one or more of their rights under the GDPR.[39]

Information related to further processing

45. Both Articles 13 and Article 14 contain a provision[40] that requires a data controller to inform a data subject if it intends to further process their personal data for a purpose other than that for which it was collected/ obtained. If so, "*the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2".* These provisions specifically give effect to the principle in Article 5.1(b) that personal data shall be collected for specified, explicit and legitimate purposes, and further processing in a manner that is *incompatible* with these purposes is prohibited.[41] The second part of Article 5.1(b) states that further processing for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes, shall, in accordance with Article 89.1, not be considered to be incompatible with the initial purposes. Where personal data are further processed for purposes that are *compatible* with the original purposes (Article 6.4 informs this issue[42]), Articles 13.3 and 14.4 apply. The requirements in these articles to inform a data subject about further processing promotes the position in the GDPR that a data subject should reasonably expect that at the time and in the context of the collection of personal data that processing

[39] Under Article 26.3, irrespective of the terms of the arrangement between joint data controllers under Article 26.1, a data subject may exercise his or her rights under the GDPR in respect of and against each of the joint data controllers.

[40] At Articles 13.3 and 14.4, which are expressed in identical terms, apart from the word "collected", which is used in Article 13, and which is replaced with the word "obtained" in Article 14.

[41] See, for example on this principle, Recitals 47, 50, 61, 156, 158; Articles 6.4 and 89

[42] Article 6.4 sets out, in non-exhaustive fashion, the factors which are to be taken into account in ascertaining whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, namely: the link between the purposes; the context in which the personal data have been collected; the nature of the personal data (in particular whether special categories of personal data or personal data relating to criminal offences and convictions are included); the possible consequences of the intended further processing for data subjects; and the existence of appropriate safeguards.

for a particular purpose may take place.[43] In other words, a data subject should not be taken by surprise at the purpose of processing of their personal data.

46. Articles 13.3 and 14.4, insofar as they refer to the provision of "*any relevant further information as referred to in paragraph 2",* may be interpreted at first glance as leaving some element of appreciation to the data controller as to the extent of and the particular categories of information from the relevant sub-paragraph 2 (i.e. Article 13.2 or 14.2 as applicable) that should be provided to the data subject. (Recital 61 refers to this as "*other necessary information*".) However the default position is that all such information set out in that sub-article should be provided to the data subject unless one or more categories of the information does not exist or is not applicable.

47. WP29 recommends that, in order to be transparent, fair and accountable, controllers should consider making information available to data subjects in their privacy statement/ notice on the compatibility analysis carried out under Article 6.4[44] where a legal basis other than consent or national/ EU law is relied on for the new processing purpose. (In other words, an explanation as to how the processing for the other purpose(s) is compatible with the original purpose). This is to allow data subjects the opportunity to consider the compatibility of the further processing and the safeguards provided and to decide whether to exercise their rights e.g. the right to restriction of processing or the right to object to processing, amongst others.[45] Where controllers choose not to include such information in a privacy notice/ statement, WP29 recommends that they make it clear to data subjects that they can obtain the information on request.

48. Connected to the exercise of data subject rights is the issue of timing. As emphasised above, the provision of information in a timely manner is a vital element of the transparency requirements under Articles 13 and 14 and is inherently linked to the concept of fair processing. Information in relation to *further processing* must be provided "prior to that further processing". WP29's position is that a reasonable period should occur between the notification and the processing commencing rather than an immediate start to the processing upon notification being received by the data subject. This gives data subjects the practical benefits of the principle of transparency, allowing them a meaningful opportunity to consider (and potentially exercise their rights in relation to) the further processing. What is a reasonable period will depend on the particular circumstances. The principle of fairness requires that the more intrusive (or less expected) the further processing, the longer the period should be. Equally, the principle of accountability requires that data controllers be able to demonstrate how the determinations they have made as regards the timing for the provision of this information are justified in the circumstances and how the timing overall is fair to data subjects. (See also the previous comments in relation to ascertaining reasonable timeframes above at paragraphs 30 to 32.)

[43] Recitals 47 and 50

[44] Also referenced in Recital 50

[45] As referenced in Recital 63, this will enable a data subject to exercise the right of access in order to be aware of and to verify the lawfulness of the processing.

Visualisation tools

49. Importantly, the principle of transparency in the GDPR is not limited to being effected simply through language communications (whether written or oral). The GDPR provides for visualisation tools (referencing in particular, icons, certification mechanisms, and data protection seals and marks) where appropriate. Recital 58[46] indicates that the accessibility of information addressed to the public or to data subjects is especially important in the online environment.[47]

Icons

50. Recital 60 makes provision for information to be provided to a data subject "in combination" with standardised icons, thus allowing for a multi-layered approach. However, the use of icons should not simply replace information necessary for the exercise of a data subject's rights nor should they be used as a substitute to compliance with the data controller's obligations under Articles 13 and 14. Article 12.7 provides for the use of such icons stating that:

> "*The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where icons are presented electronically they shall be machine-readable".*

51. As Article 12.7 states that "*Where the icons are presented electronically, they shall be machine-readable"*, this suggests that there may be situations where icons are not presented electronically,[48] for example icons on physical paperwork, IoT devices or IoT device packaging, notices in public places about Wi-Fi tracking, QR codes and CCTV notices.

52. Clearly, the purpose of using icons is to enhance transparency for data subjects by potentially reducing the need for vast amounts of written information to be presented to a data subject. However, the utility of icons to effectively convey information required under Articles 13 and 14 to data subjects is dependent upon the standardisation of symbols/ images to be

[46] "Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising."

[47] In this context, controllers should take into account visually impaired data subjects (e.g. red-green colour blindness).

[48] There is no definition of "machine-readable" in the GDPR but Recital 21 of Directive 2013/37/EU17 defines "machine-readable" as:

"a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats."

universally used and recognised across the EU as shorthand for that information. In this regard, the GDPR assigns responsibility for the development of a code of icons to the Commission but ultimately the European Data Protection Board may, either at the request of the Commission or of its own accord, provide the Commission with an opinion on such icons.[49] WP29 recognises that, in line with Recital 166, the development of a code of icons should be centred upon an evidence-based approach and in advance of any such standardisation it will be necessary for extensive research to be conducted in conjunction with industry and the wider public as to the efficacy of icons in this context.

Certification mechanisms, seals and marks

53. Aside from the use of standardised icons, the GDPR (Article 42) also provides for the use of data protection certification mechanisms, data protection seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by data controllers and processors and enhancing transparency for data subjects.[50] WP29 will be issuing guidelines on certification mechanisms in due course.

Exercise of data subjects' rights

54. Transparency places a triple obligation upon data controllers insofar as the rights of data subjects under the GDPR are concerned, as they must:[51]

- provide information to data subjects on their rights[52] (as required under Articles 13.2(b) and 14.2(c));
- comply with the principle of transparency (i.e. relating to the quality of the communications as set out in Article 12.1) when communicating with data subjects in relation to their rights under Articles 15 to 22 and 34; and
- facilitate the exercise of data subjects' rights under Articles 15 to 22.

55. The GDPR requirements in relation to the exercise of these rights and the nature of the information required are designed to *meaningfully position* data subjects so that they can vindicate their rights and hold data controllers accountable for the processing of their personal data. Recital 59 emphasises that *"modalities should be provided for facilitating the exercise of the data subject's rights"* and that the data controller should *"also provide means*

[49] Article 12.8 provides that the Commission is empowered to adopt delegated acts under Article 92 for the purpose of determining the information to be presented by the icons and the information for providing standardised icons. Recital 166 (which deals with delegated acts of the Commission in general) is instructive, providing that the Commission must carry out appropriate consultations during its preparatory work, including at expert level. However, the European Data Protection Board (EDPB) also has an important consultative role to play in relation to the standardisation of icons as Article 70.1(r) states that the EDPB shall on its own initiative or, where relevant, at the request of the Commission, provide the Commission with an opinion on icons.

[50] See the reference in Recital 100

[51] Under the Transparency and Modalities section of the GDPR on Data Subject Rights (Section 1, Chapter III, namely Article 12)

[52] Access, rectification, erasure, restriction on processing, object to processing, portability

for requests to be made electronically, especially where personal data are processed by electronic means". The modality provided by a data controller for data subjects to exercise their rights should be appropriate to the context and the nature of the relationship and interactions between the controller and a data subject. To this end, a data controller may wish to provide one or more different modalities for the exercise of rights that are reflective of the different ways in which data subjects interact with that data controller.

Example

A health service provider uses an electronic form on its website, and paper forms in the receptions of its health clinics, to facilitate the submission of access requests for personal data both online and in person. While it provides these modalities, the health service still accepts access requests submitted in other ways (such as by letter and by email) and provides a dedicated point of contact (which can be accessed by email and by telephone) to help data subjects with the exercise of their rights.

Exceptions to the obligation to provide information

Article 13 exceptions

56. The only exception to a data controller's Article 13 obligations where it has collected personal data directly from a data subject occurs *"where and insofar as, the data subject already has the information".*[53] The principle of accountability requires that data controllers demonstrate (and document) what information the data subject already has, how and when they received it and that no changes have since occurred to that information that would render it out of date. Further, the use of the phrase "insofar as" in Article 13.4 makes it clear that even if the data subject has previously been provided with certain categories from the inventory of information set out in Article 13, there is still an obligation on the data controller to supplement that information in order to ensure that the data subject now has a complete set of the information listed in Articles 13.1 and 13.2. The following is a best practice example concerning the limited manner in which the Article 13.4 exception should be construed.

Example

An individual signs up to an online email service and receives all of the required Article 13.1 and 13.2 information at the point of sign-up. Six months later the data subject activates a connected instant message functionality through the email service provider and provides their mobile telephone number to do so. The service provider gives the data subject certain Article 13.1 and 13.2 information about the processing of the telephone number (e.g. purposes and legal basis for processing, recipients, retention period) but does not provide other information that the individual already

[53] Article 13.4

has from 6 months ago and which has not since changed (e.g. the identity and contact details of the controller and the data protection officer, information on data subject rights and the right to complain to the relevant supervisory authority). As a matter of best practice however, the complete suite of information should be provided to the data subject again but the data subject also should be able to easily tell what information amongst it is new. The new processing for the purposes of the instant messaging service may affect the data subject in a way which would prompt them to seek to exercise a right they may have forgotten about, having been informed six months prior. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and their rights.

Article 14 exceptions

57. Article 14 carves out a much broader set of exceptions to the information obligation on a data controller where personal data has not been obtained from the data subject. These exceptions should, as a general rule, be interpreted and applied narrowly. In addition to the circumstances where the data subject already has the information in question (Article 14.5(a)), Article 14.5 also allows for the following exceptions:

- The provision of such information is impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or where it would make the achievement of the objectives of the processing impossible or seriously impair them;
- The data controller is subject to a national law or EU law requirement to obtain or disclose the personal data and that the law provides appropriate protections for the data subject's legitimate interests ; or
- An obligation of professional secrecy (including a statutory obligation of secrecy) which is regulated by national or EU law means the personal data must remain confidential.

Proves impossible, disproportionate effort and serious impairment of objectives

58. Article 14.5(b) allows for 3 separate situations where the obligation to provide the information set out in Articles 14.1, 14.2 and 14.4 is lifted:

(i) Where it proves impossible (in particular for archiving, scientific/ historical research or statistical purposes);
(ii) Where it would involve a disproportionate effort (in particular for archiving, scientific/ historical research or statistical purposes); or
(iii) Where providing the information required under Article 14.1 would make the achievement of the objectives of the processing impossible or seriously impair them.

"Proves impossible"

59. The situation where it "proves impossible" under Article 14.5(b) to provide the information is an all or nothing situation because something is either impossible or it is not; there are no degrees of impossibility. Thus if a data controller seeks to rely on this exemption it must demonstrate the factors that actually *prevent it* from providing the information in question to data subjects. If, after a certain period of time, the factors that caused the "impossibility" no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so. In practice, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects. The following example demonstrates this.

Example

A data subject registers for a post-paid online subscription service. After registration, the data controller collects credit data from a credit-reporting agency on the data subject in order to decide whether to provide the service. The controller's protocol is to inform data subjects of the collection of this credit data within three days of collection, pursuant to Article 14.3(a). However, the data subject's address and phone number is not registered in public registries (the data subject is in fact living abroad). The data subject did not leave an email address when registering for the service or the email address is invalid. The controller finds that it has no means to directly contact the data subject. In this case, however, the controller may give information about collection of credit reporting data on its website, prior to registration. In this case, it would not be impossible to provide information pursuant to Article 14.

Impossibility of providing the source of the data

60. Recital 61 states that "*where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided*". The lifting of the requirement to provide data subjects with information on the source of their personal data applies only where this is not possible because different pieces of personal data relating to the same data subject cannot be attributed to a particular source. For example, the mere fact that a database comprising the personal data of multiple data subjects has been compiled by a data controller using more than one source is not enough to lift this requirement if it is possible (although time consuming or burdensome) to identify the source from which the personal data of individual data subjects derived. Given the requirements of data protection by design and by default,[54] transparency mechanisms should be built into processing systems from the ground up so that all sources of personal data received into an organisation can be tracked and traced back to their source at any point in the data processing life cycle (see paragraph 43 above).

[54] Article 25

"Disproportionate effort"

61. Under Article 14.5(b), as with the "proves impossible" situation, "disproportionate effort" may also apply, in particular, for processing *"for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the safeguards referred to in Article 89(1)".* Recital 62 also references these objectives as cases where the provision of information to the data subject would involve a disproportionate effort and states that in this regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration. Given the emphasis in Recital 62 and Article 14.5(b) on archiving, research and statistical purposes with regard to the application of this exemption, WP29's position is that this exception should not be *routinely* relied upon by data controllers who are not processing personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes. WP29 emphasises the fact that where these are the purposes pursued, the conditions set out in Article 89.1 must still be complied with and the provision of the information must constitute a disproportionate effort.

62. In determining what may constitute either impossibility or disproportionate effort under Article 14.5(b), it is relevant that there are no comparable exemptions under Article 13 (where personal data is collected from a data subject). The only difference between an Article 13 and an Article 14 situation is that in the latter, the personal data is not collected from the data subject. It therefore follows that impossibility or disproportionate effort typically arises by virtue of circumstances which do not apply if the personal data is collected from the data subject. In other words, the impossibility or disproportionate effort must be directly connected to the fact that the personal data was obtained other than from the data subject.

> **Example**
>
> A large metropolitan hospital requires all patients for day procedures, longer-term admissions and appointments to fill in a Patient Information Form which seeks the details of two next-of-kin (data subjects). Given the very large volume of patients passing through the hospital on a daily basis, it would involve disproportionate effort on the part of the hospital to provide all persons who have been listed as next-of-kin on forms filled in by patients each day with the information required under Article 14.

63. The factors referred to above in Recital 62 (number of data subjects, the age of the data and any appropriate safeguards adopted) may be indicative of the types of issues that contribute to a data controller having to use disproportionate effort to notify a data subject of the relevant Article 14 information.

> **Example**
>
> Historical researchers seeking to trace lineage based on surnames indirectly obtain a large dataset relating to 20,000 data subjects. However, the dataset was collected 50

years ago, has not been updated since, and does not contain any contact details. Given the size of the database and more particularly, the age of the data, it would involve disproportionate effort for the researchers to try to trace the data subjects individually in order to provide them with Article 14 information.

64. Where a data controller seeks to rely on the exception in Article 14.5(b) on the basis that provision of the information would involve a disproportionate effort, it should carry out a balancing exercise to assess the effort involved for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information. This assessment should be documented by the data controller in accordance with its accountability obligations. In such a case, Article 14.5(b) specifies that the controller must take appropriate measures to protect the data subject's rights, freedoms and legitimate interests. This applies equally where a controller determines that the provision of the information proves impossible, or would likely render impossible or seriously impair the achievement of the objectives of the processing. One appropriate measure, as specified in Article 14.5(b), that controllers must always take is to make the information publicly available. A controller can do this in a number of ways, for instance by putting the information on its website, or by proactively advertising the information in a newspaper or on posters on its premises. Other appropriate measures, in addition to making the information publicly available, will depend on the circumstances of the processing, but may include: undertaking a data protection impact assessment; applying pseudonymisation techniques to the data; minimising the data collected and the storage period; and implementing technical and organisational measures to ensure a high level of security. Furthermore, there may be situations where a data controller is processing personal data which does not require the identification of a data subject (for example with pseudonymised data). In such cases, Article 11.1 may also be relevant as it states that a data controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purposes of complying with the GDPR.

Serious impairment of objectives

65. The final situation covered by Article 14.5(b) is where a data controller's provision of the information to a data subject under Article 14.1 is likely to make impossible or seriously impair the achievement of the processing objectives. To rely on this exception, data controllers must demonstrate that the provision of the information set out in Article 14.1 alone would nullify the objectives of the processing. Notably, reliance on this aspect of Article 14.5(b) pre-supposes that the data processing satisfies all of the principles set out in Article 5 and that most importantly, in all of the circumstances, the processing of the personal data is fair and that it has a legal basis.

Example

Bank A is subject to a mandatory requirement under anti-money laundering legislation to report suspicious activity relating to accounts held with it to the relevant financial law enforcement authority. Bank A receives information from Bank B (in

another Member State) that an account holder has instructed it to transfer money to another account held with Bank A which appears suspicious. Bank A passes this data concerning its account holder and the suspicious activities to the relevant financial law enforcement authority. The anti-money laundering legislation in question makes it a criminal offence for a reporting bank to "tip off" the account holder that they may be subject to regulatory investigations. In this situation, Article 14.5(b) applies because providing the data subject (the account holder with Bank A) with Article 14 information on the processing of account holder's personal data received from Bank B would seriously impair the objectives of the legislation, which includes the prevention of "tip-offs". However, general information should be provided to all account holders with Bank A when an account is opened that their personal data may be processed for anti-money laundering purposes.

Obtaining or disclosing is expressly laid down in law

66. Article 14.5(c) allows for a lifting of the information requirements in Articles 14.1, 14.2 and 14.4 insofar as the obtaining or disclosure of personal data *"is expressly laid down by Union or Member State law to which the controller is subject".* This exemption is conditional upon the law in question providing *"appropriate measures to protect the data subject's legitimate interests".* Such a law must directly address the data controller and the obtaining or disclosure in question should be mandatory upon the data controller. Accordingly, the data controller must be able to demonstrate how the law in question applies to them and requires them to either obtain or disclose the personal data in question. While it is for Union or Member State law to frame the law such that it provides "*appropriate measures to protect the data subject's legitimate interests",* the data controller should ensure (and be able to demonstrate) that its obtaining or disclosure of personal data complies with those measures. Furthermore, the data controller should make it clear to data subjects that it obtains or discloses personal data in accordance with the law in question, unless there is a legal prohibition preventing the data controller from doing so. This is in line with Recital 41 of the GDPR, which states that a legal basis or legislative measure should be clear and precise, and its application should be foreseeable to persons subject to it, in accordance with the case law of the Court of Justice of the EU and the European Court of Human Rights. However, Article 14.5(c) will not apply where the data controller is under an obligation to obtain data *directly from a data subject*, in which case Article 13 will apply. In that case, the only exemption under the GDPR exempting the controller from providing the data subject with information on the processing will be that under Article 13.4 (i.e. where and insofar as the data subject already has the information). However, as referred to below at paragraph 68, at a national level, Member States may also legislate, in accordance with Article 23, for further specific restrictions to the right to transparency under Article 12 and to information under Articles 13 and 14.

Example

A tax authority is subject to a mandatory requirement under national law to obtain the details of employees' salaries from their employers. The personal data is not obtained

from the data subjects and therefore the tax authority is subject to the requirements of Article 14. As the obtaining of the personal data by the tax authority from employers is expressly laid down by law, the information requirements in Article 14 do not apply to the tax authority in this instance.

Confidentiality by virtue of a secrecy obligation

67. Article 14.5(d) provides for an exemption to the information requirement upon data controllers where the personal data *"must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy".* Where a data controller seeks to rely on this exemption, it must be able to demonstrate that it has appropriately identified such an exemption and to show how the professional secrecy obligation directly addresses the data controller such that it prohibits the data controller from providing all of the information set out in Articles 14.1, 14.2 and 14.4 to the data subject.

Example

A medical practitioner (data controller) is under a professional obligation of secrecy in relation to his patients' medical information. A patient (in respect of whom the obligation of professional secrecy applies) provides the medical practitioner with information about her health relating to a genetic condition, which a number of her close relatives also have. The patient also provides the medical practitioner with certain personal data of her relatives (data subjects) who have the same condition. The medical practitioner is not required to provide those relatives with Article 14 information as the exemption in Article 14.5(d) applies. If the medical practitioner were to provide the Article 14 information to the relatives, the obligation of professional secrecy, which he owes to his patient, would be violated.

Restrictions on data subject rights

68. Article 23 provides for Member States (or the EU) to legislate for further restrictions on the scope of the data subject rights in relation to transparency and the substantive data subject rights[55] where such measures respect the essence of the fundamental rights and freedoms and are necessary and proportionate to safeguard one or more of the ten objectives set out in Article 23.1(a) to (j). Where such national measures lessen either the specific data subject rights or the general transparency obligations, which would otherwise apply to data controllers under the GDPR, the data controller should be able to demonstrate how the national provision applies to them. As set out in Article 23.2(h), the legislative measure must contain a provision as to the right of the data subject to be informed about a restriction on

[55] As set out in Articles 12 to 22 and 34, and in Article 5 insofar as its provisions correspond to the rights and obligations provided for in Articles 12 to 22.

their rights, unless so informing them may be prejudicial to the purpose of the restriction. Consistent with this, and in line with principle of fairness, the data controller should also inform data subjects that they are relying on (or will rely on, in the event of a particular data subject right being exercised) such *a national legislative restriction* to the exercise of data subject rights, or to the transparency obligation, unless doing so would be prejudicial to the purpose of the legislative restriction. As such, transparency requires data controllers to provide adequate upfront information to data subjects about their rights and any particular caveats to those rights which the controller may seek to rely on, so that the data subject is not taken by surprise at a purported restriction of a particular right when they later attempt to exercise it against the controller. In relation to pseudonymisation and data minimisation, and insofar as data controllers may purport to rely on Article 11 of the GDPR, WP29 has previously confirmed in Opinion 3/ 2017[56] that Article 11 of the GDPR should be interpreted as a way of enforcing genuine data minimisation without hindering the exercise of data subject rights, and that the exercise of data subject rights must be made possible with the help of additional information provided by the data subject.

69. Additionally, Article 85 requires Member States, by law, to reconcile data protection with the right to freedom of expression and information. This requires, amongst other things, that Member States provide for appropriate exemptions or derogations from certain provisions of the GDPR (including from the transparency requirements under Articles 12 - 14) for processing carried out for journalistic, academic, artistic or literary expression purposes, if they are necessary to reconcile the two rights.

Transparency and data breaches

70. WP29 has produced separate Guidelines on Data Breaches[57] but for the purposes of these guidelines, a data controller's obligations in relation to communication of data breaches to a data subject must take full account of the transparency requirements set out in Article 12.[58] The communication of a data breach must satisfy the same requirements, detailed above (in particular for the use of clear and plain language), that apply to any other communication with a data subject in relation to their rights or in connection with conveying information under Articles 13 and 14.

[56] Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) – see paragraph 4.2

[57] Guidelines on Personal data breach notification under Regulation 2016/679, WP 250

[58] This is made clear by Article 12.1 which specifically refers to "…any communication under Articles 15 to 22 **and 34** relating to processing to the data subject…" [emphasis added].

Annex
Information that must be provided to a data subject under Article 13 or Article 14

Required Information Type	Relevant article (if personal data collected directly from data subject)	Relevant article (if personal data not obtained from the data subject)	WP29 comments on information requirement
The identity and contact details of the controller and, where applicable, their representative[59]	Article 13.1(a)	Article 14.1(a)	This information should allow for easy identification of the controller and preferably allow for different forms of communications with the data controller (e.g. phone number, email, postal address, etc.)
Contact details for the data protection officer, where applicable	Article 13.1(b)	Article 14.1(b)	See WP29 Guidelines on Data Protection Officers[60]
The purposes and legal basis for the processing	Article 13.1(c)	Article 14.1(c)	In addition to setting out the purposes of the processing for which the personal data is intended, the relevant legal basis relied upon under Article 6 must be specified. In the case of special categories of personal data, the relevant provision of Article 9 (and where relevant, the applicable Union or Member State law under which the data is processed) should be specified. Where, pursuant to Article 10, personal data relating to criminal convictions and offences or related security

[59] As defined by Article 4.17 of the GDPR (and referenced in Recital 80), "representative" means a natural or legal person established in the EU who is designated by the controller or processor in writing under Article 27 and represents the controller or processor with regard to their respective obligations under the GDPR. This obligation applies where, in accordance with Article 3.2, the controller or processor is not established in the EU but processes the personal data of data subjects who are in the EU, and the processing relates to the offer of goods or services to, or monitoring of the behaviour of, data subjects in the EU.

[60] Guidelines on Data Protection Officers, WP243 rev.01, last revised and adopted on 5 April 2017

			measures based on Article 6.1 is processed, where applicable the relevant Union or Member State law under which the processing is carried out should be specified.
Where legitimate interests (Article 6.1(f)) is the legal basis for the processing, the legitimate interests pursued by the data controller or a third party	Article 13.1(d)	Article 14.2(b)	The specific interest in question must be identified for the benefit of the data subject. As a matter of best practice, the controller can also provide the data subject with the information from the *balancing test*, which must be carried out to allow reliance on Article 6.1(f) as a lawful basis for processing, in advance of any collection of data subjects' personal data. To avoid information fatigue, this can be included within a layered privacy statement/ notice (see paragraph 35). In any case, the WP29 position is that information to the data subject should make it clear that they can obtain information on the balancing test upon request. This is essential for effective transparency where data subjects have doubts as to whether the balancing test has been carried out fairly or they wish to file a complaint with a supervisory authority.
Categories of personal data concerned	Not required	Article 14.1(d)	This information is required in an Article 14 scenario because the personal data has not been obtained from the data subject, who therefore lacks an awareness of which categories of their personal data the data controller has obtained.

Recipients[61] (or categories of recipients) of the personal data	Article 13.1(e)	Article 14.1(e)	The term "recipient" is defined in Article 4.9 as "*a natural or legal person, public authority, agency or another body, to which the personal data are disclosed,* ***whether a third party or not****" [emphasis added].* As such, a recipient does not have to be a third party. Therefore, other data controllers, joint controllers and processors to whom data is transferred or disclosed are covered by the term "recipient" and information on such recipients should be provided in addition to information on third party recipients. The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.
Details of transfers to third countries, the fact of same and the details of the relevant	Article 13.1(f)	Article 14.1(f)	The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article

[61] As defined by Article 4.9 of the GDPR and referenced in Recital 31

safeguards[62] (including the existence or absence of a Commission adequacy decision[63]) and the means to obtain a copy of them or where they have been made available			45/ binding corporate rules under Article 47/ standard data protection clauses under Article 46.2/ derogations and safeguards under Article 49 etc.) should be specified. Information on where and how the relevant document may be accessed or obtained should also be provided e.g. by providing a link to the mechanism used. In accordance with the principle of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named.
The storage period (or if not possible, criteria used to determine that period)	Article 13.2(a)	Article 14.2(a)	This is linked to the data minimisation requirement in Article 5.1(c) and storage limitation requirement in Article 5.1(e). The storage period (or criteria to determine it) may be dictated by factors such as statutory requirements or industry guidelines but should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, what the retention period will be for specific data/ purposes. It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different

[62] As set out in Article 46.2 and 46.3

[63] In accordance with Article 45

			categories of personal data and/or different processing purposes, including where appropriate, archiving periods.
The rights of the data subject to: • access; • rectification; • erasure; • restriction on processing; • objection to processing and • portability.	Article 13.2(b)	Article 14.2(c)	This information should be specific to the processing scenario and include a summary of what the right involves and how the data subject can take steps to exercise it and any limitations on the right (see paragraph 68 above). In particular, the right to object to processing must be explicitly brought to the data subject's attention at the latest at the time of first communication with the data subject and must be presented clearly and separately from any other information.[64] In relation to the right to portability, see WP29 Guidelines on the right to data portability.[65]
Where processing is based on consent (or explicit consent), the right to withdraw consent at any time	Article 13.2(c)	Article 14.2(d)	This information should include how consent may be withdrawn, taking into account that it should be as easy for a data subject to withdraw consent as to give it.[66]
The right to lodge a complaint with a supervisory authority	Article 13.2(d)	Article 14.2(e)	This information should explain that, in accordance with Article 77, a data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or of an alleged infringement of the GDPR.
Whether there is a statutory or contractual requirement to provide the information or whether it is necessary to	Article 13.2(e)	Not required	For example in an employment context, it may be a contractual requirement to provide certain

[64] Article 21.4 and Recital 70 (which applies in the case of direct marketing)

[65] Guidelines on the right to data portability, WP 242 rev.01, last revised and adopted on 5 April 2017

[66] Article 7.3

enter into a contract or whether there is an obligation to provide the information and the possible consequences of failure.			information to a current or prospective employer. Online forms should clearly identify which fields are "required", which are not, and what will be the consequences of not filling in the required fields.
The source from which the personal data originate, and if applicable, whether it came from a publicly accessible source	Not required	Article 14.2(f)	The specific source of the data should be provided unless it is not possible to do so – see further guidance at paragraph 60. If the specific source is not named then information provided should include: the nature of the sources (i.e. publicly/ privately held sources) and the types of organisation/ industry/ sector.
The existence of automated decision-making including profiling and, if applicable, meaningful information about the logic used and the significance and envisaged consequences of such processing for the data subject	Article 13.2(f)	Article 14.2(g)	See WP29 Guidelines on automated individual decision-making and Profiling.[67]

[67] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251

ARTICLE 29 DATA PROTECTION WORKING PARTY

18/EN

WP250rev.01

Guidelines on Personal data breach notification under Regulation 2016/679

Adopted on 3 October 2017

As last Revised and Adopted on 6 February 2018

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

TABLE OF CONTENTS

INTRODUCTION

The General Data Protection Regulation (the GDPR) introduces the requirement for a personal data breach (henceforth "breach") to be notified to the competent national supervisory authority[1] (or in the case of a cross-border breach, to the lead authority) and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach.

Obligations to notify in cases of breaches presently exist for certain organisations, such as providers of publicly-available electronic communications services (as specified in Directive 2009/136/EC and Regulation (EU) No 611/2013)[2]. There are also some EU Member States that already have their own national breach notification obligation. This may include the obligation to notify breaches involving categories of controllers in addition to providers of publicly available electronic communication services (for example in Germany and Italy), or an obligation to report all breaches involving personal data (such as in the Netherlands). Other Member States may have relevant Codes of Practice (for example, in Ireland[3]). Whilst a number of EU data protection authorities currently encourage controllers to report breaches, the Data Protection Directive 95/46/EC[4], which the GDPR replaces, does not contain a specific breach notification obligation and therefore such a requirement will be new for many organisations. The GDPR now makes notification mandatory for all controllers unless a breach is unlikely to result in a risk to the rights and freedoms of individuals[5]. Processors also have an important role to play and they must notify any breach to their controller[6].

The Article 29 Working Party (WP29) considers that the new notification requirement has a number of benefits. When notifying the supervisory authority, controllers can obtain advice on whether the affected individuals need to be informed. Indeed, the supervisory authority may order the controller to inform those individuals about the breach[7]. Communicating a breach to individuals allows the controller to provide information on the risks presented as a result of the breach and the steps those individuals can take to protect themselves from its potential consequences. The focus of any breach response plan should be on protecting individuals and their personal data. Consequently, breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data. At the same time, it should be noted that failure to report a breach to either an individual or a supervisory authority may mean that under Article 83 a possible sanction is applicable to the controller.

---

[1] See Article 4(21) of the GDPR

[2] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 and http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0611

[3] See https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

[5] The rights enshrined in the Charter of Fundamental Rights of the EU, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[6] See Article 33(2). This is similar in concept to Article 5 of Regulation (EU) No 611/2013 which states that a provider that is contracted to deliver part of an electronic communications service (without having a direct contractual relationship with subscribers) is obliged to notify the contracting provider in the event of a personal data breach.

[7] See Articles 34(4) and 58(2)(e)

Controllers and processors are therefore encouraged to plan in advance and put in place processes to be able to detect and promptly contain a breach, to assess the risk to individuals[8], and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary. Notification to the supervisory authority should form a part of that incident response plan.

The GDPR contains provisions on when a breach needs to be notified, and to whom, as well as what information should be provided as part of the notification. Information required for the notification can be provided in phases, but in any event controllers should act on any breach in a timely manner.

In its Opinion 03/2014 on personal data breach notification[9], WP29 provided guidance to controllers in order to help them to decide whether to notify data subjects in case of a breach. The opinion considered the obligation of providers of electronic communications regarding Directive 2002/58/EC and provided examples from multiple sectors, in the context of the then draft GDPR, and presented good practices for all controllers.

The current Guidelines explain the mandatory breach notification and communication requirements of the GDPR and some of the steps controllers and processors can take to meet these new obligations. They also give examples of various types of breaches and who would need to be notified in different scenarios.

I. Personal data breach notification under the GDPR

A. Basic security considerations

One of the requirements of the GDPR is that, by using appropriate technical and organisational measures, personal data shall be processed in a manner to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage[10].

Accordingly, the GDPR requires both controllers and processors to have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the personal data being processed. They should take into account the state of the art, the costs of implementation and the nature, the scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons[11]. Also, the GDPR requires all appropriate technological protection an organisational measures to be in place to establish immediately whether a breach has taken place, which then determines whether the notification obligation is engaged[12].

Consequently, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.

---

[8] This can be ensured under the monitoring and review requirement of a DPIA, which is required for processing operations likely to result in a high risk to the rights and freedoms of natural persons (Article 35(1) and (11).

[9] See Opinion 03/2014 on Personal Data Breach Notification http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[10] See Articles 5(1)(f) and 32.

[11] Article 32; see also Recital 83

[12] See Recital 87

B. What is a personal data breach?

1. Definition

As part of any attempt to address a breach the controller should first be able to recognise one. The GDPR defines a "personal data breach" in Article 4(12) as:

> "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

What is meant by "destruction" of personal data should be quite clear: this is where the data no longer exists, or no longer exists in a form that is of any use to the controller. "Damage" should also be relatively clear: this is where personal data has been altered, corrupted, or is no longer complete. In terms of "loss" of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession. Finally, unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

Example

An example of loss of personal data can include where a device containing a copy of a controller's customer database has been lost or stolen. A further example of loss may be where the only copy of a set of personal data has been encrypted by ransomware, or has been encrypted by the controller using a key that is no longer in its possession.

What should be clear is that a breach is a type of security incident. However, as indicated by Article 4(12), the GDPR only applies where there is a breach of *personal data*. The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 of the GDPR. This highlights the difference between a security incident and a personal data breach – in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches[13].

The potential adverse effects of a breach on individuals are considered below.

2. Types of personal data breaches

In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorised according to the following three well-known information security principles[14]:

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
- "Availability breach" - where there is an accidental or unauthorised loss of access[15] to, or destruction of, personal data.

[13] It should be noted that a security incident is not limited to threat models where an attack is made on an organisation from an external source, but includes incidents from internal processing that breach security principles.

[14] See Opinion 03/2014

[15] It is well established that "access" is fundamentally part of "availability". See, for example, NIST SP800-53rev4, which defines "availability" as: "Ensuring timely and reliable access to and use of information,"

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

Example

Examples of a loss of availability include where data has been deleted either accidentally or by an unauthorised person, or, in the example of securely encrypted data, the decryption key has been lost. In the event that the controller cannot restore access to the data, for example, from a backup, then this is regarded as a permanent loss of availability.

A loss of availability may also occur where there has been significant disruption to the normal service of an organisation, for example, experiencing a power failure or denial of service attack, rendering personal data unavailable.

The question may be asked whether a temporary loss of availability of personal data should be considered as a breach and, if so, one which needs to be notified. Article 32 of the GDPR, "security of processing," explains that when implementing technical and organisational measures to ensure a level of security appropriate to the risk, consideration should be given, amongst other things, to "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services," and "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".

Therefore, a security incident resulting in personal data being made unavailable for a period of time is also a type of breach, as the lack of access to the data can have a significant impact on the rights and freedoms of natural persons. To be clear, where personal data is unavailable due to planned system maintenance being carried out this is not a 'breach of security' as defined in Article 4(12).

As with a permanent loss or destruction of personal data (or indeed any other type of breach), a breach involving the temporary loss of availability should be documented in accordance with Article 33(5). This assists the controller in demonstrating accountability to the supervisory authority, which may ask to see those records[16].However, depending on the circumstances of the breach, it may or may not require notification to the supervisory authority and communication to affected individuals. The controller will need to assess the likelihood and severity of the impact on the rights and freedoms of natural persons as a result of the lack of availability of personal data. In accordance with Article 33, the controller will need to notify unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Of course, this will need to be assessed on a case-by-case basis.

Examples

available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 also refers to: "The property of being accessible and useable upon demand by an authorized entity." See https://rmf.org/images/4-CNSS-Publications/CNSSI-4009.pdf. ISO/IEC 27000:2016 also defines "availability" as "Property of being accessible and usable upon demand by an authorized entity": https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

[16] See Article 33(5)

In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled and lives put at risk.

Conversely, in the case of a media company's systems being unavailable for several hours (e.g. due to a power outage), if that company is then prevented from sending newsletters to its subscribers, this is unlikely to present a risk to individuals' rights and freedoms.

It should be noted that although a loss of availability of a controller's systems might be only temporary and may not have an impact on individuals, it is important for the controller to consider all possible consequences of a breach, as it may still require notification for other reasons.

Example

Infection by ransomware (malicious software which encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals.

3. The possible consequences of a personal data breach

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals[17].

Accordingly, the GDPR requires the controller to notify a breach to the competent supervisory authority, unless it is unlikely to result in a risk of such adverse effects taking place. Where there is a likely high risk of these adverse effects occurring, the GDPR requires the controller to communicate the breach to the affected individuals as soon as is reasonably feasible[18].

The importance of being able to identify a breach, to assess the risk to individuals, and then notify if required, is emphasised in Recital 87 of the GDPR:

"It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation."

Further guidelines on assessing the risk of adverse effects to individuals are considered in section IV.

If controllers fail to notify either the supervisory authority or data subjects of a data breach or both even though the requirements of Articles 33 and/or 34 are fulfilled, then the supervisory authority is

[17] See also Recitals 85 and 75

[18] See also Recital 86.

presented with a choice that must include consideration of all of the corrective measures at its disposal, which would include consideration of the imposition of the appropriate administrative fine[19], either accompanying a corrective measure under Article 58(2) or on its own. Where an administrative fine is chosen, its value can be up to 10,000,000 EUR or up to 2 % if the total worldwide annual turnover of an undertaking under Article 83(4)(a) of the GDPR. It is also important to bear in mind that in some cases, the failure to notify a breach could reveal either an absence of existing security measures or an inadequacy of the existing security measures. The WP29 guidelines on administrative fines state: "The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement". In that case, the supervisory authority will also have the possibility to issue sanctions for failure to notify or communicate the breach (Articles 33 and 34) on the one hand, and absence of (adequate) security measures (Article 32) on the other hand, as they are two separate infringements.

II. Article 33 - Notification to the supervisory authority

A. When to notify

1. Article 33 requirements

Article 33(1) provides that:

> "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

Recital 87 states[20]:

> "It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation."

2. When does a controller become "aware"?

As detailed above, the GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become "aware" of a breach. WP29 considers that a controller should be regarded as having become "aware" when that

[19] For further details, please see WP29 Guidelines on the application and setting of administrative fines, available here: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

[20] Recital 85 is also important here.

controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject[21]. This puts an obligation on the controller to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action.

When, exactly, a controller can be considered to be "aware" of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

Examples

1. In the case of a loss of a USB key with unencrypted personal data it is often not possible to ascertain whether unauthorised persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become "aware" when it realised the USB key had been lost.

2. A third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As the controller has been presented with clear evidence of a confidentiality breach then there can be no doubt that it has become "aware".

3. A controller detects that there has been a possible intrusion into its network. The controller checks its systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, as the controller now has clear evidence of a breach there can be no doubt that it has become "aware".

4. A cybercriminal contacts the controller after having hacked its system in order to ask for a ransom. In that case, after checking its system to confirm it has been attacked the controller has clear evidence that a breach has occurred and there is no doubt that it has become aware.

After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.

Once the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered, as well as the action(s) needed to address the breach. However, a controller may already have an initial assessment of the potential risk that could result from a breach as part of a data protection impact

[21] See Recital 87

assessment (DPIA)[22] made prior to carrying out the processing operation concerned. However, the DPIA may be more generalised in comparison to the specific circumstances of any actual breach, and so in any event an additional assessment taking into account those circumstances will need to be made. For more detail on assessing risk, see section IV.

In most cases these preliminary actions should be completed soon after the initial alert (i.e. when the controller or processor suspects there has been a security incident which may involve personal data.) – it should take longer than this only in exceptional cases.

Example

An individual informs the controller that they have received an email impersonating the controller which contains personal data relating to his (actual) use of the controller's service, suggesting that the security of the controller has been compromised. The controller conducts a short period of investigation and identifies an intrusion into their network and evidence of unauthorised access to personal data. The controller would now be considered as "aware" and notification to the supervisory authority is required unless this is unlikely to present a risk to the rights and freedoms of individuals. The controller will need to take appropriate remedial action to address the breach.

The controller should therefore have internal processes in place to be able to detect and address a breach. For example, for finding some irregularities in data processing the controller or processor may use certain technical measures such as data flow and log analysers, from which is possible to define events and alerts by correlating any log data[23]. It is important that when a breach is detected it is reported upwards to the appropriate level of management so it can be addressed and, if required, notified in accordance with Article 33 and, if necessary, Article 34. Such measures and reporting mechanisms could be detailed in the controller's incident response plans and/or governance arrangements. These will help the controller to plan effectively and determine who has operational responsibility within the organisation for managing a breach and how or whether to escalate an incident as appropriate.

The controller should also have in place arrangements with any processors the controller uses, which themselves have an obligation to notify the controller in the event of a breach (see below).

Whilst it is the responsibility of controllers and processors to put in place suitable measures to be able to prevent, react and address a breach, there are some practical steps that should be taken in all cases.

- Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk.
- Risk to individuals as a result of a breach should then be assessed (likelihood of no risk, risk or high risk), with relevant sections of the organisation being informed.
- Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required.
- At the same time, the controller should act to contain and recover the breach.
- Documentation of the breach should take place as it develops.

Accordingly, it should be clear that there is an obligation on the controller to act on any initial alert and establish whether or not a breach has, in fact, occurred. This brief period allows for some

[22] See WP29 Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[23] It should be noted that log data facilitating auditability of, e.g., storage, modifications or erasure of data may also qualify as personal data relating to the person who initiated the respective processing operation.

investigation, and for the controller to gather evidence and other relevant details. However, once the controller has established with a reasonable degree of certainty that a breach has occurred, if the conditions in Article 33(1) have been met, it must then notify the supervisory authority without undue delay and, where feasible, not later than 72 hours[24]. If a controller fails to act in a timely manner and it becomes apparent that a breach did occur, this could be considered as a failure to notify in accordance with Article 33.

Article 32 makes clear that the controller and processor should have appropriate technical and organisational measures in place to ensure an appropriate level of security of personal data: the ability to detect, address, and report a breach in a timely manner should be seen as essential elements of these measures.

3. Joint controllers

Article 26 concerns joint controllers and specifies that joint controllers shall determine their respective responsibilities for compliance with the GDPR[25]. This will include determining which party will have responsibility for complying with the obligations under Articles 33 and 34. WP29 recommends that the contractual arrangements between joint controllers include provisions that determine which controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations.

4. Processor obligations

The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play to enable the controller to comply with its obligations; and this includes breach notification. Indeed, Article 28(3) specifies that the processing by a processor shall be governed by a contract or other legal act. Article 28(3)(f) states that the contract or other legal act shall stipulate that the processor "assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor".

Article 33(2) makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller "without undue delay". It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller. The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has informed it of the breach. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1). The controller might also want to investigate the breach, as the processor might not be in a position to know all the relevant facts relating to the matter, for example, if a copy or backup of personal data destroyed or lost by the processor is still held by the controller. This may affect whether the controller would then need to notify.

The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so "without undue delay". Therefore, WP29 recommends the

[24] See Regulation No 1182/71 determining the rules applicable to periods, dates and time limits, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN

[25] See also Recital 79.

processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.

As is explained above, the contract between the controller and processor should specify how the requirements expressed in Article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller's obligations to report to the supervisory authority within 72 hours.

Where the processor provides services to multiple controllers that are all affected by the same incident, the processor will have to report details of the incident to each controller.

A processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor. Such notification must be made in accordance with Article 33 and 34. However, it is important to note that the legal responsibility to notify remains with the controller.

B. Providing information to the supervisory authority

1. Information to be provided

When a controller notifies a breach to the supervisory authority, Article 33(3) states that, at the minimum, it should:

> "(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
>
> (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
>
> (c) describe the likely consequences of the personal data breach;
>
> (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."

The GDPR does not define categories of data subjects or personal data records. However, WP29 suggests categories of data subjects to refer to the various types of individuals whose personal data has been affected by a breach: depending on the descriptors used, this could include, amongst others, children and other vulnerable groups, people with disabilities, employees or customers. Similarly, categories of personal data records can refer to the different types of records that the controller may process, such as health data, educational records, social care information, financial details, bank account numbers, passport numbers and so on.

Recital 85 makes it clear that one of the purposes of notification is limiting damage to individuals. Accordingly, if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important the notification indicates these categories. In this way, it is linked to the requirement of describing the likely consequences of the breach.

Where precise information is not available (e.g. exact number of data subjects affected) this should not be a barrier to timely breach notification. The GDPR allows for approximations to be made in the number of individuals affected and the number of personal data records concerned. The focus should be directed towards addressing the adverse effects of the breach rather than providing precise figures.

Thus, when it has become clear that here has been a breach, but the extent of it is not yet known, a notification in phases (see below) is a safe way to meet the notification obligations.

Article 33(3) states that the controller "shall at least" provide this information with a notification, so a controller can, if necessary, choose to provide further details. Different types of breaches (confidentiality, integrity or availability) might require further information to be provided to fully explain the circumstances of each case.

Example

As part of its notification to the supervisory authority, a controller may find it useful to name its processor if it is at the root cause of a breach, particularly if this has led to an incident affecting the personal data records of many other controllers that use the same processor.

In any event, the supervisory authority may request further details as part of its investigation into a breach.

2. Notification in phases

Depending on the nature of a breach, further investigation by the controller may be necessary to establish all of the relevant facts relating to the incident. Article 33(4) therefore states:

"Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay."

This means that the GDPR recognises that controllers will not always have all of the necessary information concerning a breach within 72 hours of becoming aware of it, as full and comprehensive details of the incident may not always be available during this initial period. As such, it allows for a notification in phases. It is more likely this will be the case for more complex breaches, such as some types of cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data have been compromised. Consequently, in many cases the controller will have to do more investigation and follow-up with additional information at a later point. This is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1). WP29 recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on. The supervisory authority should agree how and when additional information should be provided. This does not prevent the controller from providing further information at any other stage, if it becomes aware of additional relevant details about the breach that need to be provided to the supervisory authority.

The focus of the notification requirement is to encourage controllers to act promptly on a breach, contain it and, if possible, recover the compromised personal data, and to seek relevant advice from the supervisory authority. Notifying the supervisory authority within the first 72 hours can allow the controller to make sure that decisions about notifying or not notifying individuals are correct.

However, the purpose of notifying the supervisory authority is not solely to obtain guidance on whether to notify the affected individuals. It will be obvious in some cases that, due to the nature of the breach and the severity of the risk, the controller will need to notify the affected individuals without delay. For example, if there is an immediate threat of identity theft, or if special categories of personal data[26] are disclosed online, the controller should act without undue delay to contain the

[26] See Article 9.

breach and to communicate it to the individuals concerned (see section III). In exceptional circumstances, this might even take place before notifying the supervisory authority. More generally, notification of the supervisory authority may not serve as a justification for failure to communicate the breach to the data subject where it is required.

It should also be clear that after making an initial notification, a controller could update the supervisory authority if a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred. This information could then be added to the information already given to the supervisory authority and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

Example

A controller notifies the supervisory authority within 72 hours of detecting a breach that it has lost a USB key containing a copy of the personal data of some of its customers. The USB key is later found misfiled within the controller's premises and recovered. The controller updates the supervisory authority and requests the notification be amended.

It should be noted that a phased approach to notification is already the case under the existing obligations of Directive 2002/58/EC, Regulation 611/2013 and other self-reported incidents.

3. Delayed notifications

Article 33(1) makes it clear that where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. This, along with the concept of notification in phases, recognises that a controller may not always be able to notify a breach within that time period, and that a delayed notification may be permissible.

Such a scenario might take place where, for example, a controller experiences multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way. A controller could become aware of a breach and, whilst beginning its investigation, and before notification, detect further similar breaches, which have different causes. Depending on the circumstances, it may take the controller some time to establish the extent of the breaches and, rather than notify each breach individually, the controller instead organises a meaningful notification that represents several very similar breaches, with possible different causes. This could lead to notification to the supervisory authority being delayed by more than 72 hours after the controller first becomes aware of these breaches.

Strictly speaking, each individual breach is a reportable incident. However, to avoid being overly burdensome, the controller may be able to submit a "bundled" notification representing all these breaches, provided that they concern the same type of personal data breached in the same way, over a relatively short space of time. If a series of breaches take place that concern different types of personal data, breached in different ways, then notification should proceed in the normal way, with each breach being reported in accordance with Article 33.

Whilst the GDPR allows for delayed notifications to an extent, this should not be seen as something that regularly takes place. It is worth pointing out that bundled notifications can also be made for multiple similar breaches reported within 72 hours.

C. Cross-border breaches and breaches at non-EU establishments

1. Cross-border breaches

Where there is cross-border processing[27] of personal data, a breach may affect data subjects in more than one Member State. Article 33(1) makes it clear that when a breach has occurred, the controller should notify the supervisory authority competent in accordance with Article 55 of the GDPR[28]. Article 55(1) says that:

> "Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State."

However, Article 56(1) states:

> "Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60."

Furthermore, Article 56(6) states:

> "The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor."

This means that whenever a breach takes place in the context of cross-border processing and notification is required, the controller will need to notify the lead supervisory authority[29]. Therefore, when drafting its breach response plan, a controller must make an assessment as to which supervisory authority is the lead supervisory authority that it will need to notify[30]. This will allow the controller to respond promptly to a breach and to meet its obligations in respect of Article 33. It should be clear that in the event of a breach involving cross-border processing, notification must be made to the lead supervisory authority, which is not necessarily where the affected data subjects are located, or indeed where the breach has taken place. When notifying the lead authority, the controller should indicate, where appropriate, whether the breach involves establishments located in other Member States, and in which Member States data subjects are likely to have been affected by the breach. If the controller has any doubt as to the identity of the lead supervisory authority then it should, at a minimum, notify the local supervisory authority where the breach has taken place.

2. Breaches at non-EU establishments

Article 3 concerns the territorial scope of the GDPR, including when it applies to the processing of personal data by a controller or processor that is not established in the EU. In particular, Article 3(2) states[31]:

---

[27] See Article 4(23)

[28] See also Recital 122.

[29] See WP29 Guidelines for identifying a controller or processor's lead supervisory authority, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[30] A list of contact details for all European national data protection authorities can be found at: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] See also Recitals 23 and 24

"This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

Article 3(3) is also relevant and states[32]:

"This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

Where a controller not established in the EU is subject to Article 3(2) or Article 3(3) and experiences a breach, it is therefore still bound by the notification obligations under Articles 33 and 34. Article 27 requires a controller (and processor) to designate a representative in the EU where Article 3(2) applies. In such cases, WP29 recommends that notification should be made to the supervisory authority in the Member State where the controller's representative in the EU is established[33]. Similarly, where a processor is subject to Article 3(2), it will be bound by the obligations on processors, of particular relevance here, the duty to notify a breach to the controller under Article 33(2).

D. Conditions where notification is not required

Article 33(1) makes it clear that breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons" do not require notification to the supervisory authority. An example might be where personal data are already publically available and a disclosure of such data does not constitute a likely risk to the individual. This is in contrast to existing breach notification requirements for providers of publically available electronic communications services in Directive 2009/136/EC that state all relevant breaches have to be notified to the competent authority.

In its Opinion 03/2014 on breach notification[34], WP29 explained that a confidentiality breach of personal data that were encrypted with a state of the art algorithm is still a personal data breach, and has to be notified. However, if the confidentiality of the key is intact – i.e., the key was not compromised in any security breach, and was generated so that it cannot be ascertained by available technical means by any person who is not authorised to access it – then the data are in principle unintelligible. Thus, the breach is unlikely to adversely affect individuals and therefore would not require communication to those individuals[35]. However, even where data is encrypted, a loss or alteration can have negative consequences for data subjects where the controller has no adequate backups. In that instance communication to data subjects would be required, even if the data itself was subject to adequate encryption measures.

[32] See also Recital 25

[33] See Recital 80 and Article 27

[34] WP29, Opinion 03/2014 on breach notification, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[35] See also Article 4(1) and (2) of Regulation 611/2013.

WP29 also explained this would similarly be the case if personal data, such as passwords, were securely hashed and salted, the hashed value was calculated with a state of the art cryptographic keyed hash function, the key used to hash the data was not compromised in any breach, and the key used to hash the data has been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access it.

Consequently, if personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority. This is because such a breach is unlikely to pose a risk to individuals' rights and freedoms. This of course means that the individual would not need to be informed either as there is likely no high risk. However, it should be borne in mind that while notification may initially not be required if there is no likely risk to the rights and freedoms of individuals, this may change over time and the risk would have to be re-evaluated. For example, if the key is subsequently found to be compromised, or a vulnerability in the encryption software is exposed, then notification may still be required.

Furthermore, it should be noted that if there is a breach where there are no backups of the encrypted personal data then there will have been an availability breach, which could pose risks to individuals and therefore may require notification. Similarly, where a breach occurs involving the loss of encrypted data, even if a backup of the personal data exists this may still be a reportable breach, depending on the length of time taken to restore the data from that backup and the effect that lack of availability has on individuals. As Article 32(1)(c) states, an important factor of security is the "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".

Example

A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device, utilised by the controller and its staff. Provided the encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question. If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.

However, a failure to comply with Article 33 will exist where a controller does not notify the supervisory authority in a situation where the data has not actually been securely encrypted. Therefore, when selecting encryption software controllers should carefully weigh the quality and the proper implementation of the encryption offered, understand what level of protection it actually provides and whether this is appropriate to the risks presented. Controllers should also be familiar with the specifics of how their encryption product functions. For instance, a device may be encrypted once it is switched off, but not while it is in stand-by mode. Some products using encryption have "default keys" that need to be changed by each customer to be effective. The encryption may also be considered currently adequate by security experts, but may become outdated in a few years' time, meaning it is questionable whether the data would be sufficiently encrypted by that product and provide an appropriate level of protection.

III. **Article 34 – Communication to the data subject**

A. Informing individuals

In certain cases, as well as notifying the supervisory authority, the controller is also required to communicate a breach to the affected individuals.

Article 34(1) states:

> "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

Controllers should recall that notification to the supervisory authority is mandatory unless there is unlikely to be a risk to the rights and freedoms of individuals as a result of a breach. In addition, where there is likely a high risk to the rights and freedoms of individuals as the result of a breach, individuals must also be informed. The threshold for communicating a breach to individuals is therefore higher than for notifying supervisory authorities and not all breaches will therefore be required to be communicated to individuals, thus protecting them from unnecessary notification fatigue.

The GDPR states that communication of a breach to individuals should be made "without undue delay," which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves[36]. As noted above, depending on the nature of the breach and the risk posed, timely communication will help individuals to take steps to protect themselves from any negative consequences of the breach.

Annex B of these Guidelines provides a non-exhaustive list of examples of when a breach may be likely to result in high risk to individuals and consequently instances when a controller will have to notify a breach to those affected.

B. Information to be provided

When notifying individuals, Article 34(2) specifies that:

> "The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)."

According to this provision, the controller should at least provide the following information:

- a description of the nature of the breach;
- the name and contact details of the data protection officer or other contact point;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

As an example of the measures taken to address the breach and to mitigate its possible adverse effects, the controller could state that, after having notified the breach to the relevant supervisory authority, the controller has received advice on managing the breach and lessening its impact. The controller should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised. Again, a controller can choose to provide information in addition to what is required here.

[36] See also Recital 86.

C. Contacting individuals

In principle, the relevant breach should be communicated to the affected data subjects directly, unless doing so would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner (Article 34(3)c).

Dedicated messages should be used when communicating a breach to data subjects and they should not be sent with other information, such as regular updates, newsletters, or standard messages. This helps to make the communication of the breach to be clear and transparent.

Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual. WP29 recommends that controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel.

Controllers may also need to ensure that the communication is accessible in appropriate alternative formats and relevant languages to ensure individuals are able to understand the information being provided to them. For example, when communicating a breach to an individual, the language used during the previous normal course of business with the recipient will generally be appropriate. However, if the breach affects data subjects who the controller has not previously interacted with, or particularly those who reside in a different Member State or other non-EU country from where the controller is established, communication in the local national language could be acceptable, taking into account the resource required. The key is to help data subjects understand the nature of the breach and steps they can take to protect themselves.

Controllers are best placed to determine the most appropriate contact channel to communicate a breach to individuals, particularly if they interact with their customers on a frequent basis. However, clearly a controller should be wary of using a contact channel compromised by the breach as this channel could also be used by attackers impersonating the controller.

At the same time, Recital 86 explains that:

> "Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication."

Controllers might therefore wish to contact and consult the supervisory authority not only to seek advice about informing data subjects about a breach in accordance with Article 34, but also on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.

Linked to this is the advice given in Recital 88 that notification of a breach should "take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach". This may mean that in certain circumstances, where justified, and on the advice of law-enforcement authorities, the controller may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.

Whenever it is not possible for the controller to communicate a breach to an individual because there is insufficient data stored to contact the individual, in that particular circumstance the controller should inform the individual as soon as it is reasonably feasible to do so (e.g. when an individual exercises their Article 15 right to access personal data and provides the controller with necessary additional information to contact them).

D. Conditions where communication is not required

Article 34(3) states three conditions that, if met, do not require notification to individuals in the event of a breach. These are:

- The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.
- Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.
- It would involve disproportionate effort[37] to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. For example, the warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.

In accordance with the accountability principle controllers should be able to demonstrate to the supervisory authority that they meet one or more of these conditions [38]. It should be borne in mind that while notification may initially not be required if there is no risk to the rights and freedoms of natural persons, this may change over time and the risk would have to be re-evaluated.

If a controller decides not to communicate a breach to the individual, Article 34(4) explains that the supervisory authority can require it to do so, if it considers the breach is likely to result in a high risk to individuals. Alternatively, it may consider that the conditions in Article 34(3) have been met in which case notification to individuals is not required. If the supervisory authority determines that the decision not to notify data subjects is not well founded, it may consider employing its available powers and sanctions.

IV. **Assessing risk and high risk**

A. Risk as a trigger for notification

[37] See WP29 Guidelines on transparency, which will consider the issue of disproportionate effort, available at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] See Article 5(2)

Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances:

- Notification to the competent supervisory authority is required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals.
- Communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.

This means that immediately upon becoming aware of a breach, it is vitally important that the controller should not only seek to contain the incident but it should also assess the risk that could result from it. There are two important reasons for this: firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned.

As explained above, notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals, and the key trigger requiring communication of a breach to data subjects is where it is likely to result in a *high* risk to the rights and freedoms of individuals. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur[39].

B. Factors to consider when assessing risk

Recitals 75 and 76 of the GDPR suggest that generally when assessing risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. It further states that risk should be evaluated on the basis of an objective assessment.

It should be noted that assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA)[40]. The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals.

Example

A DPIA suggests that the proposed use of a particular security software product to protect personal data is a suitable measure to ensure a level of security appropriate to the risk the processing would otherwise present to individuals. However, if a vulnerability becomes subsequently known, this would change the software's suitability to contain the risk to the personal data protected and so it would need to be re-assessed as part of an ongoing DPIA.

[39] See Recital 75 and Recital 85.

[40] See WP Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

A vulnerability in the product is later exploited and a breach occurs. The controller should assess the specific circumstances of the breach, the data affected, and the potential level of impact on individuals, as well as how likely this risk will materialise.

Accordingly, when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. WP29 therefore recommends the assessment should take into account the following criteria[41]:

- The type of breach

The type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual's medical details have been lost, and are no longer available.

- The nature, sensitivity, and volume of personal data

Of course, when assessing risk, a key factor is the type and sensitivity of personal data that has been compromised by the breach. Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of the name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child.

Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data.

Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A list of customers accepting regular deliveries may not be particularly sensitive, but the same data about customers who have requested that their deliveries be stopped while on holiday would be useful information to criminals.

Similarly, a small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.

- Ease of identification of individuals

An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match personal data to a particular individual, but it could still be possible

[41] Article 3.2 of Regulation 611/2013 provides guidance the factors that should be taken into consideration in relation to the notification of breaches in the electronic communication services sector, which may be useful in the context of notification under the GDPR. See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

under certain conditions. Identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach, and public availability of related personal details. This may be more relevant for confidentiality and availability breaches.

As stated above, personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Additionally, appropriately-implemented pseudonymisation (defined in Article 4(5) as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person") can also reduce the likelihood of individuals being identified in the event of a breach. However, pseudonymisation techniques alone cannot be regarded as making the data unintelligible.

- Severity of consequences for individuals.

Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.

Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk. There may be a confidentiality breach, whereby personal data is disclosed to a third party, as defined in Article 4(10), or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered "trusted". In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches (see section V, below).

Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term.

- Special characteristics of the individual

A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them.

- Special characteristics of the data controller

The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal

data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.

- The number of affected individuals

A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected.

- General points

Therefore, when assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the controller should err on the side of caution and notify. Annex B provides some useful examples of different types of breaches involving risk or high risk to individuals.

The European Union Agency for Network and Information Security (ENISA) has produced recommendations for a methodology of assessing the severity of a breach, which controllers and processors may find useful when designing their breach management response plan[42].

V. Accountability and record keeping

A. Documenting breaches

Regardless of whether or not a breach needs to be notified to the supervisory authority, the controller must keep documentation of all breaches, as Article 33(5) explains:

> "The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."

This is linked to the accountability principle of the GDPR, contained in Article 5(2). The purpose of recording non-notifiable breaches, as well notifiable breaches, also relates to the controller's obligations under Article 24, and the supervisory authority can request to see these records. Controllers are therefore encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not[43].

Whilst it is up to the controller to determine what method and structure to use when documenting a breach, in terms of recordable information there are key elements that should be included in all cases. As is required by Article 33(5), the controller needs to record details concerning the breach, which

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity

[43] The controller may choose to document breaches as part of if its record of processing activities which is maintained pursuant to article 30. A separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request.

should include its causes, what took place and the personal data affected. It should also include the effects and consequences of the breach, along with the remedial action taken by the controller.

The GDPR does not specify a retention period for such documentation. Where such records contain personal data, it will be incumbent on the controller to determine the appropriate period of retention in accordance with the principles in relation to the processing of personal data[44] and to meet a lawful basis for processing[45]. It will need to retain documentation in accordance with Article 33(5) insofar as it may be called to provide evidence of compliance with that Article, or with the accountability principle more generally, to the supervisory authority. Clearly, if the records themselves contain no personal data then the storage limitation principle[46] of the GDPR does not apply.

In addition to these details, WP29 recommends that the controller also document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers the breach is unlikely to result in a risk to the rights and freedoms of individuals[47]. Alternatively, if the controller considers that any of the conditions in Article 34(3) are met, then it should be able to provide appropriate evidence that this is the case.

Where the controller does notify a breach to the supervisory authority, but the notification is delayed, the controller must be able to provide reasons for that delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive.

Where the controller communicates a breach to the affected individuals, it should be transparent about the breach and communicate in an effective and timely manner. Accordingly, it would help the controller to demonstrate accountability and compliance by retaining evidence of such communication.

To aid compliance with Articles 33 and 34, it would be advantageous to both controllers and processors to have a documented notification procedure in place, setting out the process to follow once a breach has been detected, including how to contain, manage and recover the incident, as well as assessing risk, and notifying the breach. In this regard, to show compliance with GDPR it might also be useful to demonstrate that employees have been informed about the existence of such procedures and mechanisms and that they know how to react to breaches.

It should be noted that failure to properly document a breach can lead to the supervisory authority exercising its powers under Article 58 and, or imposing an administrative fine in accordance with Article 83.

B. Role of the Data Protection Officer

A controller or processor may have a Data Protection Officer (DPO)[48], either as required by Article 37, or voluntarily as a matter of good practice. Article 39 of the GDPR sets a number of mandatory tasks for the DPO, but does not prevent further tasks being allocated by the controller, if appropriate.

---

[44] See Article 5

[45] See Article 6 and also Article 9.

[46] See Article 5(1)(e).

[47] See Recital 85

[48] See WP Guidelines on DPOs here: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Of particular relevance to breach notification, the mandatory tasks of the DPO includes, amongst other duties, providing data protection advice and information to the controller or processor, monitoring compliance with the GDPR, and providing advice in relation to DPIAs. The DPO must also cooperate with the supervisory authority and act as a contact point for the supervisory authority and for data subjects. It should also be noted that, when notifying the breach to the supervisory authority, Article 33(3)(b) requires the controller to provide the name and contact details of its DPO, or other contact point.

In terms of documenting breaches, the controller or processor may wish to obtain the opinion of its DPO as to the structure, the setting up and the administration of this documentation. The DPO could also be additionally tasked with maintaining such records.

These factors mean that the DPO should play an key role in assisting the prevention of or preparation for a breach by providing advice and monitoring compliance, as well as during a breach (i.e. when notifying the supervisory authority), and during any subsequent investigation by the supervisory authority. In this light, WP29 recommends that the DPO is promptly informed about the existence of a breach and is involved throughout the breach management and notification process.

VI. Notification obligations under other legal instruments

In addition to, and separate from, the notification and communication of breaches under the GDPR, controllers should also be aware of any requirement to notify security incidents under other associated legislation that may apply to them and whether this may also require them to notify the supervisory authority of a personal data breach at the same time. Such requirements can vary between Member States, but examples of notification requirements in other legal instruments, and how these inter-relate with the GDPR, include the following:

- Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)[49].

Article 19(2) of the eIDAS Regulation requires trust service providers to notify their supervisory body of a breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where applicable—i.e., where such a breach or loss is also a personal data breach under the GDPR—the trust service provider should also notify the supervisory authority.

- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)[50].

Articles 14 and 16 of the NIS Directive require operators of essential services and digital service providers to notify security incidents to their competent authority. As recognised by Recital 63 of NIS[51], security incidents can often include a compromise of personal data. Whilst NIS requires competent authorities and supervisory authorities to co-operate and exchange information that context, it remains the case that where such incidents are, or become, personal data breaches under the

[49] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[50] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

51 Recital 63: *"Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents."*

GDPR, those operators and/or providers would be required to notify the supervisory authority separately from the incident notification requirements of NIS.

Example

A cloud service provider notifying a breach under the NIS Directive may also need to notify a controller, if this includes a personal data breach. Similarly, a trust service provider notifying under eIDAS may also be required to notify the relevant data protection authority in the event of a breach.

- Directive 2009/136/EC (the Citizens' Rights Directive) and Regulation 611/2013 (the Breach Notification Regulation).

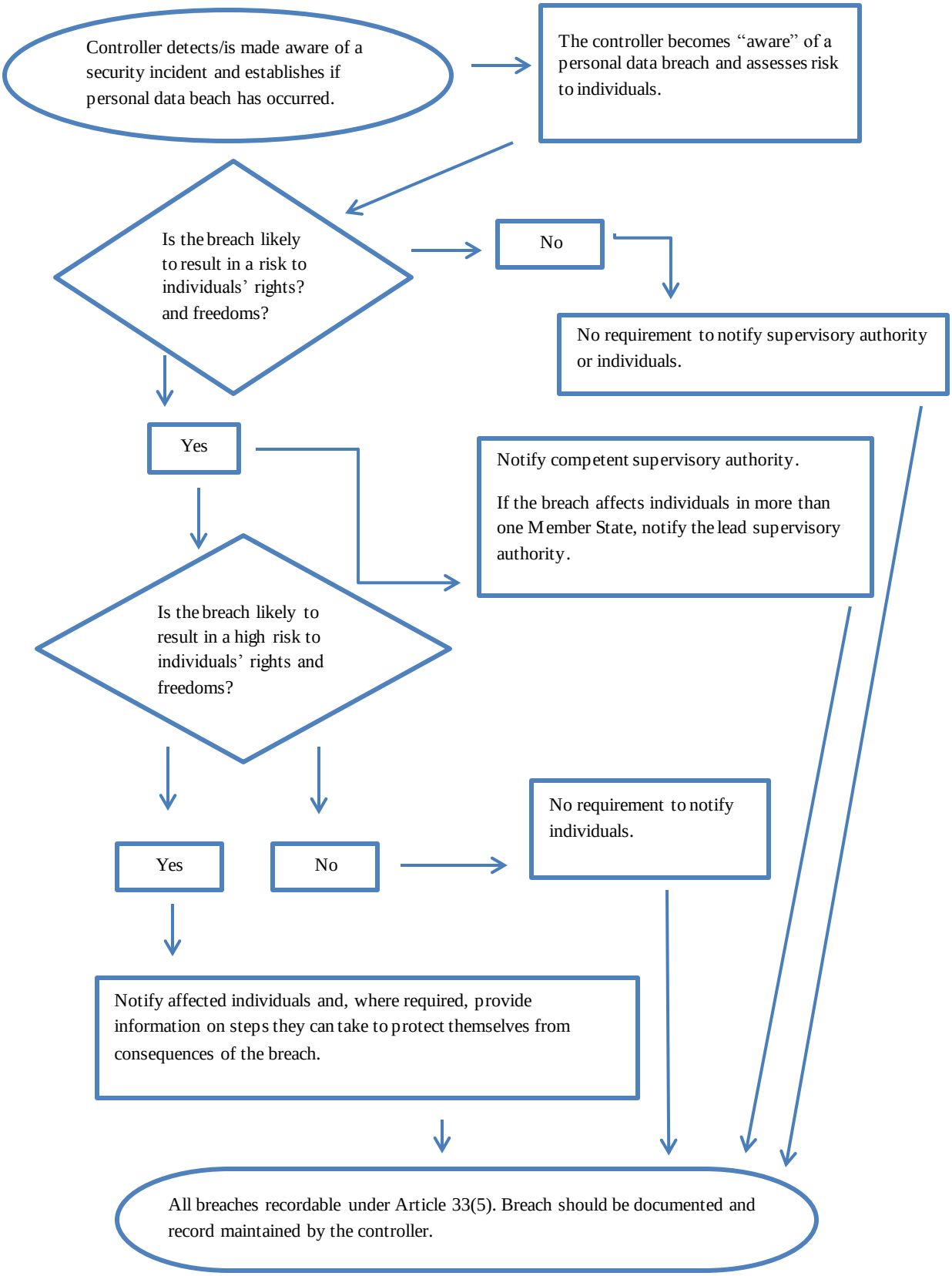
Providers of publicly available electronic communication services within the context of Directive 2002/58/EC[52] must notify breaches to the competent national authorities.

Controllers should also be aware of any additional legal, medical, or professional notification duties under other applicable regimes.

[52] On 10 January 2017, the European Commission proposed a Regulation on Privacy and Electronic Communications which will replace Directive 2009/136/EC and remove notification requirements. However, until this proposal is approved by the European Parliament the existing notification requirement remains in force, see https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

VII. **Annex**

A. Flowchart showing notification requirements



B. Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist controllers in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendations
i. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii. A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or

functionality was to encrypt the data, and that there was no other malware present in the system.		consequences.	confidentiality. However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.
v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
vi. A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross-border processing.	Yes, as could lead to high risk.	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider.
vii. A website hosting company acting as a data processor identifies an error in the code which	As the processor, the website hosting company must notify its affected clients (the controllers) without	If there is likely no high risk to the individuals they do not need to be	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS

controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	undue delay. Assuming that the website hosting company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.	notified.	Directive as a digital service provider). If there is no evidence of this vulnerability being exploited with any of its controllers a notifiable breach may not have occurred but it is likely to be recordable or be a matter of non-compliance under Article 32.
viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
ix. Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
x. A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

Anexo IV – Artigos 45.º, 46.º e 47.º do Regulamento (UE) 2016/679

Artigo 45.º
Transferências com base numa decisão de adequação

"*1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.*

2. Ao avaliar a adequação do nível de proteção, a Comissão tem nomeadamente em conta os seguintes elementos:

a) *O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência;*

b) *A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e*

c) *Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais.*

3. Após avaliar a adequação do nível de proteção, a Comissão pode decidir, através de um ato de execução, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, garante um nível de proteção adequado na aceção do n.º 2 do presente artigo. O ato de execução prevê um procedimento de avaliação periódica, no mínimo de quatro em quatro anos, que deverá ter em conta todos os desenvolvimentos pertinentes no país terceiro ou na organização internacional. O ato de execução especifica o âmbito de aplicação territorial e setorial e, se for caso disso, identifica a autoridade ou autoridades de controlo a que se refere o n.º 2, alínea b), do presente artigo. O referido ato de execução é adotado pelo procedimento de exame a que se refere o artigo 93.º, n.º 2.

4. A Comissão controla, de forma continuada, os desenvolvimentos nos países terceiros e nas organizações internacionais que possam afetar o funcionamento das decisões adotadas nos termos do n.º 3 do presente artigo e das decisões adotadas com base no artigo 25.º, n.º 6, da Diretiva 95/46/CE.

5. A Comissão, sempre que a informação disponível revelar, nomeadamente na sequência da revisão a que se refere o n.º 3 do presente artigo, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, deixou de assegurar um nível de proteção adequado na aceção do n.º 2 do presente artigo, na medida do necessário, revoga, altera ou suspende a decisão referida no n.º 3 do presente artigo, através de atos de execução, sem efeitos retroativos. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.º, n.º 2. Por imperativos de urgência devidamente justificados, a Comissão adota atos de execução imediatamente aplicáveis pelo procedimento a que se refere o artigo 93.º, n.º 3.

6. A Comissão inicia consultas com o país terceiro ou a organização internacional com vista a corrigir a situação que tiver dado origem à decisão tomada nos termos do n.º 5.

7. As decisões tomadas ao abrigo do n.º 5 do presente artigo não prejudicam as transferências de dados pessoais para o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou para a organização internacional em causa, nos termos dos artigos 46.º a 49.º.

8. A Comissão publica no Jornal Oficial da União Europeia e no seu sítio web uma lista dos países terceiros, territórios e setores específicos de um país terceiro e de organizações internacionais relativamente aos quais tenha declarado, mediante decisão, se asseguram ou não um nível de proteção adequado.

9. As decisões adotadas pela Comissão com base no artigo 25.o, n.º 6, da Diretiva 95/46/CE permanecem em vigor até que sejam alteradas, substituídas ou revogadas por uma decisão da Comissão adotada em conformidade com o n.º 3 ou o n.º 5 do presente artigo.".

Artigo 46.º

Transferências sujeitas a garantias adequadas

"*1. Não tendo sido tomada qualquer decisão nos termos do artigo 45.º, n.º 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.*

2. Podem ser previstas as garantias adequadas referidas no n.º 1, sem requerer nenhuma autorização específica de uma autoridade de controlo, por meio de:

a) *Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos;*

b) *Regras vinculativas aplicáveis às empresas em conformidade com o artigo 47.º;*

c) *Cláusulas-tipo de proteção de dados adotadas pela Comissão pelo procedimento de exame referido no artigo 93.º, n.º 2;*

d) *Cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão pelo procedimento de exame referido no artigo 93.º, n.º 2;*

e) *Um código de conduta, aprovado nos termos do artigo 40.º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados; ou*

f) *Um procedimento de certificação, aprovado nos termos do artigo 42.º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados.*

3. Sob reserva de autorização da autoridade de controlo competente, podem também ser previstas as garantias
adequadas referidas no n.º 1, nomeadamente por meio de:

a) *Cláusulas contratuais entre os responsáveis pelo tratamento ou subcontratantes e os responsáveis pelo tratamento, subcontratantes ou destinatários dos dados pessoais no país terceiro ou organização internacional; ou*

b) *Disposições a inserir nos acordos administrativos entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados.*

4. A autoridade de controlo aplica o procedimento de controlo da coerência a que se refere o artigo 63.º nos casos enunciados no n.º 3 do presente artigo.

5. As autorizações concedidas por um Estado-Membro ou uma autoridade de controlo com base no artigo 26.º, n.º 2, da Diretiva 95/46/CE continuam válidas até que a mesma autoridade de controlo as altere, substitua ou revogue, caso seja necessário. As decisões adotadas pela Comissão com base no artigo 26.º, n.º 4, da Diretiva 95/46/CE permanecem em vigor até que sejam alteradas, substituídas ou revogadas, caso seja necessário, por uma decisão da Comissão adotada em conformidade com o n.º 2 do presente artigo.".

Artigo 47.º
Regras vinculativas aplicáveis às empresas

"*1. Pelo procedimento de controlo da coerência previsto no artigo 63.º, a autoridade de controlo competente aprova regras vinculativas aplicáveis às empresas, que devem:*

a) *Ser juridicamente vinculativas e aplicáveis a todas as entidades em causa do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, incluindo os seus funcionários, as quais deverão assegurar o seu cumprimento;*

b) *Conferir expressamente aos titulares dos dados direitos oponíveis relativamente ao tratamento dos seus dados pessoais; e*

c) *Preencher os requisitos estabelecidos no n.º 2.*

2. As regras vinculativas aplicáveis às empresas a que se refere o n.º 1 especificam, pelo menos:

a) *A estrutura e os contactos do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta e de cada uma das entidades que o compõe;*

b) *As transferências ou conjunto de transferências de dados, incluindo as categorias de dados pessoais, o tipo de tratamento e suas finalidades, o tipo de titulares de dados afetados e a identificação do país ou países terceiros em questão;*

c) *O seu caráter juridicamente vinculativo, a nível interno e externo;*

d) *A aplicação dos princípios gerais de proteção de dados, nomeadamente a limitação das finalidades, a minimização dos dados, a limitação dos prazos de conservação, a qualidade dos dados, a proteção dos dados desde a conceção e por defeito, o fundamento jurídico para o tratamento, o tratamento de categorias especiais de dados pessoais, as medidas de garantia da segurança dos dados e os requisitos aplicáveis a transferências posteriores para organismos não abrangidos pelas regras vinculativas aplicáveis às empresas;*

e) *Os direitos dos titulares dos dados relativamente ao tratamento e regras de exercício desses direitos, incluindo o direito de não ser objeto de decisões baseadas unicamente no tratamento automatizado, nomeadamente a definição de perfis a que se refere o artigo 22.º, o direito de apresentar uma reclamação à autoridade de controlo competente e aos tribunais competentes dos Estados-Membros nos termos do artigo 79.º, bem como o de obter reparação e, se for caso disso, indemnização pela violação das regras vinculativas aplicáveis às empresas;*

f) *A aceitação, por parte do responsável pelo tratamento ou subcontratante estabelecido no território de um Estado-Membro, da responsabilidade por toda e qualquer violação das regras vinculativas aplicáveis às empresas cometida por uma entidade envolvida que não se encontre estabelecida na União; o responsável pelo tratamento ou o subcontratante só pode ser exonerado dessa responsabilidade, no todo ou em parte, mediante prova de que o facto que causou o dano não é imputável à referida entidade;*

g) *A forma como as informações sobre as regras vinculativas aplicáveis às empresas, nomeadamente, sobre as disposições referidas nas alíneas d), e) e f) do presente número,*

são comunicadas aos titulares dos dados para além das informações referidas nos artigos 13.º e 14.º;

h) *As funções de qualquer encarregado da proteção de dados, designado nos termos do artigo 37.º ou de qualquer outra pessoa ou entidade responsável pelo controlo do cumprimento das regras vinculativas aplicáveis às empresas, a nível do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, e pela supervisão das ações de formação e do tratamento de reclamações;*

i) *Os procedimentos de reclamação;*

j) *Os procedimentos existentes no grupo empresarial ou no grupo de empresas envolvidas numa atividade económica conjunta para assegurar a verificação do cumprimento das regras vinculativas aplicáveis às empresas. Esses procedimentos incluem a realização de auditorias sobre a proteção de dados e o recurso a métodos que garantam a adoção de medidas corretivas capazes de preservar os direitos dos respetivos titulares. Os resultados dessa verificação devem ser comunicados à pessoa ou entidade referida na alínea h) e ao Conselho de Administração da empresa ou grupo empresarial que exerce o controlo ou do grupo de empresas envolvidas numa atividade económica conjunta, devendo também ser facultados à autoridade de controlo competente, a pedido desta;*

k) *Os procedimentos de elaboração de relatórios e de registo de alterações às regras, bem como de comunicação dessas alterações à autoridade de controlo;*

l) *O procedimento de cooperação com a autoridade de controlo para assegurar o cumprimento, por qualquer entidade do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, em especial facultando à autoridade de controlo os resultados de verificações das medidas referidas na alínea j);*

m) *Os procedimentos de comunicação, à autoridade de controlo competente, de todos os requisitos legais a que uma entidade do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta esteja sujeita num país terceiro que sejam passíveis de ter forte impacto negativo nas garantias dadas pelas regras vinculativas aplicáveis às empresas; e*

n) *Ações de formação especificamente dirigidas a pessoas que tenham, em permanência ou regularmente, acesso a dados de natureza pessoal.*

3. A Comissão pode especificar o formato e os procedimentos de intercâmbio de informações entre os responsáveis pelo tratamento, os subcontratantes e as autoridades de controlo no que respeita às regras vinculativas aplicáveis às empresas na aceção do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.º, n.º 2.".