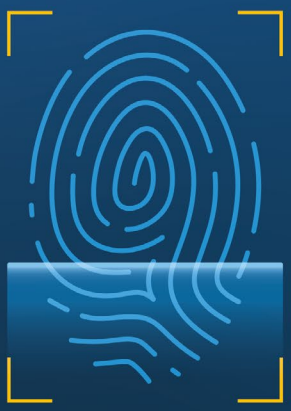


CAIXA GERAL DE DEPÓSITOS

GUIA DA PROTEÇÃO DE DADOS

MAIO 2025

CONCEITOS

PRINCÍPIOS RELATIVOS AO TRATAMENTO DE DADOS PESSOAIS

DEVER DE INFORMAÇÃO

EXERCÍCIO DE DIREITOS

CONSENTIMENTO

COOKIES

SUBCONTRATANTE

REGISTO DE ATIVIDADES DE TRATAMENTO

PROTEÇÃO DE DADOS DESDE A CONCEÇÃO E POR DEFEITO

AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

VIOLAÇÕES DE DADOS

TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

RESPONSABILIDADE CONTRAORDENACIONAL

RESPONSABILIDADE CRIMINAL

AUTORIDADE DE SUPERVISÃO

DATA PROTECTION OFFICER

ELEMENTOS DE APOIO

ENQUADRAMENTO

O 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 (doravante RGPD), aplica-se plenamente desde 25 de maio de 2018 em todos os Estados-Membros da União Europeia (UE).

O RGPD concretiza e desenvolve o direito fundamental das pessoas (singulares) à proteção dos dados de caráter pessoal que lhes digam respeito, consagrado no artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da UE e no artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da UE, bem como no artigo 35.º da Constituição da República Portuguesa.

Trata-se, em suma, da garantia e da tutela do direito de qualquer pessoa singular a que toda a informação que lhe diga respeito, identificando-a ou tornando-a identificável, possa apenas ser objeto de tratamento leal, para finalidades determinadas, limitado ao mínimo necessário e com base no seu consentimento ou noutro fundamento de licitude previsto no RGPD.

A tutela dos Titulares dos Dados implica, em contrapartida, um conjunto de obrigações a cargo do Responsável pelo Tratamento dos dados, *in casu*, a Caixa Geral de Depósitos (doravante CGD).

A Lei n.º 58/2019, de 8 de agosto, complementa o RGPD, assegurando a sua execução, na ordem jurídica nacional, e consagra, entre outros aspetos relevantes, a responsabilidade criminal em matéria de proteção de dados, incluindo das pessoas coletivas, enquanto Responsáveis pelo Tratamento e/ou Subcontratantes.

Com base no enquadramento regulatório acima referido, a CGD definiu a sua Política de Privacidade e Proteção de Dados Pessoais, acessível em permanência em www.cgd.pt, e um conjunto de normativos internos com vista a atualizar as orientações e os procedimentos destinados a operacionalizar, na CGD, o cumprimento das obrigações impostas pelo quadro legal e modelo institucional de supervisão em matéria de proteção de dados.

A atualização do *Guia da Proteção de Dados*, através da sua 2.ª edição que agora se publicita, teve como propósito servir de ferramenta de trabalho e de consulta rápida, simples e direta por qualquer Colaborador da CGD, para garantir o cumprimento da legislação e dos normativos internos sobre proteção de dados, a conformidade dos tratamentos de dados pessoais a que a CGD procede e contribuir para a cultura organizacional de conformidade sobre proteção de dados.

O *Guia da Proteção de Dados* (2.ª edição) é de cumprimento obrigatório pelos Colaboradores da CGD, pelo que o incumprimento ou violação das obrigações e regras nele definidas implica responsabilidade jurídica, à semelhança do que sucede com os demais normativos internos vigentes na CGD.

A divulgação da 2.ª edição do *Guia da Proteção de Dados* assinala também o 7.º aniversário da vigência plena do RGPD (em 25.05.2025) e renova o compromisso da CGD com a cultura organizacional de conformidade sobre proteção de dados.

Cristina Máximo dos Santos
Data Protection Officer

OBJETO

O Guia da Proteção de Dados condensa as regras legais e normativos internos, estabelece as orientações e os procedimentos adotados na CGD, incluindo as competências e responsabilidades de todos e cada um dos Colaboradores para dar cumprimento às obrigações em matéria de proteção de dados.

Trata-se de um instrumento de trabalho, de fácil consulta, com uma abordagem pragmática e simplificada, através da metodologia de 171 Perguntas – 171 Respostas, contendo exemplos práticos de situações concretas do dia a dia e indicação de outros documentos complementares para (quem quer) saber mais, visando apoiar os Colaboradores com intervenção ativa na proteção de dados pessoais, no desempenho das suas atividades.

001.
Quem é o Titular dos Dados?

O Titular dos Dados é a pessoa singular a quem os dados pessoais respeitam.

EXEMPLO

Pessoas singulares com quem a CGD interage no âmbito da sua atividade bancária (Clientes particulares e Empresários em Nome Individual, representantes de empresas e membros dos órgãos sociais); as pessoas singulares que, mediante contrato de trabalho ou equivalente, desempenham funções por conta e sob a subordinação jurídica da CGD (Colaboradores); as pessoas singulares que se tenham candidatado a qualquer tipo de função na CGD, mediante o envio do correspondente *curriculum vitae* (candidatos); visitantes, etc.

002.
O que são dados pessoais?

Dados pessoais são toda a informação relativa a uma pessoa singular que a identifique ou permita identificar, tais como:

- Nome;
- Número de identificação civil;
- Endereço de correio eletrónico;
- Número de telefone/telemóvel;
- IBAN;
- Matrícula de um veículo;
- Dados de localização;
- Identificadores por via eletrónica;
- Elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Não são dados pessoais, por exemplo:

- Número de registo de uma empresa;
- Endereço de correio eletrónico genérico: info@cgd.pt; geral@cgd.pt;
- Dados anonimizados.

003.
Quando se considera uma pessoa identificável?

Uma pessoa é considerada identificável quando possa ser identificada, direta ou indiretamente, com recurso a informação adicional.
As pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (*Internet Protocol*) ou testemunhos de conexão (*cookie*) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares.

EXEMPLO

Morada associada à ocupação profissional num determinado universo de pessoas; nível de rendimento associado à idade e ao género de uma pessoa.

004.
A CGD utiliza listas de categorias de dados pessoais?

A CGD utiliza uma lista de macro categorias de dados pessoais, para efeito de uniformização de conceitos relativos ao tratamento de dados pessoais a realizar pelas diferentes Direções ou Órgãos de Estrutura. Esta lista pode ser atualizada por iniciativa da(o) *Data Protection Officer* ou mediante pedido das Direções.

EXEMPLO

As macro categorias de dados pessoais respeitam a:

- "**Informação de Identidade e caraterização**" (dados necessários para o processamento de informação de cliente e não cliente relativo a documentos de identificação e correspondência; dados que permitam identificar o Titular dos Dados no seu contexto profissional; informação necessária para realizar o processo de habilitação de herdeiros do cliente em cumprimento das obrigações legais em vigor);
- "**Informação patrimonial**" (informação caracterizadora sobre os bens, imóveis e/ou móveis, que servem de garantia das responsabilidades de crédito; informação sobre responsabilidades de crédito e garantias para efeitos de realização da avaliação de risco de crédito);
- "**Informação transacional**" [dados necessários para a realização de débitos diretos, pagamentos e transferências (SEPA, MBWAY); dados necessários para a realização de compra e venda de moeda estrangeira];
- "**Informação de *compliance***" (dados relevantes do ponto de vista de análise do grau de risco do Titular dos Dados ao nível do branqueamento de capitais e financiamento do terrorismo);
- "**Informação comportamental**" [informação relativa às preferências do Titular dos Dados, tais como preferências de consumo e sociais; informação relativa aos dados de conexão (endereço IP, *cookies*, *logs*) recolhidos no âmbito da navegação *web*/*mobile* que o cliente efetua nos *sites* de internet ou aplicações móveis]; e
- "**Informação profissional**" (informação associada ao processamento salarial de Colaboradores).

005.
O que são categorias especiais de dados?

São categorias especiais de dados os dados pessoais constantes do respetivo catálogo previsto no RGPD, cujo tratamento beneficia de garantias reforçadas e englobam os dados que revelam:

- Origem racial ou étnica;
- Opiniões políticas;
- Convicções religiosas ou filosóficas;
- Filiação sindical;
- Dados genéticos;
- Dados biométricos que identifiquem uma pessoa de forma inequívoca;
- Dados relativos à saúde; ou,
- Dados relativos à vida sexual ou orientação sexual de uma pessoa.

006.
O que se entende por dados genéticos?

São os dados pessoais relativos às caraterísticas genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisionomia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa.

007.
O que são dados biométricos?

São os dados pessoais resultantes de um tratamento técnico específico relativo às caraterísticas físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos (identificação humana por meio de impressões digitais).

008.
O que são dados relativos à saúde?

São os dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde.

009.
O que se entende por tratamento de dados?

Considera-se tratamento de dados toda a operação ou conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados, tais como o acesso, a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

EXEMPLO

Processamento salarial; registo de tempos de trabalho; recolha de dados pessoais em ação inspetiva; destruição de documentos que contenham dados pessoais; registo de imagem, incluindo por sistema de videovigilância.

010.
Quem é o Responsável pelo Tratamento?

O Responsável pelo Tratamento é a pessoa singular ou coletiva (por regra, a CGD) que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais.

EXEMPLO

A CGD, quando determina quais os dados necessários para tratar, os meios utilizados para o efeito e a finalidade do tratamento no âmbito de uma campanha de lançamento de um novo produto comercial; quando trata dados pessoais para recrutamento de Colaboradores; quando trata dados para efeito de registo de formação de Colaboradores.

011.
Quem são os Responsáveis Conjuntos pelo Tratamento?

Verifica-se uma situação de responsabilidade conjunta pelo tratamento de dados pessoais, quando dois ou mais Responsáveis pelo Tratamento determinem conjuntamente as finalidades e os meios desse tratamento, sendo, por conseguinte, ambos Responsáveis pelo Tratamento. Estes determinam, por acordo entre si e de modo transparente as respetivas responsabilidades pelo cumprimento do RGPD, nomeadamente no que diz respeito ao exercício dos direitos do Titular dos Dados.
O referido acordo pode designar um ponto de contacto para os Titulares dos Dados e os principais aspetos desse acordo devem ser comunicados às pessoas singulares cujos dados pessoais sejam objeto de tratamento.

EXEMPLO

A CGD é Responsável Conjunto pelo Tratamento quando determina, em conjunto com uma ou mais organizações, quais as finalidades e os meios de tratamento de dados pessoais. Seria o caso, por exemplo, se no âmbito de uma parceria comercial, as empresas decidissem utilizar uma plataforma comum e partilhassem os nomes de clientes (pessoas singulares), para fins comerciais complementares. Nesta medida, as empresas intervenientes são Responsáveis Conjuntas pelo Tratamento, não só porque concordaram em oferecer a possibilidade de "serviços combinados", como também conceberam e utilizam uma plataforma comum.

012.
Quem é Subcontratante?

O Subcontratante é a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que trate os dados pessoais por conta do Responsável pelo Tratamento. O Subcontratante trata os dados pessoais em nome e representação do Responsável pelo Tratamento, observando as instruções documentadas que lhe sejam transmitidas pelo Responsável pelo Tratamento.

EXEMPLO

O prestador de serviços contratado pela CGD para armazenamento em *cloud* de informação contendo dados pessoais ou a situação em que a CGD contrata uma parceria com uma grande distribuidora do ramo alimentar em cujo âmbito são estabelecidas operações de tratamento de dados pessoais em regime de subcontratação.

013.
Em que consiste o consentimento?

O consentimento é uma manifestação de vontade, livre, específica, informada e inequívoca, pela qual o Titular dos Dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

EXEMPLO

Os clientes prestam consentimento para a CGD lhes enviar comunicações de cariz comercial publicitando novos produtos ou serviços; os Colaboradores prestam o consentimento para o tratamento da sua imagem para fins institucionais, nomeadamente no âmbito da publicação e divulgação de *newsletters* internas e externas, cartazes ou folhetos informativos da CGD.

014.
Em que consiste a Definição de perfis?

A Definição de perfis diz respeito a qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com:

- o seu desempenho profissional;
- a sua situação económica;
- a sua saúde;
- as suas preferências pessoais;
- os seus interesses;
- a sua fiabilidade;
- o seu comportamento;
- a sua localização; ou
- as suas deslocações.

EXEMPLO

A CGD recolhe informação relativa à navegação *web* dos seus clientes, categorizando-a e criando perfis de consumo.
Os Titulares dos Dados são depois incluídos nas várias categorias. Essa informação é posteriormente aproveitada para campanhas de *marketing*.

SABER MAIS

Pode consultar, na "Página RGPD" do Somos Caixa, os seguintes documentos:
EDPB - Diretrizes 8/2020 sobre o direcionamento para os utilizadores das redes sociais

WP29 - Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679

015.
O que constitui uma violação de dados?

Uma violação de dados consiste numa violação da 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.

EXEMPLO

A atribuição de acessos indevidos à Plataforma de Balcão ou à Base de Dados de Clientes; ao cadastro individual de Colaboradores; aos registos de entrada e permanência nos edifícios da CGD; o acesso indevido (não motivado pelo exercício da função) a dados de clientes; a divulgação, sem consentimento do titular ou habilitação legal para o efeito, da informação relativa ao mapa da Central de Responsabilidades de Crédito (CRC); envio de *email* para endereço de correio eletrónico incorreto atribuído/pertencente a terceiro.

016.
O que são transferências internacionais de dados?

Consideram-se transferências internacionais de dados pessoais as que são realizadas para fora do Espaço Económico Europeu (EEE) e digam respeito a dados pessoais. Estão aqui incluídas as transferências de dados para Subcontratantes e também as realizadas para outros Responsáveis pelo Tratamento.

EXEMPLO

A CGD contrata a prestação de servços *cloud* para armazenamento de informação contendo dados pessoais de clientes; a CGD utiliza redes sociais para nelas marcar presença e difundir a sua imagem e atividade; a CGD contrata a prestação de serviços tecnológicos inovadores (biometria, reconhecimento de voz, reconhecimento de texto, conexão de dados e perfilagem, entre outras); a CGD contrata a prestação de serviços de computação a empresas cujos servidores não são propriedade da CGD; a CGD procede ao envio de dados pessoais de clientes para cumprimento de obrigações legais perante autoridades (judiciais, tributárias, outras) de países terceiros.

017.
O que é o Regulamento DORA?

Este Regulamento estabelece regras uniformes sobre a segurança das redes e dos sistemas de informação das entidades financeiras, tais como bancos, companhias de seguros e empresas de investimento estabelecidas na União Europeia, exigindo-lhes que resistam, respondam e recuperem de qualquer perturbação ou ameaça no domínio das tecnologias da informação e da comunicação (TIC).

Estão abrangidas pelo Regulamento DORA:

- instituições de crédito, de pagamento, de moeda eletrónica e de pensões profissionais;
- prestadores de serviços de informação sobre contas, de criptoativos, de comunicação de dados, de financiamento colaborativo; bem como Terceiros prestadores de serviços de TIC;
- empresas de investimento, fundos de investimento alternativos, sociedades gestoras, agências de notação de crédito e administradores de índices de referência críticos;
- repositórios de transações e de titularização, centrais de valores mobiliários, contrapartes centrais e plataformas de negociação;
- empresas de seguros, mediadores de seguros e empresas de resseguros.

O Regulamento DORA impõe requisitos rigorosos para garantir a segurança das TIC, incluindo a proteção de dados pessoais.

SABER MAIS

Pode consultar o **Regulamento (UE) 2022/2554** do Parlamento Europeu e do Conselho, de 14.12.2022, **relativo à resiliência operacional digital do setor financeiro**
https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2554

018.
O que é a Inteligência Artificial (IA)?

A IA é uma família de tecnologias em rápida evolução que contribui para um vasto conjunto de benefícios económicos, ambientais e sociais em todo o leque de indústrias e atividades sociais. Ao melhorar as previsões, otimizar as operações e a repartição de recursos e personalizar as soluções digitais disponibilizadas às pessoas e às organizações, a utilização da IA pode conferir importantes vantagens competitivas às empresas e contribuir para progressos sociais e ambientais. Em função das circunstâncias relativas à sua aplicação, utilização e nível de evolução tecnológica

específicos, a IA pode criar riscos e prejudicar interesses públicos e direitos fundamentais protegidos pela legislação aplicável, causando prejuízos materiais ou imateriais, incluindo danos físicos, psicológicos, sociais ou económicos.
Como condição prévia, a IA deverá ser uma tecnologia centrada no ser humano. Deverá servir de instrumento para as pessoas, com o objetivo último de aumentar o bem-estar humano.
O direito fundamental à proteção de dados pessoais e a vida privada e a confidencialidade das comunicações estão salvaguardados e são pilares básicos que os sistemas de IA devem observar.
Os Titulares dos Dados continuam a usufruir de todos os direitos e garantias que lhes são conferidos por Regime Geral sobre a Proteção de Dados, incluindo os direitos relacionados com as decisões individuais exclusivamente automatizadas, nomeadamente a Definição de perfis.

SABER MAIS

Pode consultar o **Regulamento (UE) 2024/1689** do Parlamento Europeu e do Conselho, de 13.06.2024, **cria regras harmonizadas em matéria de Inteligência Artificial**, que define, entre outros aspetos: Práticas de IA proibidas; Sistemas de IA de risco elevado; Obrigações de transparência aplicáveis aos prestadores e responsáveis pela implementação de determinados sistemas de IA; Modelos de IA de finalidade geral.
https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ:L_202401689

019.
Quais os princípios a que deve obedecer qualquer tratamento de dados pessoais?

Qualquer tratamento deve ser:
- Lícito;
- Leal;
- Transparente;
- Ter finalidades determinadas;
- Limitado ao mínimo de dados necessários para a finalidade que determinou a recolha;
- Exato (isto é, tratar dados pessoais atualizados em cada momento);
- Garantir a integridade, disponibilidade e confidencialidade dos dados; e
- Documentado e gerador das evidências que comprovem que o Responsável pelo Tratamento cumpriu os requisitos de conformidade do tratamento.

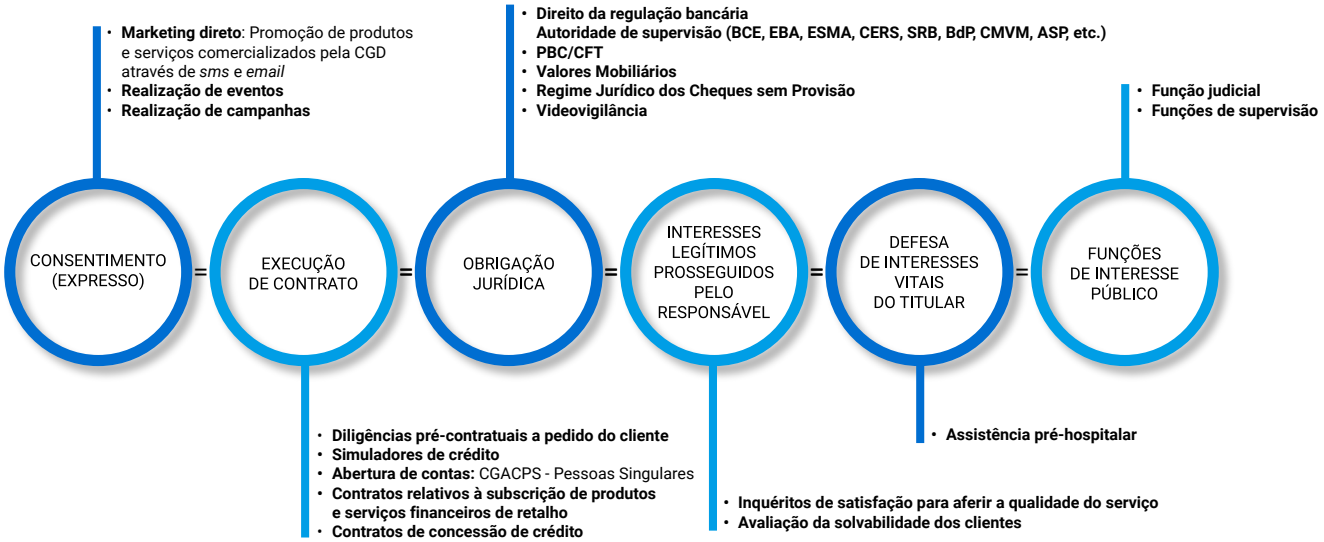
020.
Em que casos é lícito o tratamento de dados pessoais?

O tratamento é lícito sempre que necessário para:
- A celebração e/ou execução de um contrato (por exemplo, contratos de trabalho e/ou de prestação de serviços);
- O cumprimento de obrigações legais (por exemplo, obrigações fiscais e contributivas);
- A defesa de interesses vitais do Titular dos Dados ou de terceiros (por exemplo, disponibilização de informação de saúde necessária à prestação de cuidados vitais ao Colaborador);
- O exercício de funções de interesse público ou de autoridade pública (por exemplo, exercício da função judicial ou o exercício de funções de supervisão);
- Os interesses legítimos do Responsável pelo Tratamento ou de terceiros (por exemplo,

realização de inquéritos de satisfação para aferir a qualidade do serviço prestado); ou,

- Sempre que exista consentimento do Titular dos Dados (por exemplo, para envio de comunicações sobre produtos e serviços comercializados pela CGD; para realização de campanhas comerciais; realização de eventos; gravação de som e imagem de Colaborador, nos casos não abrangidos no respetivo contrato de trabalho).

Licitude dos tratamentos



021.
A CGD pode tratar dados pessoais com base nos seus "interesses legítimos"?

A CGD trata dados pessoais para prossecução dos "interesses legítimos". A CGD, enquanto Responsável pelo Tratamento, pode tratar dados pessoais quando tal seja necessário para a prossecução dos seus interesses legítimos, assegurando previamente o teste de ponderação/prevalência dos interesses em presença. Em todo o caso, nas situações conexas ou complementares às atribuições da CGD (por exemplo, realização de uma conferência), o tratamento de dados pessoais com base nesse fundamento pode ser utilizado mediante parecer da(o) *Data Protection Officer*.

SABER MAIS

Pode consultar, na "Página RGPD" do Somos Caixa, o seguinte documento:
EDPB - *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*

022.
A quem incumbe determinar a finalidade do tratamento de dados?

A finalidade do tratamento de dados é definida pela Direção que recolhe ou trata a informação no âmbito das suas competências.
Todavia, sempre que se preveja a necessidade de se tratarem os dados pessoais para outras finalidades (por exemplo, da competência da

mesma ou de outras Direções ou Entidades do Grupo), devem indicar-se, desde logo, essas finalidades aquando da recolha.

023.
Os dados recolhidos podem ser tratados para finalidade distinta daquela que determinou a recolha?

Sim, os dados recolhidos podem ser tratados para finalidade distinta daquela que determinou a recolha, sempre que haja consentimento do Titular dos Dados ou outro fundamento legal para o efeito. Nos demais casos, deve proceder-se a um juízo casuístico de compatibilidade, que deve ponderar, nomeadamente, os seguintes fatores:

- Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
- O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os Titulares dos Dados e o Responsável pelo Tratamento;
- A natureza dos dados pessoais, em especial se as categorias especiais de pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.º do RGPD;
- 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.

024.
A quem incumbe esse juízo?

Esse juízo casuístico de compatibilidade incumbe às Direções, obtido o parecer da(o) *Data Protection Officer*.

025.
Quais as finalidades de tratamento de dados pessoais da CGD?

A Lista de Finalidades de tratamento da CGD estabilizada e em uso foi elaborada com base nas Autorizações concedidas à CGD pela CNPD e que, em geral, mantêm a sua validade. Esta Lista pode ser atualizada, nomeadamente em função de novas finalidades associadas a novos tratamentos a que a CGD venha a proceder.

026.
Quem define o prazo de conservação dos dados pessoais?

O prazo de conservação dos dados pessoais é definido pela Direção que recolhe os dados pessoais e, sempre que os dados sejam objeto de tratamento para finalidade distinta daquela que determinou a recolha, pelas Direções responsáveis pelo tratamento.

SABER MAIS

Pode consultar os seguintes documentos:
Manual de Procedimentos (MP) 45/2020 – Procedimentos de Gestão Documental: Arquivo Físico e Digital

Lei n.º 75/2021, de 18 de novembro - consagra o direito ao esquecimento de pessoas que tenham superado ou mitigado situações de risco agravado de saúde ou de deficiência, tendo em vista melhorar o acesso ao crédito e a contratos de seguro destas pessoas.

Norma Regulamentar da Autoridade de Supervisão de Seguros e Fundos de Pensões n.º 12/2024-R - Esta norma tem por objeto (a) regular a operacionalização do dever de não recolha ou tratamento, pelos seguradores, da informação de saúde relativa à situação médica que originou o risco agravado de saúde ou a deficiência, nos termos da Lei n.º 75/2021; (b) detalhar o sentido e a extensão das práticas previstas no art.15.º n.ºs 2, 3 e 10, do regime jurídico do contrato de seguro (RJCS) aprovado

pelo Decreto-Lei n.º 72/2008, de 16 de abril, bem como dos fatores de risco a considerar e (c) e definir parâmetros para operacionalização do mecanismo de proteção de cobertura previsto no art. 217.º do RJCS.

027.
Qual o critério para a definição do prazo de conservação?

Sempre que haja prazo legal para conservação dos dados, deve ser este o aplicado. Nos restantes casos, a Direção deve conservar os dados pessoais apenas enquanto se mantiver a necessidade que determinou a sua recolha.

028.
Como assegurar que o tratamento garante a confidencialidade, a integridade e a disponibilidade dos dados?

Para assegurar a confidencialidade, a integridade e a disponibilidade dos dados, deve ser cumprido o disposto nas regras e orientações em matéria de segurança da informação emanadas pela CGD e nas orientações, recomendações e pareceres da(o) *Data Protection Officer*.

029.
Que mais se deve assegurar?

Deve ainda, pelo menos, garantir-se:
- A existência de um acordo de tratamento de dados com a outra parte, se aplicável; e
- Se o tratamento em causa já consta do registo de atividades de tratamento ou, pelo contrário, deve ser inscrito em tal registo.

030.
O que são medidas técnicas e organizativas (adequadas)?

Trata-se das medidas de cariz técnico e organizativo adotadas pelo Responsável pelo Tratamento (e pelo Subcontratante) que sejam adequadas para assegurar um nível de segurança adequado ao risco, 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.

EXEMPLO

Pseudonimização; cifragem; capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e serviços de tratamento, capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada em caso de incidente físico ou técnico; processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento dos dados, instruções documentadas para o tratamento de dados, classificação da informação.

SABER MAIS

No âmbito da Subcontratação, pode consultar o seguinte documento:
OS CGD 10/2025 - Política de Subcontratação do Grupo CGD

031.
O que é a pseudonimização?

Trata-se de uma forma de tratamento de dados pessoais através da qual deixam de poder ser atribuídos a um Titular dos Dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

032.
Em que consiste a anonimização?

A anonimização de dados pessoais é uma técnica de tratamento/processamento de dados que remove ou modifica informações que possam identificar uma pessoa. Essa técnica resulta em dados anonimizados, que não podem ser associados a nenhum indivíduo específico.

033.
Em que consiste a cifragem?

A cifragem consiste na codificação de mensagens para que apenas as pessoas autorizadas as possam ler.

034.
O tratamento de dados pessoais de pessoas falecidas obedece às mesmas regras?

O tratamento de dados pessoais de pessoas falecidas obedece aos mesmos princípios e regras do RGPD, sempre que os dados pessoais digam respeito a categorias especiais de dados a que se refere o n.º 1 do artigo 9.º do RGPD ou quando se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações.
Os direitos de acesso, retificação e apagamento relativos a dados pessoais de pessoas falecidas são exercidos pela pessoa designada para esse efeito pelo Titular dos Dados ou, na sua falta, pelos respetivos herdeiros. Os Titulares dos Dados falecidos podem, nos termos da legislação aplicável, determinar a impossibilidade de exercício dos direitos consagrados no RGPD após a sua morte.

035.
Quais são as consequências do incumprimento dos princípios de tratamento?

As consequências do incumprimento pelo Responsável pelo Tratamento (CGD) dos princípios relativos ao tratamento de dados pessoais, bem como as coimas aplicáveis, podem ser consultadas na secção “Responsabilidade contra-ordenacional” deste Guia.

SABER MAIS

Pode consultar, na “Página RGPD” do Somos Caixa, os seguintes documentos:
EDPB – *Guidelines 1/2025 on Pseudoymisation*

ENISA - *Data Pseudonymisation: Advanced Techniques and Use Cases* (2021)

ENISA - *Pseudonymisation techniques and best practices* (2019)

CNPD Diretriz 1/2023 – Sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais

DEVER DE INFORMAÇÃO

036.
Em que consiste o dever de informação?

O dever de informação é a obrigação que recai sobre o Responsável pelo Tratamento de prestar um conjunto de informações ao Titular dos Dados sobre as caraterísticas do tratamento.

037.
A CGD tem Política de Privacidade?

A CGD divulga a sua Política de Privacidade e Proteção de Dados Pessoais no seu *site* institucional https://www.cgd.pt/Ajuda/Pages/Politica-Privacidade-Protecao-Dados-Pessoais.aspx.
O objetivo desta Política é o de comunicar, de forma transparente, a todos os que contactam com a CGD para que finalidades determinadas, explícitas e legítimas os seus dados pessoais são recolhidos e tratados, a cada momento da relação comercial estabelecida entre a CGD e o Cliente e outros Titulares dos Dados, informando igualmente sobre o fundamento de licitude dos tratamentos de dados pessoais que, nesse âmbito, a CGD tem necessidade de efetuar.

038.
Como se cumpre o dever de informação?

O dever de informação cumpre-se através das minutas submetidas pelas Direções à prévia aprovação da(o) *Data Protection Officer*, competindo-lhes a sua adaptação ao caso concreto.
Este dever é igualmente cumprido no âmbito das Condições Gerais de Abertura de Conta e Presta-

ção de Serviços, em especial na Cláusula relativa aos Dados pessoais, que informa sobre os dados pessoais, as finalidades e fundamentos de licitude dos tratamentos de dados a que a CGD procede no exercício da sua atividade.
Em toda a documentação legal de suporte à atividade bancária e à prestação de serviços bancários celebrada com o Titular dos Dados é igualmente cumprido o dever de informação.

039.
Quando deve ser cumprido?

Nos casos em que a CGD recolha dados diretamente do titular, a informação é prestada em momento prévio à recolha. Nos casos em que a CGD recolha dados indiretamente (isto é, quando outrem lhos transmite), a informação deve ser prestada:

- Num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados;
- 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,
- Se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados.

040.
É necessário cumprir sempre esse dever?

A CGD apenas está desonerada de cumprir o dever de informação nas seguintes situações:
Nos casos de recolha direta:

a) Quando e na medida em que o Titular dos Dados já tiver conhecimento das informações;
b) Quando os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada pelo direito da União ou de um Estado-Membro, inclusive uma obrigação legal de confidencialidade; ou
c) Seja suscetível, atentas as circunstâncias do caso, de tornar impossível ou prejudicar gravemente os objetivos do tratamento e o interesse a prosseguir.

Nos casos de recolha indireta:
a) Quando e na medida em que o Titular dos Dados já tiver conhecimento das informações;
b) Quando a obtenção ou divulgação dos dados esteja expressamente prevista no direito da União ou do Estado-Membro ao qual o responsável pelo tratamento estiver sujeito, prevendo medidas adequadas para proteger os legítimos interesses do Titular dos Dados;
c) Quando os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada pelo direito da União ou de um Estado-Membro, inclusive uma obrigação legal de confidencialidade; ou,
d) Se comprove a impossibilidade de disponibilizar a informação ou que o esforço envolvido seja desproporcionado e na medida em que o cumprimento do dever de informação seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento.

Nos casos referidos na alínea c), nos casos de recolha direta, e na alínea d), nos casos de recolha indireta, a dispensa do cumprimento do dever de informação implica que a CGD tome medidas adequadas para defender os direitos, liberdades e interesses legítimos do Titular dos Dados, podendo para o efeito e se necessário obter o parecer da(o) *Data Protection Officer*.

041.
Quem determina as medidas adequadas?

As Direções responsáveis pelo tratamento, podendo, em caso de dúvida, solicitar o parecer da(o) *Data Protection Officer*.

042.
O não cumprimento, total ou parcial, do dever de informação tem de ser fundamentado?

Sim, o não cumprimento do dever de informação, mesmo que parcial, tem de ser fundamentado, tendo em vista a certeza da solução a adotar e a demonstração da justeza e da atendibilidade da mesma, se necessário, no âmbito da atividade inspetiva da Comissão Nacional de Proteção de Dados.

043.
A quem incumbe essa fundamentação?

Às Direções responsáveis pelo tratamento, podendo, em caso de dúvida, solicitar o parecer da(o) *Data Protection Officer*.

044.
Quais são as consequências do incumprimento do dever de informação?

As consequências do incumprimento pela CGD do dever de informação aos Titulares dos Dados, bem como as coimas aplicáveis, podem ser consultadas na secção "Responsabilidade contra-ordenacional" deste Guia.

SABER MAIS

Pode consultar, na "Página RGPD" do Somos Caixa, o seguinte documento:
WP29 - Orientações relativas à transparência na aceção do Regulamento 2016/679

045.
Quais são os direitos dos Titulares dos Dados?

O Titular dos Dados tem os direitos de acesso, retificação, portabilidade, oposição, limitação do tratamento, apagamento, a não ficar sujeito a qualquer decisão automatizada, reclamação e ação judicial.

Direito de acesso: permite ao Titular dos Dados confirmar junto da CGD se os seus dados pessoais estão a ser tratados. Se estiverem, o Titular dos Dados pode aceder-lhes e obter um conjunto de informações sobre a finalidade do tratamento, sobre os dados pessoais tratados, os destinatários a quem foram comunicados e o seu prazo de conservação.

Direito de retificação: permite ao Titular dos Dados exigir a correção dos seus dados pessoais, sem demora injustificada, que estejam incorretos ou incompletos.

Direito ao apagamento: atribui ao Titular dos Dados a possibilidade de exigir o apagamento dos seus dados, nomeadamente:

- Quando deixem de ser necessários para a finalidade que motivou o tratamento;
- Quando tenham sido tratados ilicitamente;
- Quando o titular retire o consentimento que legitima o tratamento dos dados e a lei o permita.

Direito à limitação do tratamento: possibilidade de o Titular dos Dados solicitar à CGD que limite o uso dos seus dados pessoais em determinadas situações.
O RGPD elenca os casos em que este direito pode ser exercido.

Direito de oposição: prerrogativa de o Titular dos Dados se opor, em determinadas circunstâncias, em qualquer momento, ao tratamento dos seus dados.

Direito de portabilidade: direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um Responsável pelo Tratamento, num formato estruturado, de uso corrente e de leitura automática, bem como o direito de transmitir esses dados a outro Responsável pelo Tratamento sempre que:

- O tratamento se basear no consentimento ou num contrato; e,
- O tratamento for realizado por meios automatizados.

Direito a não ficar sujeito a decisões individuais automatizadas: direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis.

Reclamação e ação judicial: Em qualquer caso, sempre que considere que o Responsável pelo Tratamento ou o Subcontratante violam o disposto no RGPD, o Titular dos Dados pode apresentar reclamação junto da Comissão Nacional de Proteção de Dados (CNPD) e/ou recorrer a ação judicial.

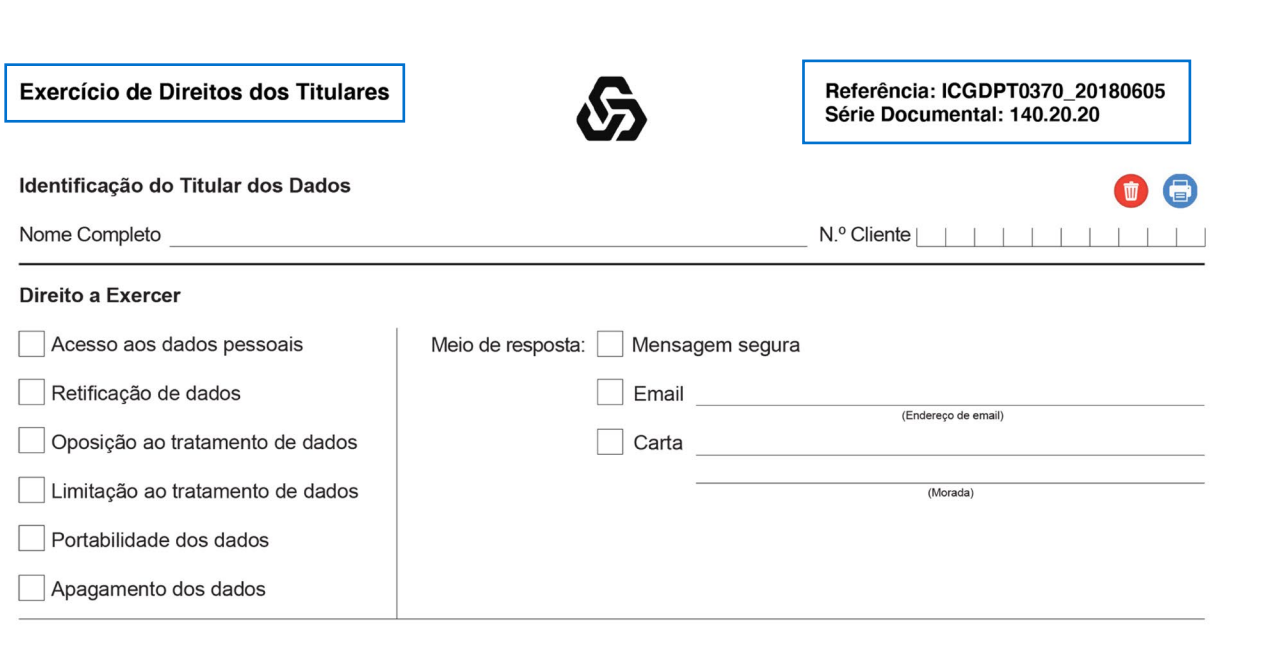
046.
Quem pode exercer esses direitos?

Por regra, o Titular dos Dados. Quando estejam em causa dados pessoais de menores de 13 (treze) anos, os titulares das responsabilidades parentais.
Relativamente a dados pessoais de pessoa falecida, sem prejuízo de a própria ter determinado a impossibilidade de exercício dos direitos após a sua morte, compete à pessoa a quem a pessoa falecida haja designado para o efeito ou, na sua falta, aos respetivos herdeiros.

047.
Como se exercem esses direitos?

Nos termos definidos no RGPD, o Responsável pelo Tratamento (CGD) deve assegurar resposta ao exercício dos direitos pelo Titular dos Dados. Os direitos dos Titulares dos Dados, nomeadamente o direito de acesso, o direito de retificação, o direito de oposição, o direito de limitação ao tratamento, o direito à portabilidade e o direito ao apagamento, podem ser exercidos pelos Titulares dos Dados mediante comunicação escrita dirigida à CGD:

1) impresso disponibilizado para o efeito - ICGDPT0370 "Exercício de Direitos dos Titulares" em qualquer Agência da Rede Comercial. Nesta situação o Colaborador deverá proceder ao preenchimento do impresso disponibilizado para o efeito - ICGDPT0370 "Exercício de Direitos dos Titulares";
2) formulário disponível no *site* da Caixa:
3) *email* enviado à Agência gestora (dirigido, de preferência, ao Gestor ou à Gerência);
4) carta (a enviar para qualquer Agência ou ao cuidado de *Data Protection Officer*, Avenida João XXI, n.º 63, 1000-300 Lisboa).



Exercício de Direitos dos Titulares

Referência: ICGDPT0370_20180605
Série Documental: 140.20.20

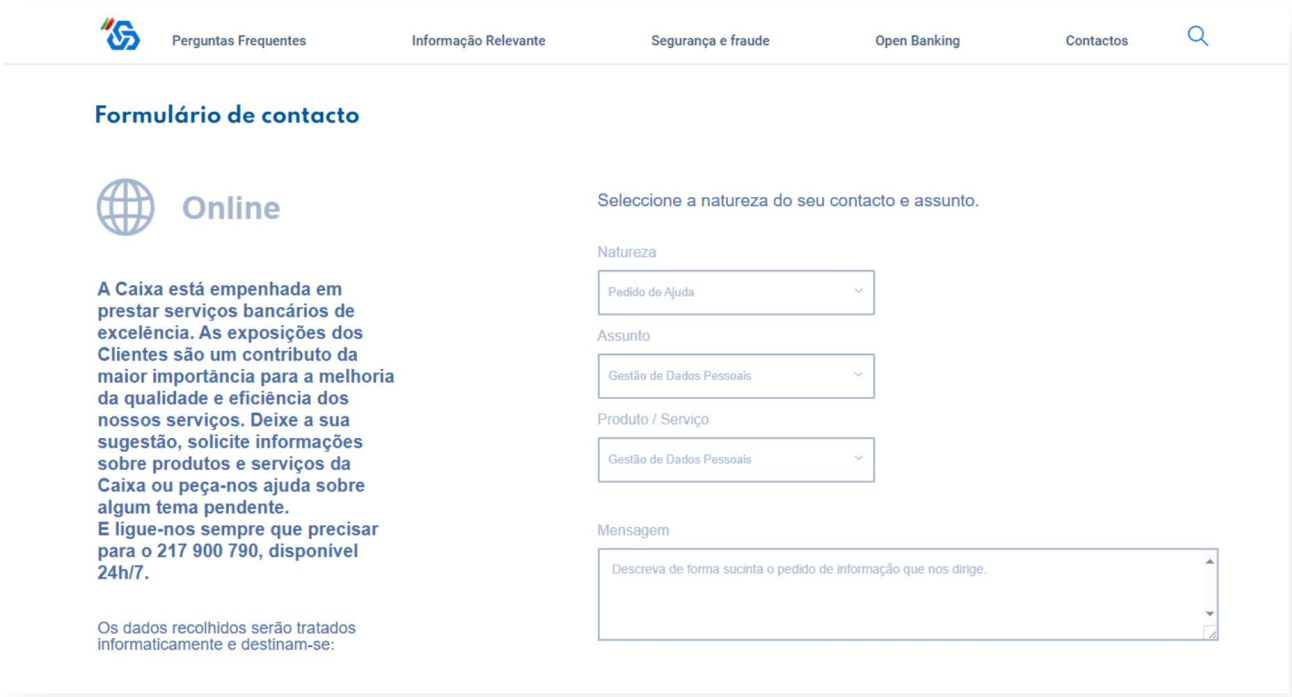
Identificação do Titular dos Dados

Nome Completo _____ N.º Cliente _____

Direito a Exercer

- ☐ Acesso aos dados pessoais
- ☐ Retificação de dados
- ☐ Oposição ao tratamento de dados
- ☐ Limitação ao tratamento de dados
- ☐ Portabilidade dos dados
- ☐ Apagamento dos dados

Meio de resposta:
- ☐ Mensagem segura
- ☐ Email _____ (Endereço de email)
- ☐ Carta _____ (Morada)



048.
O que fazer nos casos em que o Titular dos Dados se dirija à CGD por outras vias?

Caso o Titular dos Dados se dirija à CGD por outras vias, as Direções devem encaminhar a comunicação de imediato à(ao) *Data Protection Officer*, através do endereço de correio eletrónico data.protection.officer@cgd.pt.

049.
Quem responde ao Titular dos Dados?

No caso de o Titular dos Dados dirigir diretamente à(ao) *Data Protection Officer* o pedido de exercício de direitos, a(o) *Data Protection Officer* responderá ao Titular dos Dados, com base na informação facultada pelas várias Direções da CGD (responsáveis pelo tratamento).
Caso o Titular dos Dados (Cliente) formalize o pedido de exercício de direitos através da Rede Comercial (em impresso próprio) ou do Caixadirecta, os Colaboradores da CGD devem:

a) Garantir:

I. a correta instrução do pedido de exercício de direitos (v.g. entrega de comprovativos, no caso de pedido de retificação de elementos que o exijam);
II. a validação da identidade do titular;
III. a digitalização do pedido de exercício de direitos e seu arquivo no GESARQ;

b) O tratamento do pedido é efetuado nos seguintes termos:

I. **Direito de acesso** – o recetor trata o pedido mediante acesso à Plataforma de Balcão, imprimindo ou gravando ficheiro com a informação correspondente à constante da Ficha de Elementos Informativos e/ou à informação particular solicitada pelo Cliente, procedendo à sua entrega nos moldes pretendidos;
II. **Direito de retificação** – o recetor do pedido atualiza na transação respetiva a informação fornecida pelo Cliente, devidamente comprovada quando for o caso;

III. **Direito de oposição** – o recetor do pedido regista na Plataforma de Balcão a revogação do consentimento prestado, nos termos solicitados pelo Titular dos Dados;
IV. **Direito à portabilidade** – o recetor trata o pedido mediante acesso à Plataforma de Balcão, imprimindo ou gravando ficheiro e disponibilizando o ficheiro ao Cliente;
V. **Direito ao apagamento dos dados** ("direito a ser esquecido") e direito à limitação do tratamento – o recetor encaminha pedido através de AGILE para o CO, que avalia se o Cliente reúne requisitos para o efeito pretendido, procede ao registo respetivo no sistema de informação, quando aplicável, e responde ao Cliente em conformidade;

c) Quando o pedido suscite dúvidas de natureza jurídica à Rede Comercial, deverá ser solicitada a apreciação da DAJ.

Como deve a Rede Comercial proceder perante o exercício de direitos?

Aceder à transação CLIJN6, que permite o registo do exercício dos direitos:

DIREITO DE ACESSO	DIREITO DE OPOSIÇÃO	DIREITO DE RETIFICAÇÃO	DIREITO À PORTABILIDADE	DIREITO AO APAGAMENTO	DIREITO À LIMITAÇÃO
O Colaborador deve aceder, na PB, à transação **CLIJN6** e selecionar "**Direito a exercer**" e "**Meio Preferencial de Resposta**" (carta/*email* ou PDF).	O Colaborador deve aceder, na PB, à transação **CLIJN6** e selecionar "**Direito a exercer**".	O Colaborador deve aceder, na PB, à transação **CLIJN6** e selecionar "**Direito a exercer**" em simultâneo o cliente deve preencher nova **FEI** com os dados que vão ser objeto de alteração e entregar os respetivos comprovativos.	O Colaborador deve aceder, na PB, à transação **CLIJN6** e selecionar "**Direito a exercer**" e "**Meio Preferencial de Resposta**" (*email*).	O Colaborador deve aceder, na PB, à transação **CLIJN6** e selecionar "**Direito a exercer**" e endereçar o mesmo ao CO, **via AGILE** "Clientes" > "RGPD - Esqecimento ou Limitação de Tratamento de Dados Pessoais".	O Colaborador deve aceder, na PB, à transação **CLIJN6** e selecionar "**Direito a exercer**" e endereçar o mesmo ao CO, **via AGILE** "Clientes" > "RGPD - Esqecimento ou Limitação de Tratamento de Dados Pessoais".

050.
Quem responde ao Titular dos Dados se candidato a Colaborador da CGD?

No caso de o Titular dos Dados ser candidato a Colaborador da CGD, o pedido de exercício dos direitos pode ser enviado para a *mailbox* dpe.protecao.dados.pessoais@cgd.pt ou através de carta remetida à CGD, A/c. DPE – Direção de Gestão e Desenvolvimento de Pessoas, AV. João XXI, 63, 1000-300 Lisboa.

051.
Quem responde ao Titular dos Dados se Colaborador da CGD?

O Titular dos Dados que seja Colaborador da CGD deve formalizar o pedido de exercício de direitos através do Caixapessoal, por carta ou *email* dirigido a dpe.protecao.dados.pessoais@cgd.pt.
A Direção de Gestão e Desenvolvimento de Pessoas (DPE) valida a identidade do Titular dos Dados e assegura a resposta ao pedido do Titular dos Dados. A(O) *Data Protection Officer* pode ser consultada(o) pela Direção de Gestão e Desenvolvimento de Pessoas (DPE) para elaboração da resposta.

052.
Quem responde ao Titular dos Dados se ex-Colaborador da CGD?

O Titular dos Dados que seja ex-Colaborador da CGD deve formalizar o pedido por carta ou *email* dirigido a dpe.protecao.dados.pessoais@cgd.pt. A Direção de Gestão e Desenvolvimento de Pessoas (DPE) valida a identidade do Titular dos Dados e assegura a resposta ao pedido do Titular dos Dados. A(O) *Data Protection Officer* pode ser consultada(o) pela Direção de Gestão e Desenvolvimento de Pessoas (DPE) para elaboração da resposta.

053.
Como se efetua neste âmbito a colaboração e comunicação entre as Direções e a(o) *Data Protection Officer*?

Para esclarecimento de dúvidas sobre o pedido de exercício de direitos pelo Titular dos Dados, as Direções Centrais, a quem compete assegurar a resposta aos pedidos, podem contactar a(o) *Data Protection Officer* por *email* (data.protection.officer@cgd.pt) ou através do "CA – Pedido de Parecer DPO", para pedidos de emissão de parecer.

054.
Qual o prazo de resposta ao Titular dos Dados?

Trata-se do prazo de um mês a contar da receção do pedido, podendo este prazo ser prorrogado até dois meses, apenas quando for necessário, tendo em conta a complexidade do mesmo e o número de pedidos. Após o prazo de um mês, a CGD deve informar o Titular dos Dados da necessidade de prorrogação.

055.
Qual a forma de resposta ao Titular dos Dados?

Salvo solicitação do titular em contrário, preferencialmente, através de correio eletrónico.

056.
Quais são as consequências do incumprimento?

As consequências do incumprimento pela CGD (Responsável pelo Tratamento) da resposta ao exercício de direitos podem ser consultadas na secção "Responsabilidade contra-ordenacional" deste Guia.

SABER MAIS

Pode consultar, na "Página RGPD" do Somos Caixa, os seguintes documentos:
EDPB - Relatório sobre aplicação do direito de acesso pelos Responsáveis pelo Tratamento

EDPB - Orientações 1/2022 sobre o Direito de Acesso

EDPB - Diretrizes 5/2019 relativas aos critérios do direito a ser esquecido pelos motores de busca ao abrigo do RGPD

WP29 - Diretrizes sobre Decisões Individuais Automatizadas e Perfilagem para os fins do Regulamento 2016/679

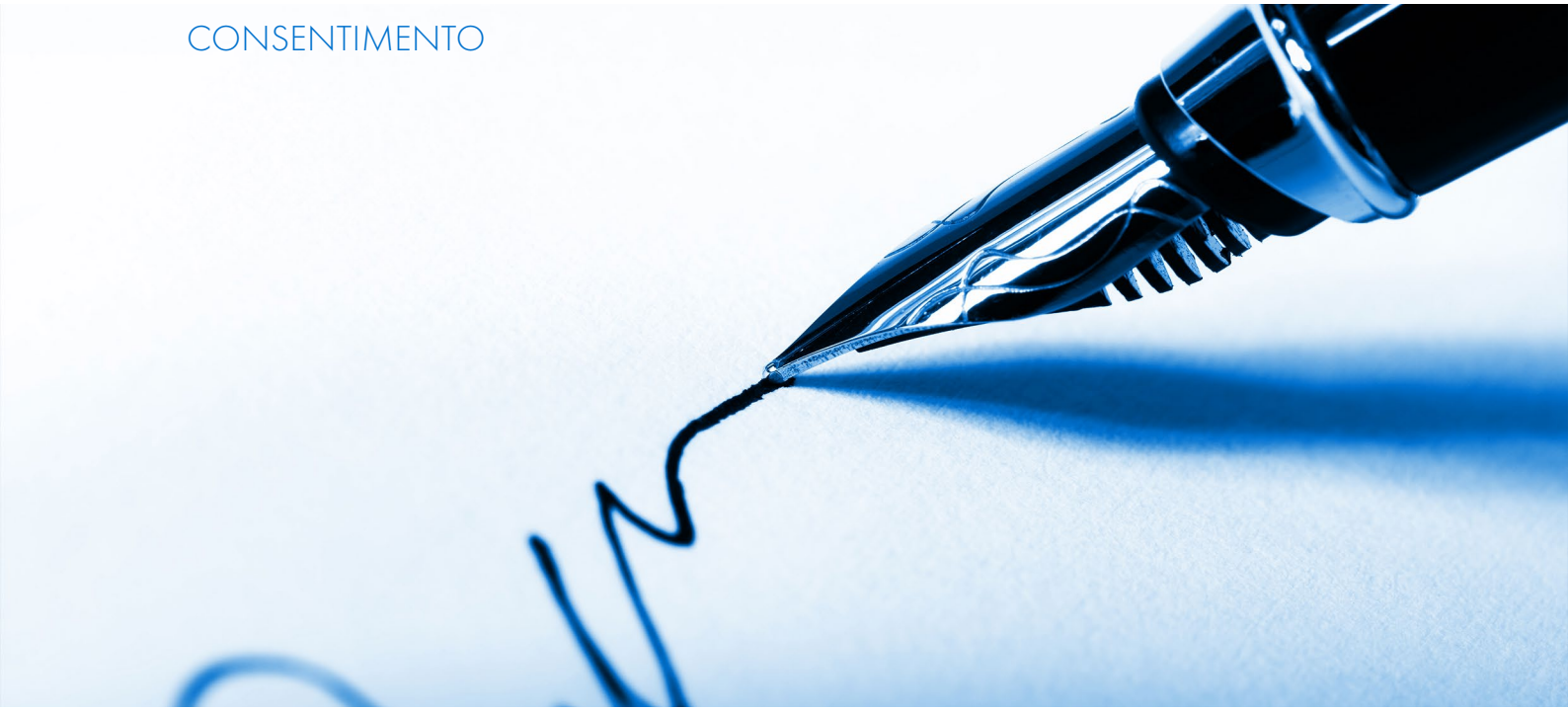
WP29 - Orientações sobre o direito à portabilidade dos dados

Lei n.º 75/2021, de 18 de novembro - consagra o direito ao esquecimento de pessoas que tenham superado ou mitigado situações de risco agravado

de saúde ou de deficiência, tendo em vista melhorar o acesso ao crédito e a contratos de seguro destas pessoas.

Norma Regulamentar da Autoridade de Supervisão de Seguros e Fundos de Pensões n.º 12/2024-R - Esta norma tem por objeto (a) regular a operacionalização do dever de não recolha ou tratamento, pelos seguradores, da informação de saúde relativa à situação médica que originou o risco agravado de saúde ou a deficiência, nos termos da Lei n.º 75/2021; (b) detalhar o sentido e a extensão das práticas previstas no art.15.º n.ºs 2, 3 e 10, do regime jurídico do contrato de seguro (RJCS) aprovado pelo Decreto-Lei n.º 72/2008, de 16 de abril, bem como dos fatores de risco a considerar e (c) e definir parâmetros para operacionalização do mecanismo de proteção de cobertura previsto no art. 217.º do RJCS.

CONSENTIMENTO



057.
Em que casos o consentimento pode ser a base legal para o tratamento dos dados?

O consentimento pode ser a base para o tratamento dos dados sempre que a CGD não disponha de outra condição de licitude (por exemplo, quando esteja em causa o cumprimento de obrigações legais ou a execução de um contrato) e o Titular dos Dados o preste validamente.

058.
O que é necessário para que o consentimento seja válido?

O consentimento só é válido se a manifestação de vontade for livre (voluntária), específica (para o concreto tratamento de dados a que se destina), informada (por exemplo, sobre finalidade, prazo de conservação, consequências do tratamento, transmissão a terceiros) e inequívoca (objetiva).

059.
O consentimento prestado por menores é válido?

O consentimento prestado por menores é válido, desde que tenham pelo menos 13 (treze) anos. Com idade inferior, só é válido o consentimento prestado pelos pais ou por outros titulares de responsabilidades parentais.

060.
O consentimento tem de revestir a forma escrita?

Não, o consentimento não tem de ser dado por escrito, mas deve ser uma manifestação clara e afirmativa e sem margem para dúvidas da vontade do Titular dos Dados. Todavia, compete à CGD demonstrar que o consentimento foi dado/prestado, devendo, sempre que possível, ser dado por escrito ou mediante outro suporte evidenciável (por exemplo, registos eletrónicos, gravações de chamadas).

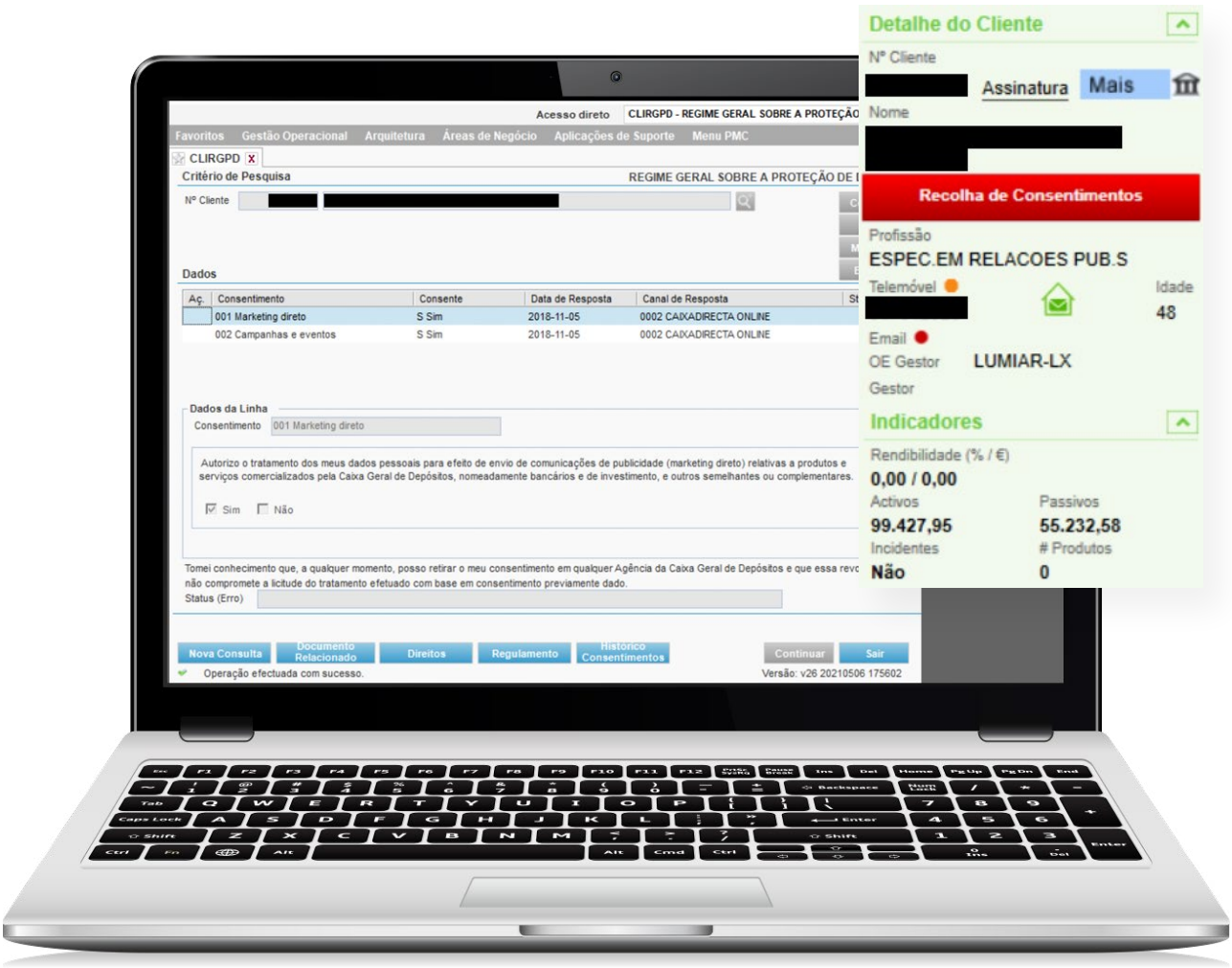
061.
De que forma deve ser dado o consentimento escrito?

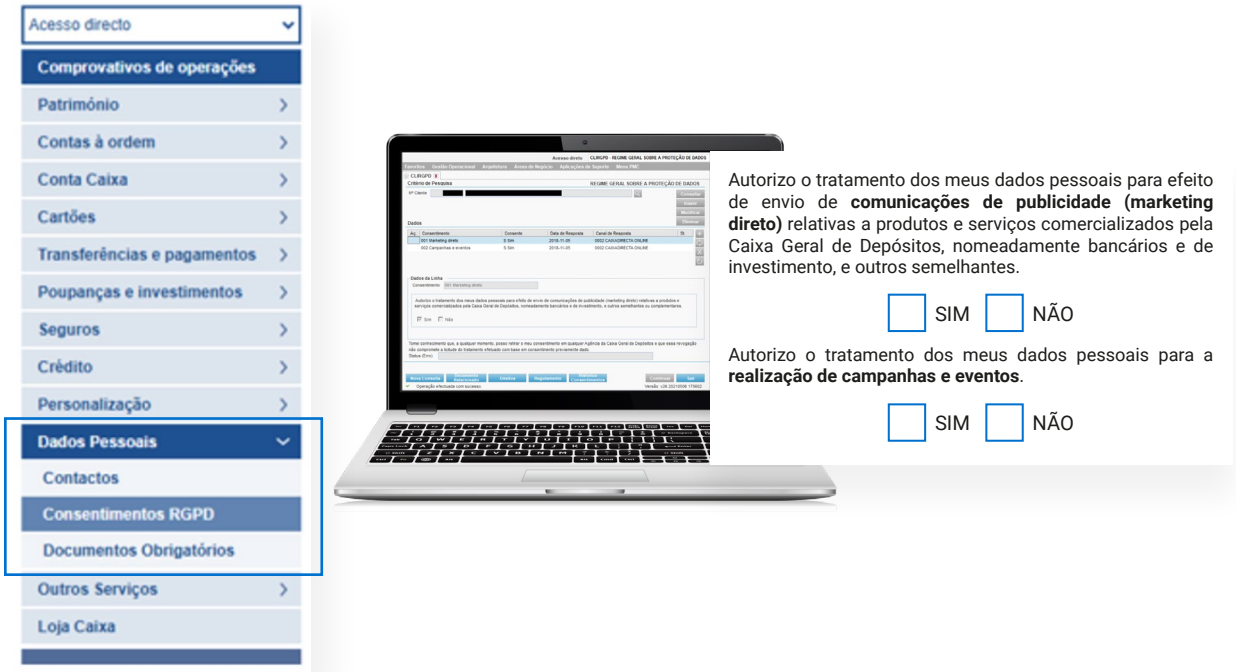
O consentimento escrito pode ser dado mediante a utilização de uma minuta definida para o efeito. Se essa minuta abordar outros assuntos, o pedido de consentimento deve ser claramente distinguível desses outros assuntos, de forma separada e destacada. O consentimento deve ser dado em momento prévio ao início de qualquer operação de tratamento.

062.
Quem regista o consentimento?

A Rede Comercial, as Direções de Negócios e qualquer Direção que recolha consentimentos devem registar e conservar os consentimentos obtidos relativamente aos tratamentos de dados que efetuem.
O consentimento pode ser comunicado pelo Cliente de forma personalizada, nas Agências ou no Caixadirecta Telefone, ou em auto-serviço, via Caixadirecta Online.
Nas agências e no Caixadirecta Telefone o consentimento é gerido na Plataforma de Balcão CLIRGPD.

Macanismos e Canais ativos para Recolha e Gestão





063.
Para que finalidades recolhemos o consentimento?

O consentimento é, atualmente, o fundamento de licitude apenas de 3 tratamentos de dados pessoais com as seguintes finalidades: comunicações de *marketing* direto, realização de campanhas e realização de eventos.

A CGD vai passar a efetuar um tratamento de dados pessoais que consiste na "Definição de Perfis" e cuja base de licitude é o consentimento dos Titulares de Dados, estando as Direções responsáveis a operacionalizar os desenvolvimentos necessários para a gestão dinâmica deste novo consentimento.

Tratamento de Dados/*Data processing* *(OBRIGATÓRIO SE INTERVENIENTE EM RELAÇÃO DE NEGÓCIO NA CGD)*
(Mandatory if intervening with a business relationship at CGD)

Autorizo o tratamento dos meus dados pessoais para definição de perfis, através do tratamento de diferentes categorias dos mesmos, incluindo o recurso a técnicas estatísticas, tendo em vista permitir à Caixa Geral de Depósitos apresentar-me ofertas mais ajustadas às minhas preferências e interesses.

I authorise the processing of my personal data for profiling purposes, through the processing of different categories of data, including the use of statistical techniques, in order to allow Caixa Geral de Depósitos to present me with offers more tailored to my preferences and interests.

☐ Sim (Autorizo)/ *Yes* ☐ Não (Não Autorizo)/ *No*

064.
Durante quanto tempo se conserva o consentimento?

Salvo imposição legal por período mais longo, o consentimento deve ser conservado pelo período necessário para cumprir as finalidades para as quais foi obtido, findo o qual deverá ser destruído.

065.
O consentimento pode ser livremente revogado?

Sim, o Titular dos Dados tem o direito de revogar o consentimento a qualquer momento, não tendo de apresentar qualquer justificação para a revogação.

066.
De que forma pode ser revogado?

A revogação do consentimento pode ser feita mediante declaração do Titular dos Dados, através do preenchimento do formulário ICGDPT0370 "Exercício de Direitos dos Titulares" em qualquer Agência da Rede Comercial e/ou do Caixadirecta *online*.

067.
Uma vez revogado o consentimento, o que fazer?

Uma vez revogado o consentimento, devem ser imediatamente cessados os tratamentos de dados que tivessem por base de licitude esse fundamento.
Quando aplicável, as Direções responsáveis pelo tratamento notificam imediatamente desse facto os Subcontratantes, destinatários e terceiros a quem os dados tenham sido transmitidos, para o mesmo efeito.

068.
A revogação do consentimento invalida o tratamento já efetuado?

Não, a revogação do consentimento não invalida o tratamento já efetuado. O tratamento de dados é, até esse momento, lícito.

069.
A revogação do consentimento é registada?

Sim. O Responsável pelo Tratamento deve manter registos que comprovem a revogação do consentimento. Sem prejuízo dos registos das Direções, nomeadamente, nos respetivos sistemas informáticos que se justifiquem e para obstar ao tratamento desses dados no futuro. A revogação é registada no sistema central através da transação CLIRGPD.

070.
Quais as consequências do desrespeito do consentimento do Titular dos Dados?

As consequências do desrespeito pela CGD da manifestação de vontade do Titular dos Dados (consentimento – não consentimento - revogação do consentimento) podem ser consultadas na secção "Responsabilidade contra-ordenacional" deste Guia.

SABER MAIS

Pode consultar, na "Página RGPD" do Somos Caixa, os seguintes documentos:
EDPB - Diretrizes 5/2020 relativas ao consentimento na aceção do Regulamento 2016/679

WP29 - Orientações sobre as decisão individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679

CNPD Diretriz 1/2022 – Sobre comunicações eletrónicas de *marketing* direto

071.
O que são *Cookies*?

Trata-se de pequenos ficheiros de informação que são armazenados no computador ou dispositivo móvel através do navegador (*browser*) utilizado pelo Titular dos Dados. Estes ficheiros permitem que durante um certo período o *website* ou a aplicação se "lembre" das ações e preferências, nomeadamente do nome de utilizador, da língua escolhida, do tamanho dos carateres e de outras definições de visualização.

EXEMPLO

Podem ser implementados *cookies* relativos ao endereço IP, ou relativos a preferências, idiomas ou cores, entre outros. Também podem existir *cookies* que armazenam senhas de acesso ou histórico de navegação em outros *sites*.

072.
Para que servem os *Cookies*?

Os *cookies* identificam o programa de navegação do utilizador no servidor, possibilitando o armazenamento de informação no dispositivo utilizado. Esta tecnologia serve para finalidades diversas, como ajudar a determinar a utilidade, interesse e o número de utilizações de *websites* ou aplicações, permitindo ao utilizador uma navegação mais rápida e eficiente, eliminando a necessidade de introduzir repetidamente as mesmas informações. Desta forma, quando percorre as páginas de um *website* ou aplicação ou regressa a um *website* ou aplicação que já visitou, em relação ao qual deu a aceitação para utilização de *cookies*, o utilizador não tem, em princípio, de voltar a indicar as suas preferências ou a inserir dados que já tinha fornecido anteriormente.

073.
O que são *Cookies* permanentes?

São *cookies* que ficam armazenados, mesmo após fechar o *browser*, nos equipamentos de

acesso (PC, *mobile* e *tablet*) e que são utilizados sempre que o utilizador faz uma nova visita a um dos *websites* ou aplicações. São utilizados, geralmente, para direcionar a navegação aos interesses do utilizador, permitindo prestar um serviço mais adequado aos meios e equipamento utilizados.

074.
O que são *Cookies* de sessão ou temporários?

São aqueles que permanecem no arquivo de *cookies* do *browser* do utilizador até finalizar a navegação. A informação obtida por *cookies* de sessão serve para analisar padrões de tráfego, permitindo identificar a utilização que cada utilizador faz durante a sua navegação, identificar melhorias de forma a fornecer uma boa experiência de navegação.

075.
O que são *Cookies* próprios?

Os *cookies* próprios são descarregados pelo *site* que o utilizador está a visitar e que partilham o mesmo domínio, sendo enviados para o equipamento terminal do utilizador a partir de um equipamento ou domínio gerido e a partir do qual se presta o serviço solicitado pelo utilizador.

076.
O que são *Cookies* de terceiros?

Os *cookies* de terceiros são descarregados para o dispositivo de acesso do utilizador à *internet* por *sites* de um domínio diferente daquele que se está a visitar. Isto pode acontecer, por exemplo, em conteúdos multimédia alojados em canais de vídeo, de uma terceira entidade.

077.
A CGD utiliza *Cookies* para que finalidades?

A CGD utiliza *Cookies* para várias finalidades como, por exemplo, melhorar a experiência do utilizador, fazendo com que o *website* ou aplicação se "lembre" das ações e preferências do utilizador (como o seu nome ou a língua escolhida) e para análise de uso (determinar a utilidade, interesse e número de utilizações dos *websites* ou aplicações da CGD). Para mais detalhe sobre esta questão, consulte a Política de *Cookies* da CGD https://www.cgd.pt/Ajuda/Pages/Privacidade-e-cookies.aspx.

078.
Na CGD, como gerir os *Cookies*?

Todos os *browsers* permitem ao respetivo utilizador aceitar, recusar ou apagar *cookies*, nomeadamente através da seleção das definições apropriadas no respetivo navegador.

O utilizador pode, assim, configurar o seu *browser* para informar sempre que um *cookie* é recebido ou mesmo desativar a sua aceitação. A CGD alerta para que, nesse caso, poderá afetar, parcialmente, a utilização de alguns dos nossos serviços, não tendo uma navegação, no nosso *website*, melhorada e personalizada.

Se a configuração de privacidade do seu *browser* estiver definida como "Alta", não conseguirá aceder a alguns dos nossos serviços e poderá ser impedido de utilizar em pleno todas as funcionalidades dos nossos *websites* ou aplicações.
Para solucionar esta questão, adicione os nossos endereços de *Internet* à lista de *websites* permitidos nas configurações de privacidade do seu *browser*.

Se estiver a aceder aos nossos *websites* através de um computador empresarial e não conseguir aceder, o problema poderá estar nas configurações de segurança corporativa do computador.

Recomendamos que entre em contacto com o administrador do sistema.

O utilizador pode aceitar, recusar ou remover *cookies* através da gestão das definições do seu *browser*, sendo sempre dada a possibilidade ao utilizador de alterar as suas permissões. O utilizador pode configurar os *cookies* no menu "opções" ou "preferências" do seu *browser*.

079.
Na CGD, como desativar os *Cookies*?

Todos os *browsers* (navegadores) de *internet* permitem ao utilizador a gestão dos *cookies* das páginas que visita.
Para mais informações sobre este tema, consulte a Política de *Cookies* da CGD https://www.cgd.pt/Ajuda/Pages/Privacidade-e-cookies.aspx.

SABER MAIS

Pode consultar a "Cookiepedia" da Plataforma OneTrust https://cookiepedia.co.uk/.

080.
O que fazer quando há a necessidade de recorrer a um Subcontratante para tratar dados pessoais?

Para este efeito, é necessário:

- Utilizar um acordo de tratamento de dados, validado pela(o) *Data Protection Officer*, a assegurar por cada Direção adquirente do serviço e que visa garantir o cumprimento de todas as obrigações exigidas pelo RGPD, no procedimento de subcontratação;
- Adotar cláusulas específicas na documentação contratual aplicável, consoante os casos.

081.
O acordo de tratamento de dados pode sofrer alterações?

Sim, em virtude das especificidades de cada contrato/situação.

082.
Justifica-se em todos os procedimentos pré-contratuais?

Não. Apenas quando o contrato implique o tratamento de dados pessoais.

083.
Pode recorrer-se a qualquer Subcontratante?

Não. Sem prejuízo da regulação bancária aplicável, o RGPD determina que apenas se pode recorrer aos Subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas.

084.
É possível a subcontratação em cadeia de funções essenciais ou importantes da CGD?

O acordo de subcontratação deve especificar se é ou não autorizada a subcontratação em cadeia (sub-subcontratação) de funções essenciais ou importantes ou de partes significativas das mesmas.

085.
Como se afere o cumprimento do RGPD por parte da CGD em relação às partes contratantes?

Mediante verificação da existência e implementação de medidas técnicas e organizativas adequadas por parte das demais partes contratantes.

086.
Como demonstrar esse cumprimento?

Mediante disponibilização de evidências que devem revestir a forma escrita.

087.
Há algum elenco de evidências definido?

Quanto a esta questão, recomenda-se que as Direções se dotem de um catálogo de evidências necessário à tomada de decisão no âmbito do caso/contrato concreto.

088.
Quem define as evidências a solicitar em cada contrato?

De acordo com a natureza dos dados a tratar, cabe a cada Direção(ões) envolvida(s) indicar as especificações técnicas e as respetivas evidências, se as houver, para endereçar à Área de Procurement (atualmente, a CSP) com vista a serem inseridas no Caderno de Encargos a assegurar pelo fornecedor.

089.
Quem avalia a existência de garantias adequadas?

A existência de garantias adequadas deve ser avaliada pela(s) Direção(ões) da CGD que pretende(m) contratar o produto ou serviço (Direção "cliente"), obtendo-se ainda o envolvimento das Direções que emitem parecer obrigatório (DGR, DC e DSI) para avaliação e seleção do Subcontratante. A(O) *Data Protection Officer* emite parecer, se e quando é solicitado para o efeito pela Direção "cliente".

Obtida esta avaliação, é(são) a(s) Direção(ões) "cliente(s)" que, de acordo com as especificações definidas, informa(m) a Área de *Procurement* (atualmente, a CSP) de que as garantias adequadas prestadas pelo fornecedor estão em conformidade com o RGPD.

090.
Como se avalia a existência de garantias adequadas?

Enquanto não houver certificações de proteção de dados, essa avaliação é efetuada mediante verificação da aptidão das evidências para demonstrar a existência e a implementação das medidas técnicas e organizativas exigidas. A DSI avalia, entre outras matérias, os requisitos de segurança da informação.

091.
Em que fase é feita essa avaliação?

Por regra, no contexto da fase de habilitação a concurso, na fase de avaliação das propostas, que antecede a decisão de adjudicação e a celebração do contrato.

Todavia, nos casos de procedimentos fechados (isto é, a convite) ou em casos de contratação excluída, essa avaliação deverá ser feita a título prévio a qualquer convite ou contratação.

092.
Qual o prazo para o efeito?

A apresentação das evidências por parte do fornecedor é feita no decurso das negociações e troca de informações necessárias à avaliação das propostas, tendo em vista a celebração do contrato.

093.
Quais são as consequências da falta de apresentação de evidências?

A falta de apresentação de evidências implica a exclusão do potencial fornecedor do processo de avaliação e a não contratação.

094.
Quais são as consequências do incumprimento do recurso regular a Subcontratante?

As consequências do incumprimento pela CGD do recurso regular de Subcontratante, bem como as coimas aplicáveis, podem ser consultadas na secção "Responsabilidade contra-ordenacional" deste Guia.

SABER MAIS

Pode consultar, na "Página RGPD" do Somos Caixa, os seguintes documentos:
EDPB - Orientações 07/2020 sobre os conceitos de Responsável pelo Tratamento e Subcontratante no RGPD

EBA/GL/2019/02 – Orientações relativas à subcontratação

OS CGD 10/2025 - Política de Subcontratação do Grupo CGD

IS CGD 15/2022 – Processo de Subcontratação de Funções da CGD

095.
O que é o registo de atividades de tratamento?

É um registo escrito organizado do qual constam todas as atividades de tratamento de dados pessoais sob responsabilidade da CGD e que específica:

- O nome e os contactos do responsável pelo tratamento e da(o) *Data Protection Officer*;
- As finalidades do tratamento dos dados;
- A descrição das categorias de Titulares dos Dados e das categorias de dados pessoais;
- As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais;
- Se aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais;
- Os prazos previstos para o apagamento das diferentes categorias de dados;
- Uma descrição geral das medidas técnicas e organizativas no domínio da segurança.

096.
É um registo estático ou dinâmico?

É dinâmico, pois deve refletir em cada momento a atualidade dos tratamentos de dados pelos quais a CGD é o responsável. As Direções responsáveis da CGD registam na plataforma *One Trust* (OT) as

respetivas atividades de tratamento e devem proceder anualmente à sua atualização. Este registo centralizado está confiado à(ao) *Data Protection Office*, que o guarda e controla a conformidade desta iniciativa para a atualização regular pelo Responsável pelo Tratamento.

097.
Quem comunica as operações a incluir no registo de atividades de tratamento?

As Direções devem comunicar à(ao) *Data Protection Officer* as novas operações de tratamento de dados que pretendam iniciar, as que já não se justificam e as que subsistam, mas que tenham sofrido alterações (por exemplo, quanto ao prazo de conservação, recurso a outro Subcontratante).

098.
Há a necessidade de avaliação periódica?

Sim. Sem prejuízo de outras comunicações sempre que se justificar, pelo menos, anualmente, por iniciativa da(o) *Data Protection Officer*, as Direções devem confirmar a atualidade da informação constante do registo de atividades de tratamento.

099.
Quem pode consultar o registo de atividades de tratamento?

Podem consultar o registo de atividades de tratamento o Conselho de Administração, a(o) *Data Protection Officer* e os Colaboradores do *Data Protection Office*, no âmbito das suas atribuições. As Direções podem consultar o registo de atividades de tratamento quanto às respetivas atividades de tratamento e a outras, apenas com base na justificação dessa necessidade perante a(o) *Data Protection Officer*. No âmbito da sua atividade inspetiva, a Comissão Nacional de Proteção de Dados pode consultar este registo.

100.
Quais são as consequências do incumprimento do registo de atividades de tratamento?

As consequências do incumprimento pela CGD das obrigações relativas ao registo de atividades de tratamento, bem como as coimas aplicáveis, podem ser consultadas na secção “Responsabilidade contra-ordenacional” deste Guia.

SABER MAIS

Pode consultar, na “Página RGPD” do Somos Caixa, os seguintes documentos:
OS COR CGD 7/2023 - Regulamento da Proteção de Dados Pessoais

OS CGD 11/2023 - Regulamento da Proteção de Dados Pessoais

OS COR 11/2018 - Política de Proteção de Dados Pessoais

OS CGD 20/2018 - Política de Proteção de Dados Pessoais

101.
Em que consiste a proteção de dados “desde a conceção” e “por defeito”?

A proteção de dados desde a conceção e por defeito é a obrigação do Responsável pelo Tratamento aplicar - tendo em conta as técnicas mais avançadas, os custos da sua aplicação, a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas - as medidas adequadas para garantir os princípios da proteção de dados.

102.
Em que momento releva essa obrigação?

Essa obrigação releva, desde logo, no momento de definição dos meios de tratamento (conceção do projeto) como no momento do próprio tratamento (execução do projeto).

103.
Como acautelar esse cumprimento?

O Responsável pelo Tratamento, para acautelar o cumprimento da proteção de dados desde a conceção e por defeito, deve rodear-se e envolver todas as áreas técnicas cujos contributos sejam relevantes para o desenvolvimento do projeto, garantindo que todos os requisitos jurídicos, técnicos, operacionais e humanos estão preenchidos.

104.
Quando deve a(o) *Data Protection Officer* ser envolvida(o)?

O envolvimento da(o) *Data Protection Officer* deve verificar-se tão cedo quanto possível, isto é, na conceção do projeto, como requisito do mesmo, cabendo a iniciativa ao Responsável pelo Tratamento, que deverá prestar toda a informação e colaboração para o efeito.

105.
Qual a importância?

A proteção de dados desde a conceção e por defeito permite acautelar os riscos tecnológico, jurídico e reputacional de incumprimento do RGPD, identificar desde logo a necessidade de realização de uma avaliação de impacto sobre a proteção de dados (DPIA), gerir eficazmente os recursos humanos e financeiros. O desenvolvimento do projeto deve permitir a prevenção de eventuais constrangimentos futuros, bem como demonstrar e documentar a conformidade, em particular, no âmbito da atividade inspetiva da Comissão Nacional de Proteção de Dados.

106.
Como se documenta?

Através da documentação relativa aos respetivos requisitos do projeto, atas de reuniões de trabalho, documentação de suporte e pareceres ou relatórios, consoante os casos, do gestor do projeto e da(o) *Data Protection Officer*.

SABER MAIS

Pode consultar, na "Página RGPD" do Somos Caixa, o seguinte documento: **EDPB - Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados desde a Conceção e por Defeito**

107.
O que é a avaliação de impacto sobre a proteção de dados (DPIA)?

A DPIA é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais, avaliando-os e determinando as medidas necessárias para mitigar esses riscos.

108.
Em que consiste a DPIA?

A DPIA inclui, pelo menos:

- Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do Responsável pelo Tratamento;
- Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;
- Uma avaliação dos riscos para os direitos e liberdades dos Titulares dos Dados;
- As medidas previstas para mitigar os riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o RGPD, tendo em conta os direitos e os legítimos interesses dos Titulares dos Dados e de outras pessoas em causa; e,
- O parecer da(o) *Data Protection Officer*.

109.
Quem realiza as DPIAs?

As DPIAs são realizadas pela(s) Direção(ões) responsável(eis) pelo projeto, que define(m), em cada caso, a metodologia, com acompanhamento do *Data Protection Office*, em articulação com as Direções envolvidas na sua realização.

110.
Qual a importância?

As DPIAs são instrumentos importantes em matéria de responsabilização, uma vez que ajudam os Responsáveis pelo Tratamento a cumprir os requisitos do RGPD, bem como a demonstrar que foram tomadas medidas adequadas para assegurar a conformidade com o RGPD. A DPIA é um processo que visa estabelecer e demonstrar a conformidade, nomeadamente no âmbito da atividade inspetiva da Comissão Nacional de Proteção de Dados.

111.
É necessário realizar-se uma DPIA relativamente a todos os tratamentos?

Não, apenas naqueles que revelem um elevado risco. E para novos tratamentos, em que a inovação tecnológica esteja presente.

112.
Quais são os tratamentos que revelam um elevado risco?

Nos termos do RGPD, o Responsável pelo Tratamento deve realizar uma DPIA em caso de:

a) avaliação sistemática e completa de aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
b) operações de tratamento em larga escala de categorias especiais de dados (artigo 9.º, n.º 1) ou de dados pessoais relacionados com condenações penais e infrações (artigo 10.º); ou
c) controlo sistemático de zonas acessíveis ao público em grande escala.

113.
Há listas de tratamentos obrigatoriamente sujeitos a DPIA?

Além deste elenco constante do RGPD sobre tratamentos que revelam elevado risco, a Comissão Nacional de Proteção de Dados elaborou uma lista de tratamentos de dados (cf. Regulamento n.º 1/2018 da CNPD) em que é obrigatória a realização de DPIA, concretamente:

1. Tratamento de informação decorrente da utilização de dispositivos eletrónicos que transmitam, por redes de comunicação, dados pessoais relativos à saúde;
2. Interconexão de dados pessoais ou tratamento que relacione dados pessoais previstos no n.º 1 do artigo 9.º (categorias especiais de dados) ou no artigo 10.º (dados pessoais relacionados com condenações penais e infrações) do RGPD ou dados de natureza altamente pessoal;
3. Tratamento de dados pessoais previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal com base em recolha indireta dos mesmos, quando não seja possível ou exequível assegurar o direito de informação nos termos da alínea b) do n.º 5 do artigo 14.º do RGPD;
4. Tratamento de dados pessoais que implique ou consista na criação de perfis em grande escala;
5. Tratamento de dados pessoais que permita rastrear a localização ou os comportamentos dos respetivos titulares (por exemplo, trabalhadores, clientes ou apenas transeuntes), que tenha como efeito a avaliação ou classificação

destes, exceto quando o tratamento seja indispensável para a prestação de serviços requeridos especificamente pelos mesmos;
6. Tratamento dos dados previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou ainda dos dados de natureza altamente pessoal para finalidade de arquivo de interesse público, investigação científica e histórica ou fins estatísticos, com exceção dos tratamentos previstos e regulados por lei que apresente garantias adequadas dos direitos dos titulares;
7. Tratamento de dados biométricos para identificação inequívoca dos seus titulares, quando estes sejam pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados;
8. Tratamento de dados genéticos de pessoas vulneráveis, com exceção de tratamentos previstos e regulados por lei que tenha sido precedida de uma avaliação de impacto sobre a proteção de dados;
9. Tratamento de dados pessoais previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou dados de natureza altamente pessoal com utilização de novas tecnologias ou nova utilização de tecnologias já existentes.

114.
Esta(s) lista(s) pode(m) ser alterada(s)?

Sim, nomeadamente, em virtude de progressos tecnológicos. A lista de tratamentos sujeitos a DPIA não é taxativa.

115.
Há tratamentos de dados não constantes daquela lista suscetíveis de constituir elevado risco?

Sim. A lista da CNPD não dispensa os Responsáveis pelo Tratamento de avaliar e realizar DPIA nos casos em que considerem existir um elevado risco.

116.
O que fazer se se pretender iniciar um tratamento não constante daquela lista?

Em caso de dúvida, solicitar a pronúncia da(o) *Data Protection Officer* sobre a necessidade de realizar uma DPIA.

117.
Há sempre a necessidade de consultar previamente a Comissão Nacional de Proteção de Dados consoante o resultado da DPIA?

Não, apenas nos casos em que da DPIA se constate que o tratamento resultaria num elevado risco para os direitos dos Titulares dos Dados na ausência das medidas tomadas pelo Responsável pelo Tratamento.

118.
Feita a consulta prévia, em que prazo se pronuncia a CNPD?

No prazo máximo de oito semanas a contar da receção do pedido de consulta, a CNPD dá orientações, por escrito, ao Responsável pelo Tratamento e, se o houver, ao Subcontratante, sem prejuízo do exercício dos demais poderes de que dispõe (realizar inspeções, fazer advertências, repreensões, avaliar sistemas informáticos, etc.).

119.
Quais as consequências se não efetuar uma DPIA que for devido?

As consequências do incumprimento pelo Responsável pelo Tratamento (CGD) das obrigações em matéria de avaliação de impacto sobre a proteção de dados, bem como as coimas aplicáveis, podem ser consultadas na secção “Responsabilidade contra-ordenacional” deste Guia.

SABER MAIS

Pode consultar, na "Página RGPD" do Somos Caixa, os seguintes documentos:
WP29 Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «susceptível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679

CNPD - Regulamento n.º 1/2018 – Lista de avaliações de impacto sobre a proteção de proteção de dados de realização obrigatória

OS CGD 11/2023 – Regulamento da Proteção de Dados Pessoais (ponto 6.1.2)

120.
Há algum catálogo estabelecido de violações de dados?

Não. A qualificação é feita casuisticamente. Não obstante e como auxílio, o *template* para reporte deste tipo de incidentes contempla os seguintes exemplos:

- *Phishing*;
- *Malware* (*ransomware*);
- Divulgação não intencional (exemplo, envio massivo de campanhas de produtos e serviços para Clientes deixando visível o endereço de *email* de todos os outros destinatários);
- Alteração de dados pessoais sem autorização;
- Furto ou extravio de equipamentos eletrónicos contendo dados pessoais;
- Furto ou extravio de documentos físicos;
- Extravio ou abertura ilícita de correio;
- Divulgação verbal não autorizada de dados pessoais.

São *triggers* de violação de dados (constantes do Anexo IV da OS CGD 11/2023 – Regulamento da Proteção de Dados Pessoais):

Triggers - Violação de Dados

INCIDENTES DE SEGURANÇA **FÍSICA**
Furto ou extravio de equipamento eletrónico (portátil, dispositivos amovíveis)
Furto ou extravio de documentos em suporte de papel
Perda de chaves eletrónicas
Incêndio nos servidores de dados do *Data Center*
Extravio ou abertura ilícita de correio
Destruição incorreta de papel com informação sensível
Divulgação verbal não autorizada de dados pessoais
Acesso não autorizado de terceiros

INCIDENTES DE SEGURANÇA **LÓGICA/INFORMÁTICA**
Malware (ransomwares)
Phishing (apropriarem-se das credenciais)
Hacking
Ewast (dados pessoais ainda presentes em dispositivo obsoleto)
Divulgação não intencional (envio de *email* para destinatário errado, caso de campanhas em que os clientes vão em Bcc, etc.)
Ação deliberada ou por inércia de um Colaborador/prestador
Alteração de dados pessoais sem autorização
Indisponibilidade de dados pessoais

121.
As violações de dados pessoais são violações da segurança da informação?

Sim, mas mais circunscritas. As violações de segurança da informação não implicam que a informação protegida diga necessariamente respeito a dados pessoais.

122.
Quem deteta, em primeira linha, esses incidentes?

1) Os Colaboradores da CGD (Direções Centrais, Rede Comercial e eventuais Unidades de estrutura autónomas);
2) O CSIRT – Área de Segurança da Informação, no âmbito das suas responsabilidades;
3) Subcontratantes;
4) Prestadores de serviços;
5) Utilizadores externos; e, eventualmente,
6) Titulares dos Dados.

123.
Havendo dúvidas quanto à qualificação de um incidente como violação de dados pessoais, o que fazer?

Existindo essa dúvida, os Colaboradores da CGD deverão comunicar o incidente no Catálogo de Serviços "RGPD – Violação de dados" para se proceder, de imediato, a uma análise do mesmo.

124.
Como comunicar/reportar um incidente?

O Colaborador que detete ou tenha conhecimento de situação que possa configurar violação de dados deve proceder ao registo do incidente no CA – "RGPD – Violação de Dados".

125.
Em que prazo deve ser reportado o incidente?

Imediatamente, isto é, tão cedo quanto possível.

126.
Em que casos se comunica o incidente à (ao) *Data Protection Officer*?

O incidente deve ser comunicado à(ao) *Data Protection Officer* sempre que, após análise das Direções designadas para o efeito (CO-Reclamações, DC, DPE, DSI e GPS), se conclua que o incidente reportado tem impacto para a disponibilidade, a confidencialidade e a integridade de dados pessoais.
O reporte deve descrever tão detalhadamente quanto possível:

- A natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de Titulares de Dados afetados;
- As consequências prováveis da violação de dados pessoais;
- As medidas adotadas ou propostas para reparar a violação de dados pessoais.

127.
Quem trata o incidente de violação de dados?

A Equipa de Urgência da Proteção de Dados, após convocatória da(o) *Data Protection Officer*, analisa e aprecia o incidente, pronunciando-se também sobre a obrigação legal de notificação à CNPD e de comunicação aos Titulares dos Dados. Sempre que necessário, podem ser envolvidas outras Direções na apreciação a efetuar pela Equipa de Urgência da Proteção de Dados.

128.
Quem avalia a necessidade de notificar a CNPD ou os Titulares dos Dados sobre a violação?

A necessidade de notificação é avaliada pela Equipa de Urgência da Proteção de Dados, que caracteriza o incidente como de risco ou de elevado risco, nos termos do RGPD. O entendimento da Equipa de Urgência da Proteção de Dados é submetido à apreciação final do Conselho Delegado de Continuidade de Negócio, Risco Operacional e Controlo Interno.

129.
Quem notifica a CNPD?

Compete à Direção ou ao Órgão de Estrutura onde foi detetada a situação de violação de dados assegurar a notificação à Comissão Nacional de Proteção de Dados, com o eventual apoio da Equipa de Urgência da Proteção de Dados e/ou da(o) *Data Protection Officer*, recorrendo ao formulário disponibilizado pela CNPD no respetivo *site*.

130.
Quem comunica aos Titulares dos Dados?

A comunicação aos Titulares dos Dados compete também à Direção ou ao Órgão de Estrutura onde foi detetada a situação de violação de dados, em colaboração com a DCM, se necessário, e observando o Manual de Comunicação Corporativa da CGD.

O Órgão de Estrutura responsável pela comunicação aos Titulares dos Dados informa e documenta perante a(o) *Data Protection Officer* o teor da comunicação.

131.
Há outros deveres de registo do incidente?

A Direção ou Órgão de Estrutura onde foi detetada a situação de violação de dados procede ao registo da situação no SAS e eGRC (a acompanhar pela DGR), bem como ao Registo de incumprimento (a acompanhar pela DC).

132.
Há algum registo central de violações de dados?

Sim. Os registos de incidentes estão centralizados no CA "RGPD – Violação de Dados Pessoais" no qual:

- Se conservam e documentam as violações de dados pessoais reportadas;
- Se elencam os factos relacionados com as mesmas e os respetivos efeitos;
- As avaliações efetuadas pela Equipa de Urgência da Proteção de Dados; e
- Se especificam as medidas de reparação adotadas e as comunicações realizadas, quer junto da Comissão Nacional de Proteção de Dados, quer dos respetivos titulares.

133.
Quais as consequências do incumprimento das obrigações em matéria de violação de dados?

As consequências do incumprimento pela CGD das obrigações em matéria de violação de dados, bem como as coimas aplicáveis, podem ser consultadas na secção "Responsabilidade contra-ordenacional" deste Guia.

SABER MAIS

Pode consultar, na "Página RGPD" do Somos Caixa, os seguintes documentos:
EDPB - Orientações 9/2022 sobre a notificação da violação de dados pessoais ao abrigo do RGPD

EDPB - Orientações 1/2021 sobre exemplos da notificação de uma violação de dados pessoais

Lei n.º 58/2019 - designadamente o Artigo 37º e seguintes, que estabelecem os limites e a classificação das contraordenações

CNPD - Deliberação 2019/494 – Desaplica normas da Lei n.º 58/2019

OS CGD 11/2023 - Regulamento da Proteção de Dados Pessoais (pontos 4.8.3., 4.8.4. e 6.1.3).

134.
As transferências internacionais de dados devem obedecer a regras específicas?

As transferências internacionais de dados pessoais efetuadas para fora do Espaço Económico Europeu (EEE) devem a obedecer a regras específicas e só poderão ocorrer se estiverem preenchidos determinados requisitos legais (art. 44.º e seguintes do RGPD).
Nomeadamente, o Responsável pelo Tratamento dos dados pessoais só pode efetuar transferências internacionais de dados se:

a) existir uma decisão de adequação (art. 45.º do RGPD);
b) se existirem garantias adequadas (art. 46.º do RGPD);
c) se tiverem sido adotadas regras vinculativas aplicáveis às empresas (art. 47.º do RGPD);
d) se o caso se enquadrar numa das derrogações previstas no art. 49.º, do RGPD.

135.
Em que consistem as transferências internacionais de dados com base numa decisão de adequação?

Designa-se por "decisão de adequação" a decisão adotada pela Comissão Europeia na qual reconhece que determinado país ou território assegura um nível de proteção adequado relativamente aos dados pessoais.

No caso de existir decisão de adequação relativamente a um país ou território, são permitidas as transferências de dados pessoais sem necessidade de garantias adicionais ou autorizações específicas.

136.
Em que consistem as transferências internacionais de dados sujeitas a garantias adequadas?

Na ausência de uma decisão de adequação, o Responsável pelo Tratamento pode efetuar transferências internacionais de dados quando

existam garantias adequadas e na condição de os Titulares dos Dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.
O RGPD indica vários tipos de garantias adequadas:

a) a existência de um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos;
b) a prévia aprovação de regras vinculativas aplicáveis às empresas;
c) a existência de cláusulas-tipo de proteção de dados adotadas pela Comissão;
d) a existência de cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão;
e) a existência de um código de conduta, 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, ainda,
f) a existência de um procedimento de certificação, 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.

137.
O que são regras vinculativas aplicáveis às empresas?

As regras vinculativas aplicáveis às empresas são regras aprovadas por uma Autoridade de Controlo (no caso português, a CNPD), relativamente a um grupo económico ou grupo de empresas, a seu pedido. Estas regras devem ser juridicamente vinculativas e aplicáveis a todas as entidades do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, incluindo os seus funcionários, as quais deverão assegurar o seu cumprimento, bem como, conferir expressamente aos Titulares dos Dados direitos oponíveis relativamente ao tratamento dos seus dados pessoais.
Além disso, para serem aprovadas pela Autoridade de Controlo, estas regras devem ainda respeitar todos os requisitos jurídicos constantes do n.º 2, do artigo 47.º, do RGPD.

138.
Fora das situações anteriores, é possível efetuar transferências internacionais de dados?

Fora das situações anteriormente elencadas, o Responsável pelo Tratamento poderá efetuar transferências internacionais de dados pessoais em casos excecionais elencados no art. 49.º, n.º 1, alíneas a) a g), do RGPD.
Ou seja, casos em que:

a) o Titular dos Dados tiver 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 seja necessária para a execução de um contrato entre o Titular dos Dados e o Responsável pelo Tratamento ou de diligências prévias à formação do contrato a pedido do Titular dos Dados;
c) a transferência seja necessária para a celebração ou execução de um contrato, celebrado no interesse do Titular dos Dados, entre o Responsável pelo Tratamento e outra pessoa singular ou coletiva;
d) a transferência seja necessária por importantes razões de interesse público;
e) a transferência seja necessária à declaração, ao exercício ou à defesa de um direito num processo judicial;
f) a transferência seja 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 seja realizada a partir de um

registo que, nos termos do direito da União ou do Estado-Membro, 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 no direito da União ou de um Estado-Membro se encontrem preenchidas nesse caso concreto.

139.
Quais as consequências do incumprimento das obrigações em matéria de transferências internacionais de dados?

As consequências do incumprimento pela CGD das obrigações em matéria de transferências internacionais de dados, bem como as coimas aplicáveis, podem ser consultadas na secção "Responsabilidade contra-ordenacional" deste Guia.

SABER MAIS

Pode consultar, na "Página RGPD" do Somos Caixa, os seguintes documentos:
EDPB - *Guidelines* 2/2024 *on Article 48* GDPR

EDPB - *Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*

EDPB - Orientações 7/2022 relativas à cerificação enquanto instrumento para as transferências

EDPB - Diretrizes 5/2021 sobre a interação entre a aplicação do artigo 3.º e as disposições relativas às transferências internacionais nos termos do capítulo V do RGPD

EDPB - Diretrizes 4/2021 relativas aos códigos de conduta enquanto instrumento para as transferências

EDPB - Diretrizes 2/2020 sobre a aplicação doa artigo 46.º, n.º 2, al. a) e do artigo 46.º, n.º 3, al. b) do Regulamento (UE) 2016/679 às transferências de dados pessoais entre autoridades e organismos públicos estabelecidos no EEE e fora do EEE

EDPB - Recomendações 1/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE

140.
Quais são as consequências do incumprimento dos princípios de tratamento?

O incumprimento, pelo Responsável pelo Tratamento, dos princípios de tratamento constitui um ilícito contraordenacional punível com coima até 20 000 000 EUR ou, no caso de uma empresa (CGD), até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

O Titular dos Dados lesado tem direito a interpor ação judicial contra a CGD (enquanto Responsável pelo Tratamento), bem como a receber desta uma indemnização pelos danos materiais ou imateriais que tiver sofrido.

141.
Quais são as consequências do incumprimento do dever de informação?

Se o Responsável pelo Tratamento não cumprir as obrigações legais relativas ao dever de informação dos Titulares dos Dados, esta sua conduta constitui um ilícito contraordenacional punível com coima até 20 000 000 EUR ou, no caso de uma empresa (CGD), até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

O Titular dos Dados lesado tem direito a interpor ação judicial contra a CGD (enquanto Responsável pelo Tratamento), bem como a receber desta uma indemnização pelos danos materiais ou imateriais que tiver sofrido.

142.
Quais são as consequências do incumprimento quanto ao exercício de direitos?

O desrespeito/incumprimento pelo Responsável pelo Tratamento relativo à resposta ao exercício dos direitos dos Titulares dos Dados constitui um ilícito contraordenacional punível com coima até 20 000 000 EUR ou, no caso de uma empresa (CGD), até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

O Titular dos Dados lesado pode também interpor ação judicial para reparação dos seus direitos contra a CGD (Responsável pelo Tratamento), bem como receber uma indemnização pelos danos materiais ou imateriais que tiver sofrido.

143.
Quais as consequências do desrespeito do consentimento do Titular dos Dados?

A violação, pelo Responsável pelo Tratamento, dos requisitos e obrigações relativos ao consentimento do Titular dos Dados constitui um ilícito contraordenacional punível com coima até 20 000 000 EUR ou, no caso de uma empresa (CGD), até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

O Titular dos Dados lesado tem direito a interpor ação judicial contra a CGD (enquanto Responsável pelo Tratamento), bem como a receber desta uma indemnização pelos danos materiais ou imateriais que tiver sofrido.

144.
Quais são as consequências do incumprimento do regular recurso a Subcontratante?

O incumprimento, pelo Responsável pelo Tratamento, das obrigações relativas à subcontratação constitui um ilícito contraordenacional punível com coima até 10 000 000 EUR (dez milhões de euros) ou, no caso de uma empresa (CGD), até 2% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior.

Caso o Titular dos Dados sofra danos materiais ou imateriais resultantes do recurso irregular a Subcontratante, poderá interpor ação judicial contra o Responsável pelo Tratamento (CGD), bem como a receber desta uma indemnização.

145.
Quais são as consequências do incumprimento do registo de atividades de tratamento?

O incumprimento, pelo Responsável pelo Tratamento (a CGD), das obrigações relativas ao registo de atividades de tratamento constitui um ilícito contraordenacional punível com coima até 10 000 000 EUR (dez milhões de euros) ou, no caso de uma empresa, até 2% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior.

146.
Quais as consequências se não efetuar uma DPIA que for devida?

A não realização pelo Responsável pelo Tratamento de uma DPIA nos casos em que seria devida constitui um ilícito contraordenacional, punível com coima até 10 000 000 EUR (dez milhões de euros) ou, no caso de uma empresa (CGD), até 2% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior.

147.
Quais as consequências do incumprimento das obrigações em matéria de violações de dados?

O incumprimento, pelo Responsável pelo Tratamento, das obrigações em matéria de violações de dados constitui um ilícito contraordenacional punível com coima até 10 000 000 EUR (dez milhões de euros) ou, no caso de uma empresa (CGD), até 2% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior.

O Titular dos Dados lesado tem direito a interpor ação judicial contra a CGD (enquanto Responsável pelo Tratamento), bem como a receber desta uma indemnização pelos danos materiais ou imateriais que tiver sofrido.

148.
Quais as consequências do incumprimento das obrigações em matéria de transferências internacionais de dados?

O incumprimento, pelo Responsável pelo Tratamento, das obrigações em matéria de transferências internacionais de dados constitui um ilícito contraordenacional punível com coima até 20 000 000 EUR (dez milhões de euros) ou, no caso de uma empresa (CGD), até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior.

O Titular dos Dados lesado tem direito a interpor ação judicial contra a CGD (enquanto Responsável pelo Tratamento), bem como a receber desta uma indemnização pelos danos materiais ou imateriais que tiver sofrido.

149.
Poderá haver outras consequências pela prática de uma contra-ordenação?

Além das coimas, podem ser aplicadas ao Responsável pelo Tratamento incumpridor um conjunto de sanções acessórias (por exemplo, limitação temporária ou definitiva do tratamento de dados; a proibição do tratamento de dados; bloqueio, apagamento obrigatório ou destruição total ou parcial dos dados pessoais; publicidade da condenação por período não inferior a 90 dias).

150.
Quais as consequências do incumprimento das obrigações em matéria de Proteção de Dados e Privacidade das Telecomunicações?

O incumprimento, pelo Responsável pelo Tratamento, das obrigações em matéria de proteção de dados e privacidade nas telecomunicações (Lei n.º 41/2004, de 18 de agosto, na redação dada pela Lei n.º 16/2022, de 16 de agosto) constitui um ilícito contraordenacional punível com coima mínima de 5000 (cinco mil euros) EUR e máxima de 5 000 000 (cinco milhões de euros) EUR, quando praticada por pessoas coletivas (CGD).

SABER MAIS

Pode consultar, na "Página RGPD" do Somos Caixa, os seguintes documentos:
EDPB - Diretrizes 4/2022 sobre o cálculo das coimas ao abrigo do RGPD

Lei n.º 58/2019 - designadamente o Artigo 37.º e seguintes, que estabelecem a classificação das contraordenações e os limites mínimos das coimas

Lei n.º 41/2004, de 18 de agosto (na redação dada pela Lei n.º 16/2022, de 16 de agosto) - Lei de Proteção de Dados e Privacidade nas Telecomunicações

CNPD - Deliberação 2019/494 – Desaplica normas da Lei n.º 58/2019, em especial quanto aos limites mínimos das coimas e critérios a ter em conta na determinação da medida da coima

151.
Em que consiste a responsabilidade criminal?

A Lei n.º 58/2019, de 8 de agosto, que assegura a execução na ordem jurídica interna do RGPD, prevê a responsabilidade criminal em matéria de proteção de dados relativamente aos Responsáveis pelo Tratamento, incluindo os titulares de cargos dirigentes e Colaboradores.
A responsabilidade criminal respeita aos cargos dirigentes e aos Colaboradores da CGD.
A CGD e as Entidades do Grupo CGD são passíveis de serem punidas criminalmente.

152.
Quantos crimes sobre proteção de dados consagra a Lei n.º 58/2019?

A Lei n.º 58/2019, de 8 de agosto, prevê 7 crimes puníveis com pena de prisão ou de multa.

153.
Em que consiste o crime de utilização de dados de forma incompatível com a finalidade da recolha?

O crime de utilização de dados de forma incompatível consiste na utilização de dados pessoais de forma incompatível com a finalidade determinante da respetiva recolha. Este crime é punido com pena de prisão até 1 ano, ou pena de multa até 120 dias.
A pena é agravada para o dobro no caso de se tratar de dados pessoais de categoria especial (raça, orientação sexual, saúde, entre outros).

EXEMPLO

A CGD recolheu dados pessoais do cliente no âmbito da abertura de conta de depósitos à ordem (finalidade: gestão de cliente).

Se, posteriormente, os dados recolhidos para a abertura de conta vierem a ser utilizados pela CGD, através da partilha dos mesmos com uma empresa de distribuição alimentar para esta promover uma qualquer iniciativa sob sua responsabilidade, esta conduta configurará o crime referido. Com efeito, esta transmissão de dados exige o consentimento expresso do cliente, uma vez que a sua finalidade não é compatível com a finalidade original para a qual os dados foram tratados.

154.
Em que consiste o crime de acesso indevido?

Incorre neste crime quem, sem a devida autorização ou justificação, aceder, por qualquer modo, a dados pessoais. Esta conduta é punida com pena de prisão até 1 ano, ou pena de multa até 120 dias. A pena é agravada para o dobro:

I) no caso de dados de categoria especial (raça, orientação sexual, saúde, entre outros);
II) o acesso for conseguido através de violação de regras técnicas de segurança;
III) tiver proporcionado benefício ou vantagem patrimonial ao autor ou a terceiros.

EXEMPLO

A técnica A, de uma Direção Central da CGD, não tem acesso a dados pessoais de clientes. No entanto, tem curiosidade em saber a nova morada, os saldos bancários e as aplicações financeiras de uma sua amiga, cliente da CGD. Para este efeito, esperou que o seu Colega B, que tem acesso à Plataforma de Balcão, se ausentasse para almoço, aproveitando para consultar a informação da amiga, naquela plataforma. A atuação da Colaboradora A configura a prática deste crime.

155.
Em que consiste o crime de desvio de dados?

Pratica este crime quem copiar, subtrair, ceder ou transferir – a título oneroso ou gratuito – dados pessoais sem previsão legal ou consentimento, independentemente da finalidade prosseguida, sendo punido com pena de prisão até 1 ano, ou pena de multa até 120 dias. A pena é agravada para o dobro:

I) caso os dados sejam de categoria especial (raça, orientação sexual, saúde, entre outros);
II) o acesso for conseguido através de violação de regras técnicas de segurança;
III) tiver proporcionado benefício ou vantagem patrimonial ao autor ou a terceiros.

EXEMPLO

M, Colaborador da CGD, copia os dados pessoais de clientes e colaboradores da região Norte para os ceder a um amigo CEO de uma *start up* tecnológica, para facilitar a expansão da sua carteira de clientes. A atuação de M configura a prática deste crime.

156.
Em que consiste o crime de viciação ou destruição de dados?

Incorre neste crime quem, sem a devida autorização ou justificação, apagar, destruir, danificar, ocultar, suprimir ou modificar dados pessoais, tornando-os inutilizáveis ou afetando o seu potencial

de utilização. Este crime é punido com pena de prisão até 2 anos, ou pena de multa até 240 dias. A pena pode ser agravada para o dobro se o dano produzido for particularmente grave.
A negligência é punida.

EXEMPLO

Um Colaborador de uma Direção Central sem autorização ou justificação, apaga ou destrói (ou danifica, oculta, suprime ou modifica) dados pessoais armazenados de um cliente em aplicações informáticas ou arquivos físicos respeitantes por exemplo, a contactos (morada, telefones, endereço de *email*) com vista a impedir a receção, por tal cliente, de comunicações emitidas pela CGD. Esta conduta configura a prática deste crime.

157.
Em que consiste o crime de inserção de dados falsos?

O crime de inserção de dados falsos consiste em inserir ou facilitar a inserção de dados pessoais falsos, com a intenção de obter vantagem indevida para si ou para terceiro, ou para causar prejuízo. Esta conduta é punida com pena de prisão até 2 anos, ou pena de multa até 240 dias. A pena é agravada para o dobro se resultar prejuízo efetivo da inserção de dados falsos.

EXEMPLO

Um Colaborador da Rede Comercial insere ou facilita a inserção de dados falsos relativos ao património financeiro de clientes, permitindo a concessão de crédito que resultará, por incumprimento, em prejuízos avultados para a CGD.

158.
Em que consiste o crime de violação do dever de sigilo?

Incorre neste crime quem, obrigado a sigilo profissional nos termos da lei, sem justa causa e sem o devido consentimento, revelar ou divulgar, no todo ou em parte, dados pessoais. Tal conduta é punida com pena de prisão até 1 ano, ou pena de multa até 120 dias. A pena é agravada para o dobro se o agente for:

I) Trabalhador em funções públicas ou equiparado;
II) *Data Protection Officer*;
III) determinado pela intenção de obter vantagem patrimonial ou outro benefício ilegítimo;
IV) puser em perigo a reputação, honra ou intimidade da vida privada de terceiros.

A negligência é punida.

EXEMPLO

C, Gestor de Clientes Caixa Azul na Região de Coimbra, recebeu um novo Cliente, que diz ter um vasto património familiar em Vilamoura. Este Cliente queria abrir conta e solicitar a concessão de um financiamento elevado, dando como garantia parte desse património.
C telefona ao seu amigo T, que é Gestor em Vilamoura num banco concorrente, partilha com ele informações (dados pessoais) do novo cliente, com vista a confirmar a existência do alegado património e as relações familiares.
Esta atuação de C configura a prática deste crime.

EXEMPLO

M, *pop star* internacional, tornou-se cliente Caixa Azul em Sintra, onde pretende adquirir um imóvel para residência e instalação de um estúdio com recurso ao crédito da CGD. Não obstante, o processo estar a ser acompanhado pelo Gestor Caixa Azul Z, os demais Colaboradores têm enorme curiosidade em saber a localização (e futura morada) de M, bem como confirmar se houve alguma entrada de verbas na conta de depósitos à ordem, dadas as notícias da comunicação social relativas à realização gratuita de um concerto recente.
Nas férias de Z, Gestor de M, o colega que o substitui faz uma consulta à conta, não fundamentada em qualquer pedido de M, para, finalmente, satisfazer a curiosidade e partilhar com os colegas, família e amigos as "novidades".
Esta atuação de C configura a prática deste crime.

159.
Em que consiste o crime de desobediência?

Pratica este crime quem não cumprir as obrigações previstas no RGPD e na legislação sobre proteção de dados, depois de ultrapassado o prazo que tiver sido fixado pela CNPD para o respetivo cumprimento.
Esta conduta é punida com pena de prisão até 1 ano, ou pena de multa até 120 dias. A pena é agravada para o dobro se notificado o agente:

I) não interromper, cessar ou bloquear o tratamento ilícito de dados;
II) não proceder ao apagamento ou destruição dos dados quando legalmente exigível ou findo o prazo legal de conservação;
III) recusar, sem justa causa, a colaboração solicitada e devida à CNPD.

EXEMPLO

A CGD não cessou, dentro do prazo fixado pela CNPD na sequência de interpelação da CGD para o efeito, os contactos telefónicos dirigidos a clientes que não prestaram consentimento positivo para receber comunicações de *marketing* direto.

160.
Há sanções acessórias de âmbito criminal?

Além das penas aplicáveis pela prática dos crimes relativos à proteção de dados, podem ser aplicadas acessoriamente:

- a proibição temporária ou definitiva do tratamento de dados pessoais, o bloqueio, o apagamento ou a destruição total ou parcial dos dados; ou
- a publicação da condenação, por meio de extrato contendo a identificação do agente, os elementos da infração e as sanções aplicadas, no Portal do Cidadão, por período não inferior a 90 dias, no caso de crimes ou coimas aplicadas de montante superior a 100 000 EUR (cem mil euros).

161.
Quem é a autoridade que controla a conformidade da aplicação do RGPD?

Em Portugal, a Comissão Nacional de Proteção de Dados (CNPD) é a autoridade que controla a conformidade da aplicação do RGPD.

162.
Quais são os poderes da Comissão Nacional de Proteção de Dados?

A Comissão Nacional de Proteção de Dados deixou de autorizar previamente os tratamentos de dados. A intervenção daquela Comissão é, essencialmente, inspetiva ou fiscalizadora. A CNPD pode, nomeadamente:

- Realizar investigações sob a forma de auditorias sobre a proteção de dados;
- Notificar o Responsável pelo Tratamento ou o Subcontratante de alegadas violações do RGPD;
- Obter acesso a todas as instalações do responsável pelo tratamento e do Subcontratante, incluindo os equipamentos e meios de tratamento de dados;
- Fazer advertências no sentido de que as operações de tratamento previstas são suscetíveis de violar as disposições do RGPD;
- Fazer repreensões sempre que as operações de tratamento tiverem violado o RGPD;
- Pronunciar-se no âmbito da emissão de projetos regulamentares;

- Ordenar:
  - Que lhe sejam fornecidas as informações de que necessite para o desempenho das suas funções;
  - Que se satisfaçam os pedidos de exercício de direitos apresentados pelo Titular dos Dados;
  - Que se tomem medidas para que as operações de tratamento cumpram as disposições do RGPD e, se necessário, de uma forma específica e dentro de um prazo determinado;
  - Que se comunique ao Titular dos Dados uma

violação de dados pessoais;
  - A retificação ou o apagamento de dados pessoais ou a limitação do tratamento nos termos dos artigos 16.º a 19.º do RGPD;
  - A suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais.

- Impor:
  - Limitações temporárias ou definitivas ao tratamento de dados, ou mesmo a sua proibição;
  - Coimas;
  - Retirar certificações.

163.
As autorizações concedidas pelas autoridades de controlo antes do RGPD mantém-se válidas?

As autorizações que tenham sido emitidas pelas autoridades de controlo com base na Diretiva 95/46/CE, permanecem em vigor até ao momento em que sejam alteradas, substituídas ou revogadas. Ou seja, as autorizações de tratamentos de dados pessoais emitidas pela CNPD, a favor da CGD, antes da aplicação plena do RGPD, permanecem válidas, desde que não contrariem as disposições do RGPD.

SABER MAIS

Pode consultar, na "Página RGPD" do Somos Caixa, os seguintes documentos:
EDPB - Orientações 8/2022 sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do Subcontratante

Lei n.º 58/2019, de 8 de agosto, lei que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 – Cf. art. 60.º

164.
Qual é a função da(o) *Data Protection Officer*?

Incumbe à (ao) *Data Protection Officer*:

- Informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do RGPD e de outras disposições de proteção de dados da União ou dos Estados-Membros;
- Controlar a conformidade com o RGPD, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do Responsável pelo Tratamento ou do Subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e a formação do pessoal implicado nas operações de tratamento de dados, assim como as auditorias correspondentes;
- Prestar aconselhamento no que respeita à avaliação de impacto sobre a proteção de dados e controlar a sua realização;
- Cooperar com a autoridade de controlo;
- Servir de ponto de contacto para a Comissão Nacional de Proteção de Dados sobre questões relacionadas com o tratamento;
- Assegurar a realização de auditorias, quer periódicas, quer não programadas;
- Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança, acompanhando os incidentes de segurança de dados, garantindo que as violações sejam tratadas

de acordo com os requisitos legais.
- Assegurar as relações com os titulares dos dados nas matérias abrangidas pelo RGPD e pela legislação nacional em matéria de proteção de dados.

A(O) *Data Protection Officer* atua com independência, não recebe instruções relativamente ao exercício das suas funções, tem competência própria e reporta diretamente à Comissão Executiva, nos termos previstos no RGPD.

165.
Qual é a função do *Data Protection Office*?

O *Data Protection Office* presta, em exclusivo, colaboração e assistência institucional à(ao) *Data Protection Officer* no exercício das suas funções. Nesse sentido, procede à pesquisa e divulgação de legislação e regulamentação relevante sobre proteção de dados e temas conexos; à elaboração de propostas de parecer, à realização de estudos; intervêm, participa e acompanha os temas de proteção de dados no âmbito de projetos internos (proteção de dados desde a conceção), sob a orientação da(o) *Data Protection Officer*, contribuindo para o controlo da conformidade.

166.
Qual o papel da(o) DPO no Grupo CGD?

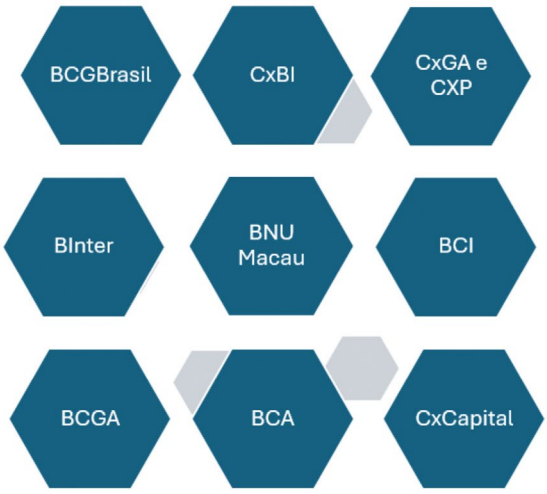
Considerando que o Grupo CGD desenvolve o seu negócio a nível nacional e internacional, a conformidade da sua atividade com a legislação sobre proteção de dados deve ser assegurada em todas as geografias e jurisdições correspondentes.

A importância da vertente corporativa da Função de Proteção de Dados decorre não só da consagração do "grupo empresarial" como entidade obrigada, mas também de o regime sancionatório resultante do RGPD fazer corresponder (quanto aos limites máximos das coimas aplicáveis em caso de incumprimento) o volume de negócios anual a nível mundial respeitante ao exercício financeiro anterior.

A(O) DPO corporativa(o) mantém diálogo e cooperação institucionais com as Entidades do Grupo CGD, nomeadamente através da partilha de documentação e informação, da realização de reportes e *confereces calls* regulares, por forma a promover uma estratégia coordenada de proteção de dados no Grupo CGD e a fomentar uma cultura organizacional de conformidade nesta matéria.

Sucursais

Filiais (domésticas e no estrangeiro)

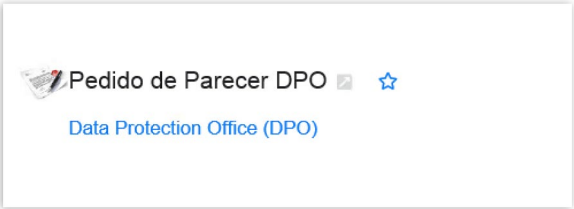


167.
Como se organizam os DPOS locais (Filiais) e os Pivots de Proteção de Dados (Sucursais)?

Nas Entidades CGD, a conformidade sobre a proteção de dados é assegurada de forma independente pelas estruturas locais, encabeçadas pelo *Data Protection Officers* nas Filiais e os *Pivots* de Proteção de Dados nas Sucursais, que asseguram, em estreita articulação com a(o) *Data Protection Officer* corporativa(o), a coordenação da gestão da proteção de dados nas respetivas entidades CGD.

168.
Como se processa a comunicação entre as Direções da CGD e as Entidades do Grupo CGD com a(o) *Data Protection Officer*?

A(O) *Data Protection Officer* pode ser contactada(o) por email ou através do "CA – Pedido de Parecer DPO", para pedidos de emissão de parecer. A caixa de correio eletrónico data.protection.officer@cgd.pt destina-se ainda ao exercício de direitos dos titulares dos dados e demais comunicação externa.



169.
Qual é a função dos *Pivots* de Proteção de Dados da CGD?

Os *Pivots* de Proteção de Dados são nomeados por cada uma das Direções da CGD e apoiam os respetivos Diretores de primeira linha, coordenando as atividades de proteção de dados nas respetivas Direções ou Estruturas organizacionais. Articulam a sua atividade com o *Data Protection Office* no que respeita à identificação, avaliação, acompanhamento e controlo dos riscos de proteção de dados, cumprindo e fazendo cumprir a legislação de proteção de dados e os deveres aplicáveis às respetivas áreas de negócio, de suporte e demais atividades. Os *Pivots* de Proteção de Dados têm as seguintes responsabilidades:

a) Controlar o cumprimento das obrigações legais, de conduta e outros deveres aplicáveis sobre proteção de dados;
b) Identificar os riscos sobre proteção de dados e respetivas medidas de mitigação, garantindo o respetivo acompanhamento e a monitorização contínua da atividade da respetiva Direção ou Estrutura organizacional para conformidade em matéria de proteção de dados;
c) Comunicar à(ao) *Data Protection Officer*, com conhecimento das respetivas hierarquias, as situações detetadas de não conformidade sobre proteção de dados, bem como as respetivas ações corretivas adotadas.

170.
Qual a relação entre a(o) *Data Protection Officer* e as obrigações do Regulamento DORA (*Digital Operational Resilience Act*)?

O Regulamento DORA e o papel da (o) *Data Protection Officer* estão interligados, especialmente no contexto da segurança e resiliência das tecnologias de informação e comunicação (TIC) das instituições financeiras:

- O DORA impõe requisitos rigorosos para garantir a segurança das TIC, incluindo a proteção de dados pessoais. A(O) *Data Protection Officer* tem um papel crucial na colaboração relativa à supervisão e implementação de políticas que assegurem a conformidade com esses requisitos.
- O DORA exige que as instituições financeiras estabeleçam mecanismos robustos de governo interno e gestão de risco relacionados às TIC. A(O) *Data Protection Officer* deve garantir que as práticas de proteção de dados estejam integra-

das nesses mecanismos, promovendo a resiliência operacional.
- O DORA obriga as instituições a monitorizar continuamente a segurança das TIC. A(O) *Data Protection Officer* deve colaborar na criação de processos de monitorização que incluam a proteção de dados pessoais, assegurando que qualquer vulnerabilidade seja rapidamente identificada e mitigada.

171.
Qual a relação entre a(o) *Data Protection Officer* e a aplicação do artigo 27.º do Regulamento da Inteligência Artificial (RIA)?

O artigo 27.º do RIA trata da conformidade dos sistemas de IA com os riscos de segurança e proteção de dados. O papel da(o) *Data Protection Officer* na aplicação deste artigo é crucial para garantir que os sistemas de IA operam de forma segura e em conformidade com as normas de proteção de dados.

A(O) *Data Protection Officer* colabora na realização de avaliações de risco para identificar e mitigar possíveis vulnerabilidades nos sistemas de IA e na implementação de medidas de segurança adequadas para proteger os dados pessoais tratados.

Estas responsabilidades ajudam a assegurar que os sistemas de IA operem de maneira ética e segura, protegendo os direitos dos Titulares dos Dados e promovendo a confiança na tecnologia.

SABER MAIS

Pode consultar, na "Página RGPD" do Somos Caixa, os seguintes documentos:
2023 *Coordinated Enforcement Action*
Designation and Position of Data Protection Officers

WP29 Orientações sobre Encarregados de Proteção de Dados

OS CGD 11/2023 – Regulamento da Proteção de Dados Pessoais

OS CGD 20/2018 – Política de Proteção de Dados Pessoais

ELEMENTOS DE APOIO

Legislação
Regulamento (UE) 2016/679, de 27 de abril de 2016 (RGPD)
Regulamento (UE) 2024/1689 (Regulamento da Inteligência Artificial)
Regulamento (UE) 2022/2554, de 14.12.2022 (DORA)
Lei n.º 58/2019, de 8 de agosto - Lei que assegura a execução, na ordem jurídica nacional, o RGPD
Lei n.º 59/2019, de 8 de agosto - Aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais
Lei n.º 41/2004, de 18 de agosto - Lei de Proteção de Dados e Privacidade nas Telecomunicações
Lei n.º 75/2021, de 18 de novembro - Consagra o direito ao esquecimento de pessoas que tenham superado ou mitigado situações de risco agravado de saúde ou de deficiência, tendo em vista melhorar o acesso ao crédito e a contratos de seguro destas pessoas.

CNPD
CNPD Diretriz 1/2023 - Sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais
CNPD Diretriz 1/2022 - Sobre comunicações eletrónicas de marketing direto
CNPD - Deliberação 2019/494 - Desaplica normas da Lei n.º 58/2019
CNPD - Regulamento n.º 1/2018 - DPIA - Lista de Avaliação de Impacto sobre a Proteção de Dados de realização obrigatória

CGD - Proteção de Dados
Política de Privacidade e Proteção de Dados Pessoais
Política de Cookies
OS CGD 20/2018 (V4) - Política de Proteção de Dados Pessoais
OS CGD 11/2023 - Regulamento da Proteção de Dados Pessoais

CGD - Outras matérias
OS CGD 10/2025 - Política de Subcontratação do Grupo CGD
IS CGD 15/2022 - Processo de Subcontratação de Funções da CGD
MP Manual de Procedimentos 45/2020 - Procedimentos de Gestão Documental: Arquivo Físico e Digital

EDPB - *European Data Protection Board*
EDPB - *Guidelines 1/2025 on Pseudonymisation*
EDPB - *Guidelines 2/2024 on Article 48 GDPR*
EDPB - *Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*
EDPB - *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*
EDPB - Relatório sobre aplicação do direito de acesso pelos Responsáveis pelo Tratamento
EDPB - *2023 Coordinated Enforcement Action Designation and Position of Data Protection Officers*
EDPB - Orientações 9/2022 sobre a notificação da violação de dados pessoais ao abrigo do RGPD
EDPB - Orientações 8/2022 sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do Subcontratante
EDPB - Orientações 7/2022 relativas à cerificação enquanto instrumento para as transferências
EDPB - Orientações 1/2022 sobre o Direito de Acesso
EDPB - Diretrizes 5/2021 sobre a interação entre a aplicação do artigo 3.º e as disposições relativas às transferências internacionais nos termos do capítulo V do RGPD

EDPB - Diretrizes 4/2021 relativas aos códigos de conduta enquanto instrumento para as transferências
EDPB - Orientações 1/2021 sobre exemplos da notificação de uma violação de dados pessoais
EDPB - Diretrizes 8/2020 sobre o direcionamento para os utilizadores das redes sociais
EDPB - Orientações 7/2020 sobre os conceitos de Responsável pelo Tratamento e Subcontratante no RGPD
EDPB - Diretrizes 2/2020 sobre a aplicação doa artigo 46.º, n.º 2, al. a) e do artigo 46.º, n.º 3, al. b) do Regulamento (UE) 2016/679 às transferências de dados pessoais entre autoridades e organismos públicos estabelecidos no EEE e fora do EEE
EDPB - Diretrizes 5/2020 relativas ao consentimento na aceção do Regulamento 2016/679
EDPB - Recomendações 1/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE
EDPB - Diretrizes 5/2019 relativas aos critérios do direito a ser esquecido pelos motores de busca ao abrigo do RGPD
EDPB - Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados desde a Conceção e por Defeito

WP29 – *Article 29 Working Party*
WP29 2017/260 - Orientações relativas à transparência na aceção do Regulamento 2016/679
WP29 2017/251 - Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679
WP29 2017/248 - Orientações relativas à avaliação de impacto sobre a proteção de dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco»
WP29 2016/243 - Orientações sobre encarregados de proteção de dados
WP29 2016/242 - Orientações sobre o direito à portabilidade dos dados

EBA - *European Banking Authority*
EBA/GL/2019/02 - Orientações relativas à subcontratação

ENISA - *European Union Agency for Cybersecurity*
ENISA *Data Pseudonymisation: Advanced Techniques and Use Cases (2021)*
ENISA *Pseudonymisation techniques and best practices (2019)*