SEGURANÇA 4.0

Guia RGPD

Guia prático para aplicação das medidas de proteção de dados, incluindo as áreas de gestão de sistemas de informação e proteção e privacidade de dados

APSEI
ASSOCIAÇÃO PORTUGUESA DE SEGURANÇA

apsei.org.pt

Elaborado por:

Bureau Veritas

Cofinanciado por:

COMPETE 2020

PORTUGAL 2020

UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

Autores.

Bureau Veritas

Jorge Mendes

Revisão Jurídica

Carla Sofia Neto

Projeto gráfico e paginação

Raquel Magalhães Mendes

Edição

Dezembro de 2021

Índice.

Privacidade no contexto atual.

A cibersegurança em geral, e a proteção de dados pessoais em particular, são cada vez mais importantes para melhorar a competitividade no mundo dos negócios, impulsionada pelas vantagens da conectividade, imediatismo e omnipresença para a inevitável transformação digital.

Nos últimos anos a segurança dos sistemas de informação também designada por cibersegurança tornou-se uma prioridade para as empresas, em particular do nosso setor. Prova disso são as mudanças que têm ocorrido na regulamentação Europeia e nacional, mudanças essas que representam desafios significativos para as nossas organizações.

Em 2014 — É publicado o Regulamento sobre identificação eletrónica e serviços de confiança (eIDAS) **[1]**. Regulamento (UE) 910/2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.

Em 2015 — Sai a Diretiva de Serviços de Pagamento (PSD2) **[2]**. Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro, relativa aos serviços de pagamento no mercado interno. Esta diretiva tem como intuito o desenvolvimento do mercado interno de pagamentos eletrónicos que se aplica aos prestadores do setor das instituições financeiras e do comércio eletrónico.

Em 2016 — A Diretiva NIS (network and information security)/ SRI (segurança das redes e da informação) **[3]**. Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. A Diretiva NIS para segurança em redes e sistemas de informação, que insta os Estados-Membros a estarem equipados e preparados para responder a incidentes de grande escala, e que é aplicável a operadores de serviços essenciais (energia, transporte, bancos, mercados financeiros, saúde, abastecimento de água potável e infraestrutura digital) e fornecedores de serviços digitais (mercados online, motores de busca online e serviços na nuvem).

Ainda em 2016, é publicado o **Regulamento Geral de Proteção de dados, RGPD** **[4]**, relativo à proteção de dados pessoais, que se encontra especificada no Regulamento Geral de Proteção de dados, RGPD. Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, também chamado de GDPR quando utilizada a sigla em inglês, e este aplica-se a todas as empresas que realizam processamento de dados pessoais.

Em 2019 — A Diretiva dos direitos de autor e direitos conexos no mercado único digital **[5]**. Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos direitos de autor e direitos conexos no mercado único digital.

Neste contexto, é importante que as empresas examinem a sua situação de segurança da informação e a forma como estão organizadas, em particular as suas políticas de privacidade

além das definidas pelos seus fornecedores de serviços digitais, uma vez que a confiança dos seus clientes, e com ela a sua própria competitividade, está em jogo.

Poderíamos dizer que o RGPD é amplo, uma vez que empresas de todas as dimensões e dos diversos setores são abrangidas. É um facto que os titulares, ao interagirem com as empresas, utilizam cada vez mais a tecnologia, como por exemplo, redes sociais, aplicações móveis e lojas online. Nestas interações, trocam uma grande quantidade de informações e dados de identificação pessoal, hábitos de compra e preferências que, por sua vez, são essenciais para o sucesso e estratégia das empresas. Mas os titulares dos dados estão cada vez mais conscientes do valor da sua privacidade, e não estão dispostos a serem localizados quando não era suposto que o fossem ou serem discriminados por causa do seu perfil, e muito menos de serem vítimas indiretas de uma fuga massiva de dados dos seus fornecedores ou lojas de confiança, ou de serem vítimas de roubo de identidade.

O que é o RGPD.

A preocupação com a privacidade não é nova. Já em Janeiro de 1981, o Conselho Europeu adotou a Convenção para a proteção de pessoas no que diz respeito ao tratamento automatizado de dados pessoais. A Convenção 108 [6], foi mais tarde revista para incluir questões como proteção em redes sociais, perfis ou no local de trabalho. Desde 2006, celebra-se a 28 de janeiro, o Dia da Proteção de Dados na Europa, em comemoração da assinatura deste acordo.

Em 2000, a Carta dos Direitos Fundamentais da UE incluiu no seu artigo 8º a "Proteção de dados pessoais"[7].

Em 2004 Portugal transpôs para a ordem jurídica nacional a Diretiva da Proteção de dados pessoais e privacidade nas telecomunicações [8].

Com a entrada em vigor do Tratado de Lisboa em dezembro de 2009, a Carta dos Direitos Fundamentais da UE tornou-se juridicamente vinculativa e, portanto, elevou o direito à proteção de dados pessoais à categoria de direito fundamental independente do direito à privacidade.

A Estratégia Europa 2020 do Conselho Europeu é construída em torno de 7 pilares, um dos quais é a Agenda Digital para a Europa, que promove a criação de um Mercado Único Digital Europeu gratuito e seguro, no qual as empresas podem vender em toda a UE e os cidadãos podem fazer compras online além—fronteiras. A estratégia para um mercado único digital foi adotada em maio de 2015.

No âmbito desta estratégia da harmonização foram promovidos os regulamentos acima mencionados, incluindo a privacidade de dados pessoais, com o objetivo de criar um quadro de confiança para que um mercado interno digital se desenvolva com segurança jurídica e transparência para os titulares. Estes esforços culminaram na publicação do Regulamento Geral de Proteção de Dados (RGPD) [4].

Este regulamento Europeu, torna-se o sucessor dos atuais regulamentos de proteção de dados de todos os países membros. No caso português este regulamento foi transporto para o nosso ordenamento jurídico pela LEI DA PROTEÇÃO DE DADOS PESSOAIS — Lei n.º 58/2019, de 08 de Agosto[9]. Mas também em Portugal esta preocupação não é nova. Já a Constituição CRP (Constituição da República Portuguesa) tem no seu Artigo 35.º, sob a epígrafe "Utilização da informática" preocupações com a cibersegurança e a privacidade dos dados do cidadão [10].

O RGDP tem por base dois conceitos fundamentas: Privacidade *by design* (desde a conceção) e Privacidade *by defult* (por defeito).

Na proteção de dados, o responsável pelo tratamento é obrigado a aplicar, tanto no momento de definição dos meios de tratamento *by design* como no momento do próprio tratamento,

as medidas técnicas e organizacionais adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento para que cumpra os requisitos do RGPD e proteja os direitos dos titulares dos dados.

Além dos princípios de privacidade e dos direitos dos indivíduos sobre os seus dados pessoais, este regulamento trata dos seguintes aspetos:

INFORMAR	OBTER CONSENTIMENTO	GARANTIR DIREITOS	NOTIFICAR VIOLAÇÕES
Tratamento	Inequívoco	Que podam exercê-los	Que colocam em risco a privacidade
Decisões automatizadas	Não tácito		
Perfis	Expresso em caso de dados de especial proteção	De acordo com os prazos do RGPD	A autoridade de controlo (CNPD*)
Transferências internacionais			Aos detentores dos dados

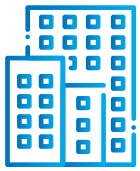
***CNPD**
Comissão Nacional de Proteção de Dados

3.1

Conceitos chave.

As cinco figuras fundamentais do RGDP são:

1



DATA PROTECTION OFFICER (EPD/DPO)

As organização têm de nomear um EPD/DPO se realizarem operações de tratamento de dados pessoais e/ou sensíveis de forma regular ou sistemática

2

SUBCONTRATANTE

Pessoa singular ou coletiva que trata os dados pessoais por conta do responsável pelo tratamento

3

TITULAR DOS DADOS

Pessoa singular residente na UE

4

RESPONSÁVEL PELO TRATAMENTO

Pessoa singular ou coletiva que determina as finalidades e os meios do tratamento de dados pessoais

5

AUTORIDADE DE CONTROLO

Autoridade pública independente, responsável pela fiscalização da aplicação do RGPD

O Artigo 4º do RGPD contém um conjunto de definições, para efeitos de aplicação do RGPD, algumas destas definições serão explicitadas nesta secção.

Dados pessoais

«Dados pessoais» — informação relativa a uma pessoa singular identificada ou identificável «titular dos dados». É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular *(texto extraído do Artigo 4º do RGPD).*

Exemplos: Nome, números de identificação (BI/CC [11], NIF, carta de condução, passaporte), endereços de identificação e localização. Físicos como por exemplo a morada, eletrónicos tais como endereço de email, página web, página de Facebook, etc., número de telefone, estado civil, identificador de cliente da Via Verde, IP de um computador ou matrícula de um automóvel.

«Dados sensíveis» — estão sujeitos a condições de tratamento específicas, os dados que estão abrangidos por esta classificação são os seguintes:

A origem racial ou étnica; as opiniões e filiações políticas e sindicais; as convicções religiosas ou filosóficas; dados genéticos; dados biométricos que permitam identificar uma pessoa de forma inequívoca; dados relacionados com a saúde; dados sobre a vida sexual ou orientação sexual da pessoa, bem como dados pessoais relacionados com condenações penais e infrações. (*Artigo 4.º, nos 13, 14 e 15; artigo 9.º e artigo 10.º do RGPD*).

Exemplos de dados não considerados pessoais: N.º de registo de uma empresa; endereço de correio eletrónico tipo info@empresa.pt (Nota: o email manuel@empresa.pt é um dado pessoal); dados anonimizados.

Exemplos de dados Biométricos: Leitura facial e de digital com indicador por equipamento.

Exemplo de dados Genéticos: Resultado e informações de testes genéticos clínicos e não clínicos.

Exemplo de dados relacionados com a saúde: A ficha de aptidão, esta deve ser arquivada em local seguro seja fisicamente ou em suporte informático com acesso restrito.

Tratamento de dados

Princípios base do tratamento de dados

Transparência — O tratamento deve ser feito de forma lícita, leal e transparente em relação ao titular dos dados;

Finalidade — Os dados devem ser recolhidos para finalidades determinadas e explícitas e não podem ser tratados posteriormente para finalidades diversas;

Minimização — Os dados recolhidos devem ser limitados ao que é necessário relativamente às finalidades para os quais são tratados;

Precisão — Os dados devem ser exatos e atualizados sempre que necessário e quando forem inexatos devem ser corrigidos ou eliminados;

Conservação — Os dados devem ser conservados apenas durante o período necessário para a concretização das finalidades para que foram recolhidos;

Integralidade e confidencialidade dos dados — Os dados devem ser tratados de uma forma que garanta a sua segurança, protegendo-os de tratamentos não autorizados ou ilícitos e contra a sua perda, destruição ou danificação;

Responsabilidade — O responsável pelo tratamento é responsável pelo cumprimento das normas do RGPD;

«Tratamento» — uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição; *(texto extraído do Artigo 4º do RGPD);*

Exemplos de operação de tratamento: O tratamento ou processamento de dados é normalmente efetuado através de sistemas ou ferramentas informáticas como:

- Processamento salarial e gestão de pessoas;
- Destruição de documentos que contenham dados pessoais;
- Recolha de elementos identificativos num serviço de receção;
- Email;
- Processamento de texto;
- Bases de dados (Access) e Folhas de cálculo (Excel);
- Software de ERP ou CMR;
- Página nas redes sociais, Facebook, LinkdIn, WhatsApp, Instagram, ou website com divulgação de informações com dados pessoais;
- Colocação de fotografias pessoais em websites;
- Newsletter com dados pessoais.

As operações executadas nestes sistemas ou ferramentas que envolvam dados pessoais estão abrangidas pelo RGPD. As operações podem ser simples:

- Informação pessoal num documento Word ou Excel;
- Envio de um email com informações pessoais;
- Introdução, alteração ou remoção de dados num ERP ou CRM; outros *softwares* de marcação de ponto, salários, etc.

Ou mais complexas:

- Alteração de um algoritmo que processa dados pessoais;
- Um *backup* dos servidores onde são armazenados dados pessoais;
- Migração de um sistema entre servidores ou para um serviço de *cloud*;
- Migração de dados sensíveis para *upgrade* de *software*.

«Limitação do tratamento», a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro; *(texto extraído do Artigo 4º do RGPD);*

«Tratamento transfronteiriço», o tratamento de dados pessoais que ocorre no contexto das atividades de estabelecimentos em mais do que um Estado—Membro de um responsável pelo tratamento ou um subcontratante na União, caso o responsável pelo tratamento ou o subcontratante esteja estabelecido em mais do que um Estado—Membro; ou

O tratamento de dados pessoais que ocorre no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, mas que afeta substancialmente, ou é suscetível de afetar substancialmente, titulares de dados em mais do que um Estado-Membro *(texto extraído do Artigo 4º do RGPD).*

Tratamento de dados Sensíveis

É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. (...) — RGPD, Art. 9.ª, 1.

Raça ou etnia | **Opinião política** | **Crença religiosa** | **Filiação sindical** | **Dados biométricos** | **Dados de saúde**

«Dados genéticos», os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa;

«Dados biométricos», dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos *(texto extraído do Artigo 4º do RGPD)* (por exemplo, altura, peso, conotações físicas diversas; genética, impressões digitais ou imagens faciais);

«Dados relativos à saúde», 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 *(texto extraído do Artigo 4º do RGPD)* (por exemplo, dados relativos a consultas médicas ou baixas médicas, Síndromas, doenças, Desempenho físico ou mental, Dados de diagnósticos como pressão arterial ou ECG, Dados e medicina no trabalho [12]).

Responsáveis pelo tratamento

«Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado—Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado—Membro; *(texto extraído do Artigo 4º do RGPD).*

É a entidade que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais.

Subcontratante e outros

«Subcontratante», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes; *(texto extraído do Artigo 4º do RGPD).* É a entidade que trata os dados pessoais por conta do responsável pelo tratamento.

Exemplos: uma empresa que procede ao processamento de salários, uma empresa que armazena o arquivo de documentos e processos administrativos de uma outra empresa. Como por exemplo o contabilista da empresa.

«Destinatário», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou dos Estados—Membros não são consideradas destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento; *(texto extraído do Artigo 4º do RGPD).*

«Terceiro», a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais; *(texto extraído do Artigo 4º do RGPD).*

Exemplos: uma empresa que, para prestar assistência informática, necessite de aceder a dados pessoais, um trabalhador que tenha como funções proceder à introdução de dados pessoais num ficheiro informático.

Outras definições

«Definição de perfis», 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, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações; *(texto extraído do Artigo 4º do RGPD).*

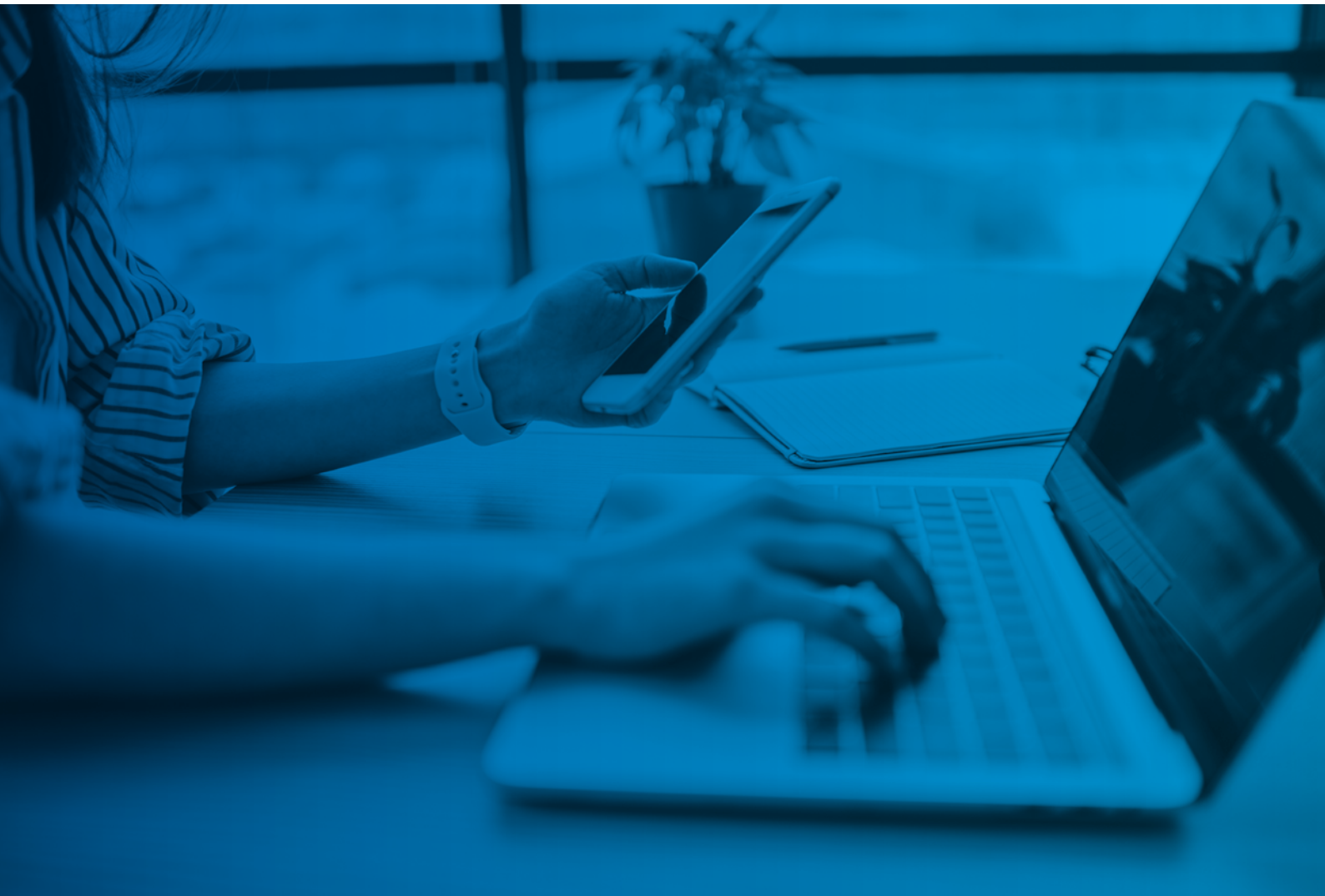
«Anonimização», tornar ou ficar anónimo. Técnica de tratamento automático de informação para que determinados dados deixem, de forma irreversível, de poder ser atribuídos ao seu titular.

«Pseudonimização», o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de 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; *(texto extraído do Artigo 4º do RGPD).*

«Ficheiro», qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico; *(texto extraído do Artigo 4º do RGPD).*

«Consentimento», do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, 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; *(texto extraído do Artigo 4º do RGPD).*

«Violação de dados pessoais», uma 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; *(texto extraído do Artigo 4º do RGPD).*



4.1

Aplicação do RGPD à empresa.

Princípios relativos ao tratamento de dados pessoais

Princípio da Licitude, Lealdade e Transparência — (Art.5º —1—a) — O tratamento dos dados pessoais deve assentar numa das causas de licitude do tratamento previstas no artigo 6.º do RGPD.

Princípio da Limitação das Finalidades — (Art.5º —1—b) — Os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas, e não podem ser tratados posteriormente de uma forma incompatível com essas finalidades.

Princípio da Minimização dos dados — (Art.5º —1—c) — Só devem ser tratados dados que sejam adequados, pertinentes e necessários à finalidade estabelecida.

Princípio da exatidão — (Art.5º —1—d) — Os dados devem ser exatos, e atualizados sempre que necessário. Os dados inexatos devem ser apagados ou retificados sem demora.

Princípio da Limitação da Conservação — (Art.5º —1—e) — Os dados devem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período estritamente necessário para as finalidades para as quais são tratados.

Princípio da Integralidade e Confidencialidade — (Art.5º —1—f) — Os dados devem ser tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental **[13]**.

Fundamentos de legitimidade para o tratamento de dados

Consentimento — (Art.6º1—a) — O responsável pelo tratamento deve obter do titular dos dados uma declaração de vontade livre, informada, explícita e inequívoca.

Nota: o consentimento exige um ato expresso e positivo. O pedido de consentimento deve ser apresentado de modo inteligível e de fácil acesso, e numa linguagem clara e simples. Não são admitidos consentimentos tácitos nem opções pré-validadas. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento.

Relação contratual — (Art.6º1—b) — Os dados são necessários para a execução de um contrato no qual o titular é parte.

Exemplo: para pagar o vencimento aos trabalhadores, os serviços têm de dispor de dados pessoais seus, como o NIF e um número de conta bancária. Não é necessário o consentimento para o tratamento desses dados.

Obrigação jurídica — (Art.6º1—c) — Os dados são necessários para o cumprimento de uma obrigação legal a que o responsável pelo tratamento está sujeito.

Exemplo: uma norma que determine que devem ser identificados todos os trabalhadores da empresa que, para o exercício das suas funções, tenham que ter Registo Criminal. Não é necessário o consentimento para o tratamento desses dados.

Interesses vitais — (Art.6º1—d) — O tratamento de dados pessoais também deverá ser considerado lícito quando for necessário à proteção de um interesse essencial à vida do titular dos dados ou de qualquer outra pessoa singular.

Interesse público — (Art.6º1—e) — Os dados são necessários ao exercício da autoridade pública ou de funções de interesse público.

Exemplo: Interesses vitais - Um hospital está a tratar um doente que sofreu um acidente rodoviário grave. O hospital não precisa do consentimento do doente para pesquisar a sua identidade e verificar se a pessoa existe na base de dados do hospital, a fim de consultar o seu processo clínico ou os contactos dos familiares mais próximos.

Interesse público - uma investigação pública ou averiguações que envolvam dados pessoais.

Interesses legitimidade — (Art.6º1—f) — A empresa deve documentar e identificar expressamente o fundamento da licitude do tratamento, e a finalidade a que se destina **[14]**. A legitimidade no âmbito das relações laborais está definida no Artigo 28.º da LPDP [9] "O empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais" (*texto extraído do Artigo* 28.º da LPDP*).*

Direitos dos titulares dos dados

Os titulares dos dados pessoais, podem exercer, de acordo com o RGPD, os seus direitos, que são 8, e se esquematizam da seguinte forma:

1 — Direito de informação — (Art.13º+14º) — Direito de receber informações sobre os termos do tratamento de dados pessoais aquando da sua recolha. Deve ser prestada a seguinte informação ao titular dos dados:

- Quem é o responsável pelo tratamento e respetivos contactos;
- Quem são os subcontratantes da proteção de dados e respetivos contactos;
- Quais as finalidades do tratamento em causa;
- O prazo de conservação dos dados ou, se tal não for possível, os critérios para definir tal prazo, se o tratamento se basear no consentimento, a existência do direito de retirar tal consentimento;
- Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;

- Quando os dados pessoais não são recolhidos junto do titular, devem ainda ser prestadas as seguintes informações adicionais: os destinatários ou categoria de destinatários dos dados pessoais, se aplicável, a origem dos dados e a categoria dos mesmos.

Nota: a prestação de informação pelo responsável ao titular dos dados deve ser registada, de modo a garantir a prova dessa prestação por parte do responsável.

---

2 — Direito de acesso — (Art.15º) — Direito de obter confirmação de que os dados pessoais são ou não objeto de tratamento e, se for o caso, ter acesso aos seus dados pessoais; com as seguintes informações:

- Quais os fins do tratamento;
- Quais os dados pessoais em causa;
- Quais os destinatários dos dados;
- Qual o prazo de conservação dos dados;
- Se os dados não tiverem sido recolhidos junto do titular, qual a origem desses dados;
- Qual a forma de exigir a retificação ou o apagamento dos dados.

Nota: É reconhecido o direito ao titular dos dados obter uma cópia dos dados pessoais objeto do tratamento. Poderá ser oferecido ao interessado o acesso remoto a um sistema seguro que permita o acesso direto aos seus dados.

---

3 — Direito de retificação — (Art.16º) — O titular tem o direito de obter, sem demora injustificada a retificação ou atualização dos dados pessoais inexatos. O titular dos dados pode exigir a retificação/alteração dos dados que lhe digam respeito e que não correspondam à verdade. Tem também, o direito de exigir que os seus dados sejam completados, caso se encontrem incompletos.

Nota: a retificação/alteração deve fazer-se no mais curto período de tempo possível.

---

4 — Direito de apagamento dos dados (Art.17º) (direito a ser esquecido) — O titular tem o direito de obter o apagamento dos seus dados pessoais, sem demora injustificada, dentro dos limites legalmente previstos;

O titular dos dados tem o direito de exigir o apagamento de dados, nomeadamente, nas seguintes situações:

- Quando os dados pessoais deixem de ser necessários para a finalidade que motivou a sua recolha;
- Quando o titular retire o consentimento em que se baseia o tratamento dos dados, nos casos em que a lei o permite;
- Quando os dados tenham sido tratados ilicitamente.

Nota: O exercício do direito ao apagamento não pode afetar, designadamente:

- O cumprimento de obrigações legais;
- Razões de interesse público na área da saúde pública;
- O tratamento para fins de arquivo público, investigação científica e histórica e fins estatísticos;
- O exercício de direitos em processos judiciais.

---

5 — Direito à limitação de tratamento — (Art.18º) — O titular dos dados tem o direito de obter a limitação do seu tratamento. O titular dos dados pode exigir junto do responsável pelo tratamento que o tratamento seja limitado a determinados dados.

6 — Direito de Portabilidade — (Art.20º) — O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido num formato de uso corrente e de leitura automática;

Sempre que o tratamento seja informatizado e feito com base no consentimento, o titular dos dados tem:

- o 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;
- o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável inicial o possa impedir;
- o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.

Exemplo: uma pessoa dirige-se a um hospital e solicita que os exames médicos que realizou nesse hospital sejam transmitidos a uma outra unidade hospitalar ou a um médico em particular. O hospital deve transmitir esses dados.

7 — Direito de não ficar sujeito a decisões individuais automatizadas — (Art.22º) — O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado dos seus dados pessoais, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

O titular dos dados pode opor-se a qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar dados pessoais para avaliar e determinar características do titular dos dados, designadamente para prever aspetos relacionados com a sua situação económica, tendências comportamentais, saúde e interesses (definições de perfis/*profiling*).

Profiling: qualquer forma de tratamento automatizado de dados pessoais que consiste na utilização de dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, em particular para analisar ou prever aspetos relacionados com o desempenho profissional, situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou movimentos dessas pessoas. " Art. 4 GDPR.

8 — Direito de oposição — (Art.21º) — O titular dos dados tem o direito de se opor, a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, nomeadamente quando os seus dados sejam tratados para efeitos de comercialização direta.

Quando seja exercido o direito de oposição, o responsável pelo tratamento deve cessar o tratamento, salvo se razões imperiosas e legítimas justificarem a prossecução desse tratamento.

Os titulares dos dados pessoais também têm o direito de ser notificados (Art. 34 RGPD) de forma clara, simples e sem demora quando sofrer uma violação de segurança (ver nota) que envolva um alto risco para os seus direitos e liberdades, indicando um contacto para obter mais informações, as consequências da violação e as medidas que podem ser tomadas.

Nota: "Violação de segurança de dados pessoais: qualquer violação de segurança que cause destruição, perda ou alteração acidental ou ilegal de dados pessoais transmitidos, armazenados ou de outra forma processados ou comunicação ou acesso não autorizado a tais dados." Art. 4 GDPR.

INFORMAR	OBTENHA CONSENTIMENTO	DIREITOS DE GARANTIA	DENUNCIAR/NOTIFICAR VIOLAÇÕES
• Tratamento • Decisões automatizadas • Perfis • Transferências internacionais	• Inequívoco • Não tácito • Expresso em caso de dados de proteção especial	• Que possam ser exercidos • De acordo com os prazos do GDPR	• Que representem riscos para a privacidade • À autoridade • Aos titulares dos dados

O titular dos dados tem direito a apresentar queixa individualmente ou por meio de associações junto da (CNPD) Comissão Nacional de Proteção de dados e exigir indemnização por danos pelo tratamento ilícito dos seus dados pessoais.

Responsável pelo exercício dos direitos

É necessário garantir que haverá um responsável por analisar os pedidos dos titulares dos dados para o exercício dos seus direitos e assuma a responsabilidade de responder a tais pedidos. Mesmo que na empresa não seja requerida a nomeação de um EPD/DPO, recomendamos que o faça, este colaborador será a única via de comunicação entre o titular dos dados e a empresa na resposta ao exercício dos direitos. Importa ter em atenção que estas respostas deverão ser dadas no prazo máximo de 30 dias.

Obrigações do responsável pelo tratamento

É fundamental avaliar os riscos no tratamento de dados pessoais, para determinar se temos um risco elevado ou baixo para os direitos das pessoas titulares dos dados. Podemos dizer que são de alto risco, quando por exemplo, aqueles que processam dados de categorias especiais (dados Sensíveis), os que realizam tratamento de dados de:

- Saúde — Exemplos: Ficha de aptidão [15]; comunicação de baixas médicas; dados de medicina no trabalho [12]; comunicação de uma gravidez, ect [14].
- Que envolvam informação de natureza judicial — Exemplo: Registos criminais, penhora de salários, infrações;
- Seguro — Exemplos: Acidentes de trabalho, acidentes rodoviários, seguros de saúde;
- Atividades políticas ou sindicais — Exemplo: Filiação partidária e/ou sindical, cotas do sindicato;
- Convicções religiosas, étnicas ou raciais — Restrições alimentares por motivos religiosos ou étnicos;
- Dados de videovigilância, biométricos ou geolocalização;
- Dados relativos à vida sexual ou à orientação sexual;
- Dados de menores (em Portugal menores de 13 anos) — Todos os dados relativos aos filhos dos funcionários incluindo o nome.

Aqueles que realizam processamento massivo de dados, como por exemplo:

- Serviços de telecomunicações,
- Entidades bancárias e financeiras,
- Geração e uso de perfis,
- Publicidade.

Podemos por oposição dizer que são de baixo risco, os que realizam apenas tratamentos de dados com contacto pessoal de clientes ou fornecedores, dados básicos associados às questões dos recursos humanos.

Inventariação de dados

Todos os responsáveis pelo tratamento devem proceder ao diagnóstico e à inventariação das operações de tratamento de dados, incluindo a inventariação dos sistemas informáticos que tratam dados pessoais, tendo em conta:

1. Que dados possuo?
2. Que condição de licitude me permite tratá-los?

3. Para que finalidade são recolhidos?
4. As operações de tratamento respeitam os princípios consagrados no artigo 5.º do RGPD (licitude, lealdade e transparência)?
5. Quem é que recolhe e trata os dados?
6. De que forma estou a documentar a conformidade com as regras do RGPD?
7. Os contratos assinados com subcontratantes (quando existam) oferecem garantias de respeito pelo RGPD?
8. Onde é que os dados são conservados, e como é que são protegidos?
9. Em caso de quebra de segurança, quais os procedimentos definidos?
10. Que mecanismos estão implementados para garantir a prestação de informações aos titulares dos dados e facilitar o efetivo exercício dos seus direitos?

Registo de operações de tratamento

A empresa e os seus subcontratantes devem proceder ao registo das operações de tratamento de dados, do qual conste:

- Nome e contactos do responsável;
- Finalidades do tratamento;
- Descrição das categorias de titulares dos dados e das categorias dos dados;
- Categorias dos destinatários;
- Transferência de dados para países terceiros ou organizações internacionais;
- Se possível, prazos de conservação;
- Se possível, uma descrição das medidas técnicas e organizativas no domínio da segurança;
- A obrigação de registo não existe para entidades com menos de 250 trabalhadores, mas
- é recomendável até porque nas empresas existem tratamentos de dados que;
- Pode implicar um risco para os direitos, liberdades e garantias do titular dos dados;
- Abranja as categorias especiais de dados (dados sensíveis) ou dados pessoais relativos a condenações penais e infrações.

Operações de tratamento: O tratamento abrange um amplo conjunto de operações efetuadas sobre dados pessoais, por meios manuais ou automatizados. Inclui **a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão** ou qualquer outra

forma de disponibilização, **a comparação ou interconexão, a limitação, o apagamento ou a destruição** de dados pessoais.

O Encarregado de Proteção de Dados (EPD/DPO)

O RGPD, diz que é o responsável pelo tratamento que nomeia o EPD, que ofereça garantias para a aplicação de medidas técnicas e organizacionais para que o tratamento de dados seja efetuado de acordo com os requisitos do regulamento [16].

O EPD pode ser por exemplo, do suporte tecnológico ou jurídico, interno ou externo, que contratamos para cumprir o Regulamento. A relação entre o Responsável e o EPD deve ser formalizada num contrato vinculativo. O conteúdo mínimo deste contrato deve incluir:

- Objeto, duração, natureza e propósito do tratamento;
- Tipos de dados pessoais e categorias de partes interessadas;
- Obrigação do EPD de tratar dados pessoais apenas seguindo as instruções documentadas do responsável do tratamento;
- Condições para que o EDP possa dar sua autorização prévia, específica ou geral, para as subcontratações;
- Prestar apoia ao responsável, sempre que possível, na resposta ao exercício dos direitos das partes interessadas.

Quando é necessário um EPD/DPO

Nota: Embora o Artigo 91º do RGPD defina o que são tratamento de grande escala, ele não define um número. Para determinar se o tratamento é em larga escala, recomenda-se considerar estes fatores:

- O número de partes interessadas afetadas, seja como um número específico ou como uma proporção da população correspondente;
- O volume de dados ou a variedade de elementos de dados que estão sujeitos a tratamento;
- A duração, ou permanência, da atividade de processamento de dados;
- O âmbito geográfico da atividade de processamento.

São funções do Encarregado de Proteção de Dados:

- Informar e aconselhar o responsável pelo tratamento, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações em matéria de proteção de dados;
- Verificar se as obrigações constantes do RGPD e da lei estão a ser cumpridas;
- Cooperar com a autoridade de controlo (CNPD), servindo de ponto de contacto;
- Servir de ponto de contacto dos titulares dos dados relativamente a todas questões relacionadas com o tratamento dos seus dados pessoais;
- Assegurar que, em todas as fases do tratamento, desde a recolha à destruição, são observados os princípios do registo e tratamento de dados.

Responsabilidade proativa

A responsabilidade proactiva implica que o responsável pelo tratamento deve aplicar as medidas técnicas e organizacionais adequadas para garantir e poder demonstrar que o tratamento está de acordo com o Regulamento.

Para aplicar medidas de responsabilidade proativa deve ter por base, tal como no Sistema de Gestão da Qualidade o pensamento baseado em risco, tendo em consideração a natureza, âmbito, contexto e propósitos do tratamento, bem como o risco para os direitos e liberdades dos titulares dos dados. Na prática, isto pressupõe que algumas medidas (por exemplo, avaliação de impacto (AIPD) ou a nomeação do EDP/DPO) serão aplicadas apenas quando existe um alto risco e os restantes (por exemplo, privacidade por Design) serão adaptados ao nível e tipo de risco que os tratamentos apresentam. A responsabilidade proactiva concretiza-se com medidas como:

a. manter um registo das operações de tratamento nos casos em que é obrigatório;

b. adotar e adaptar as diferentes medidas com base na análise dos riscos do tratamento e direitos e liberdades do titular dos dados;

c. aplicar a proteção da privacidade desde o projeto *design* e por defeito *default* para garantir que os titulares possam exercer seus direitos e a segurança de seus dados pessoais;

d. notificar as violações da segurança dos dados à CNPD e às pessoas afetadas, a menos que seja improvável que representem um risco para os direitos e liberdade das pessoas afetadas;

e. realizar uma avaliação de impacto sobre a proteção de dados no tratamento que apresentam alto risco para os direitos e liberdade das pessoas;

f. nomear um EPD/DPO quando for necessário.

Análise de risco e a análise de impacto de proteção de dados (AIPD)

Para saber se a sua empresa é obrigada a manter um registo das operações de tratamento ou nomear um EDP/DPO e/ou para realizar uma avaliação de impacto, é necessário que o responsável faça uma avaliação contínua dos riscos que o tratamento de dados representam para os direitos e liberdade dos titulares dos dados. Esta análise também servirá para estabelecer o resto das medidas de responsabilidade de uma forma proativa.

Caso se trate de uma grande empresa, certamente já existirá uma metodologia própria ou de acordo com uma norma para a análise de riscos para a segurança da informação. Algumas Normas sobre Sistemas de Gestão de Risco tais como a NP ISO 31000:2018 — Gestão do Risco ou a ISO/IEC 27005:2018, *Information technology — Security techniques — Information security risk management* ou mais especificamente para riscos de privacidade ISO / IEC 27701 é uma norma especifica que fornece requisitos e diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um sistema de gestão de privacidade da informação (SGPI), podemos dizer por outras palavras que é uma norma de suporte ao RGPD.

Para começar a realizar a análise de risco de privacidade **[17]**, deve:

- Identificar todas as fontes de dados pessoais do tratamento, catalogar todos os agentes responsáveis e os tipos de operações que são feitas com estes dados.
- Seja exaustivo com os dados que são recolhidos: onde são armazenados? Por quanto tempo? Num ficheiro ou numa base de dados? Eles seguem os princípios do tratamento GDPR?
- Faça um diagrama com o fluxo de dados do tratamento, ou seja, desde que os recolhe até que sejam usados ou eliminados com transformações intermédias.
- Analisar em primeiro lugar os intervenientes envolvidos no tratamento e ações problemáticas sobre os dados, ou seja, aquelas que podem ter um efeito adverso na privacidade das pessoas.

Para a proteção da privacidade, o objetivo da análise de riscos é determinar se o tratamento tem consequências negativas para as pessoas como a marginalização, exclusão social, dificuldades de acesso a um emprego, problemas na contratação de serviços, etc.

Análise da necessidade de realização de avaliação de impacto de proteção de dados (AIDP)[18], descrição das atividades de processamento, ou para documentar a análise de riscos e para o registo das atividades de tratamento do responsável. Para começar, poderá verificar se respondeu sim a estas perguntas:

1. Os dados especialmente protegidos são processados de forma sistemática e em grande escala?
2. Estão incluídos dados de um grande número de pessoas ou grandes quantidades de dados dos titulares?
3. Os dados de menores são processados de forma significativa ou não acidental?
4. O tratamento tem como finalidade avaliar ou prever aspetos pessoais dos titulares ou do seu comportamento?
5. O tratamento inclui a criação de perfis para qualquer finalidade, incluindo o envio de publicidade personalizada?
6. Os dados obtidos dos titulares são cruzados com outros dados disponíveis noutras fontes?
7. Pretende utilizar os dados obtidos para uma determinada finalidade, numa nova finalidade mais intrusiva?
8. Está a tratar dados em grande volume com técnicas de análise massiva, como *Big Data*?
9. São tecnologias particularmente invasivas para a privacidade, como *drones* ou relacionados a geolocalização, videovigilância, biometria, RFID ou certas aplicações da internet das coisas (IoT)?
10. Os dados serão transferidos ou comunicados a terceiros que antes não tinham acesso a eles?
11. Os dados serão transferidos para países fora da EU (União Europeia) que não possuem uma declaração de adequação?
12. Se vai entrar em contacto com pessoas de uma forma particular intrusiva?
13. Vai utilizar dados pessoais não dissociados ou não anonimizados de forma irreversível para fins de pesquisa estatística, histórica ou de investigação científica?
14. Existem riscos específicos que podem comprometer a confidencialidade, integridade ou disponibilidade de dados pessoais?

Se respondeu afirmativamente a uma ou mais das questões acima, a sua empresa é uma das que deve fazer uma avaliação de impacto e consultar previamente a CNPD [18].

A avaliação de risco resultará na adoção das medidas necessárias para eliminar ou mitigar

os riscos que o produto ou serviço pode acarretar para a proteção dos dados das pessoas. A avaliação de impacto permitirá aplicar privacidade desde o projeto *by Design*, evitando custos da mitigação de risco à *posteriori*.

Algumas técnicas que podem ser adotadas desde o projeto são: anonimização, pseudonimização, criptografia, controlo de acesso (autenticação) e rastreabilidade, proteção perímetral, VPN, redes sem fio seguras, etc. Algumas medidas organizacionais são: formação, treino e consciencialização, definição e comunicação de políticas, separação de funções, etc.

Notificação de violações de segurança dos dados pessoais

As violações de dados pessoais traduzem-se em quebras de segurança que provocam a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais.

Exemplos: um trabalhador perde o portátil que contém dados pessoais, envio de um e-mail com dados pessoais para um destinatário errado, cópia sem autorização de bases contendo dados pessoais para dispositivos móveis (telemóveis, *pen drives, tabletes* ect.).

Nota: em caso de violação de dados pessoais, o responsável pelo tratamento deve notificar a CNPD no prazo de 72 horas após ter tido conhecimento dela **[19 e 20]**.

A notificação deve:

- Descrever a natureza da violação dos dados pessoais;
- Comunicar o nome e os contactos do EPD;
- Descrever as consequências prováveis da violação de dados pessoais;
- Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais.
- O responsável pelo tratamento deve registar as violações de dados pessoais, bem como os factos com elas relacionadas, os respetivos efeitos e a medida de reparação adotada.

Nota: quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos, liberdades e garantias de pessoas singulares, o responsável pelo tratamento deve comunicar a violação de dados pessoais ao titular dos dados sem demora injustificada, em linguagem clara e simples.

A obrigação de comunicação ao titular dos dados não existe se se verificar um dos seguintes casos:

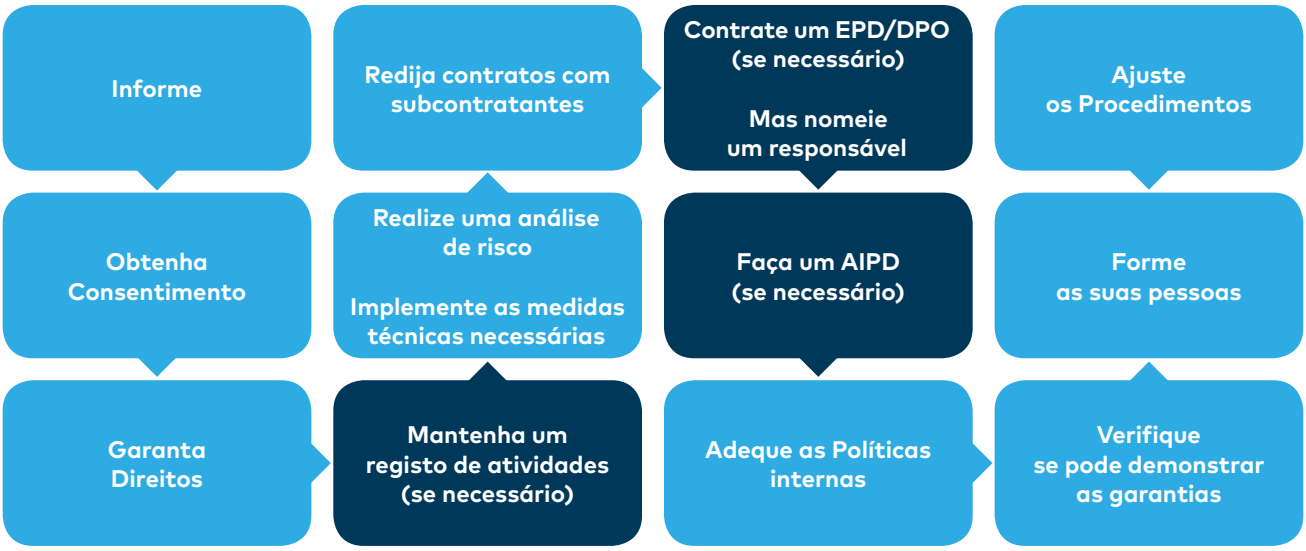
- O responsável pelo tratamento tiver aplicado aos dados pessoais afetados medidas de proteção adequadas, especialmente medidas que tornem os dados pessoais incompreensíveis (cifragem, anonimização, pseudonimização);
- O responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o risco não se concretizará; ou a comunicação implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante.

5.1

Medidas de segurança a aplicar.

Já dissemos que a proteção da privacidade no âmbito do RGPD deve ser feita de forma proativa, tomando precauções para garantir os direitos e liberdades dos titulares no que diz respeito aos seus dados pessoais. Por exemplo, fornecer—lhes informações sobre o tratamento, obter o seu consentimento inequívoco e expresso, ou possibilitar formas simples para que possam exercer os seus direitos ARCO (**Acesso** à Informação, **Retificação**, **Cancelamento** ou Esquecimento e **Oposição**), portabilidade, e limitação do tratamento.

De uma forma resumida este fluxograma identifica as medidas básicas a tomar.



Estas não são as únicas medidas que deve tomar na empresa para dar garantias aos titulares dos dados, fornecedores e funcionários sobre os seus dados pessoais. Todo o pessoal envolvido no tratamento deve estar empenhado na segurança dos dados e na garantia dos direitos dos titulares dos mesmos. Por isso:

- O seu suporte de Tecnologias de Informação e o seu suporte jurídico sejam internos ou externos terão que rever contratos, adequar políticas e ajustar procedimentos para garantir que os tratamentos são confiáveis,
- Os restantes membros da equipa devem compreender as mudanças e serem capaz de executá-las.

Além disso, não devemos apenas ser capazes de fornecer garantias sobre os dados às pessoas, devemos estar preparados para ser capazes de demonstrar que o fazemos corretamente.

Nas empresas e dependendo do seu tamanho, e do tipo de processamento que realizam e das categorias de dados que processam, deverão tomar diferentes medidas organizacionais, como nomear um EPD/DPO ou realizar uma análise de impacto. Ter-se-á também que alterar as políticas e procedimentos internos para que, entre outras coisas, saber como agir em caso de incidente ou fazer com que todos os envolvidos no tratamento estejam conscientes das garantias que devemos oferecer e como aplicar a segurança nos tratamentos.

Em qualquer caso, e após a realização de uma avaliação dos riscos dos nossos tratamentos para a privacidade das pessoas, também teremos que adotar diferentes medidas técnicas. Exemplos dessas medidas são a pseudonimização, a encriptação, os mecanismos de garantia da confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços dedicados ao processamento, ou restaurar o acesso em caso de incidente e, em qualquer dos casos, a verificação da sua eficácia.

Medidas organizacionais

Já identificamos algumas medidas organizacionais que devem ser tomadas na empresa, sendo que algumas delas em certos casos são obrigatórias:

- Registos de atividades de tratamento, esta medida nem sempre é obrigatória, mas é recomendável que o faça;
- Contratos entre o responsável **[21]** e subcontratante **[22]**, caso confie o tratamento a terceiros.

Medidas organizacionais das responsabilidades atribuídas ao responsável ou ao EPD/DPO se for o caso:

- Determinar a existência de dados pessoais, classificá-los e documentar a sua existência, verificar se não estão incorretos e se foram compartilhados dados incorretos, informar para que sejam corrigidos.
- Identificar os tratamentos dos dados pessoais, documentá-los e verificar os fundamentos legais que os justificam, entre outros, rever a forma como obteve o consentimento e como garante os direitos.
- Analisar os riscos apresentados pelos tratamentos para os direitos dos titulares de uma forma contínua, para garantir um nível adequado de segurança em extensão e profundidade, dependendo da natureza dos dados, tipos de tratamento, número de afetados e outros tratamentos realizados pela empresa.
- Implementar avaliações de impacto se realizar tratamentos de alto risco.
- Estabelecer um procedimento, como parte de um plano de resposta a incidentes,

para comunicar as violações de segurança à CNPD [19 e 20], sem demoras e dentro de 72 horas, e aos dos titulares dos dados afetados se envolver um alto risco para sua privacidade.

- Ter os meios para aplicar medidas de proteção de dados desde o projeto e por defeito, como por exemplo reduzir ao mínimo os dados pessoais a serem processados, pseudonimizando o mais rápido possível e dando transparência ao tratamento para permitir a supervisão.

Elaborar ou rever e disponibilizar os meios para aplicar políticas internas de proteção de dados, incluindo políticas relativas à atribuição de responsabilidades, conscientização, formação, treino e auditorias. Formar todos os funcionários que participam no tratamento:

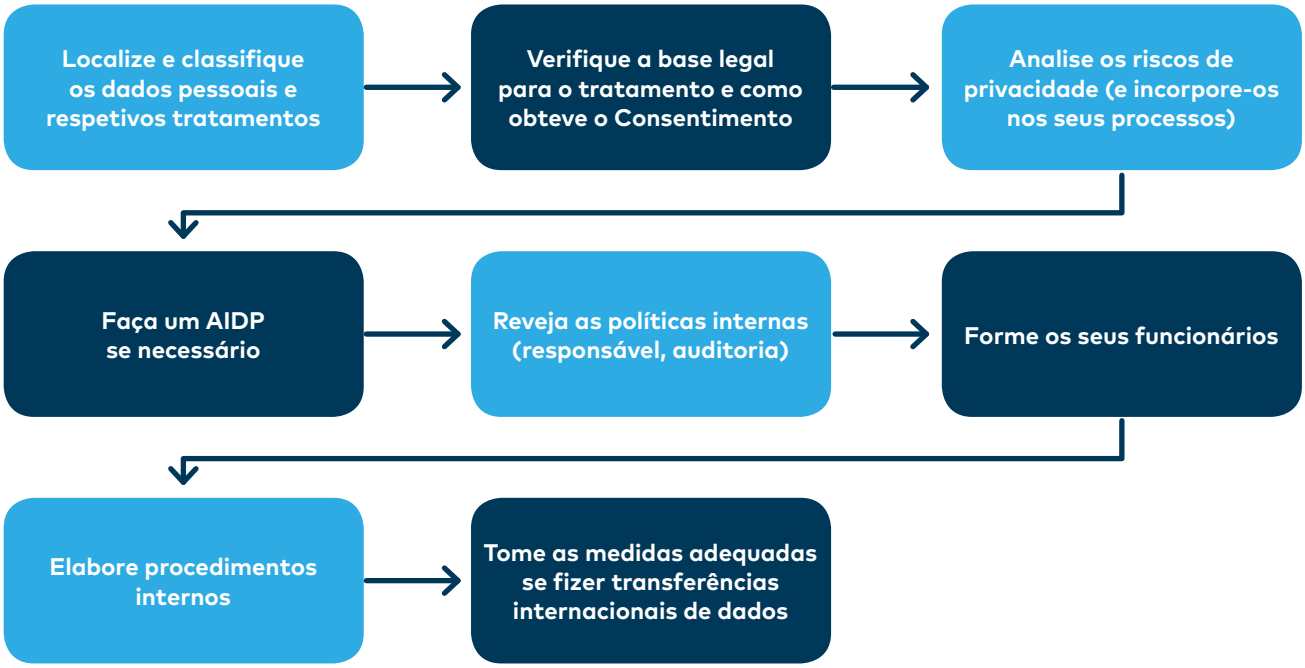
- Nos direitos que têm de assegurar e nos procedimentos para fazer cumprir esses direitos;
- No dever de confidencialidade e sigilo, tornando-os participantes das políticas para que evitem o acesso de terceiros aos dados e divulgação acidental, apliquem as medidas para o correto armazenamento e destruição segura de suportes e assinem acordos de confidencialidade que vão além do fim dos seus contratos;

Elaborar e divulgar procedimentos internos para os colaboradores que intervêm no tratamento que em qualquer caso deve contemplar o conhecimento dos direitos e requisitos de transparência do RGPD.

Se os seus tratamentos incluem transferências internacionais para países fora da UE ou com os quais não há acordo:

- Elaborar ou rever, e fornecer os meios para aplicar as políticas relacionadas às transferências internacionais dentro do grupo empresarial.
- Implementar auditorias para garantir a conformidade com os regulamentos vinculativos relativos à proteção de dados dentro de um grupo empresarial e métodos para garantir ações corretivas para proteger os direitos das pessoas.
- Estabelecer um ponto centralizado para lidar com uma autoridade nacional, por exemplo, para gerir reclamações de titulares, se a empresa estiver estabelecida em vários países.

Este fluxograma resume a sequência das ações a implementar



Exemplos de boas práticas de proteção de dados ao nível organizacional

Importa antes de mais, enumerar todos os dados que se encontram em suporte físico tais como (recibos de vencimento, justificação de faltas e outros) e garantir que os mesmos se encontram guardados num local que garanta a sua segurança e integridade.

O armazenamento dos documentos físicos, sobretudo os que contenham dados sensíveis, deve privilegiar locais de acesso restrito e condicionado e que ofereçam garantias de segurança e à prova de vulnerabilidades, perda, destruição e outros.

Os dossiês e documentos que contenham dados pessoais não poderão ser arquivados em local de fácil acesso, ou expostos em secretárias ou locais de fácil acesso por parte de terceiros ou de trabalhadores que não devam ter acesso a essa informação. Uma boa prática é definir uma política de secretária limpa.

O envio de informação sensível por correio e a utilização de correio registado com aviso de receção são uma das várias medidas possíveis de segurança dos dados.

Tratamento de dados em suporte físico:

- Minimizar a disponibilidade e o fácil acesso a documentos físicos;
- Política de proibição de fotografar documentos com dados pessoais;
- Controlo de todas as fotocópias e documentos com dados pessoais para que não possam ser utilizadas como folhas de rascunho ou outras finalidades que impliquem a sua dispersão e acesso por parte de terceiros;
- Não transportar dossiês e documentos com dados pessoais, a menos que tal seja estritamente inevitável.

Medidas Técnicas

As medidas técnicas que também podemos designar de Segurança de Informação (SI) devem obedecer aos seguintes princípios base:

Confidencialidade, Integridade e Disponibilidade (*CID*).

Confidencialidade, é uma propriedade de que a informação esteja disponível somente às pessoas autorizadas.

Integridade da informação, é uma propriedade que garante que a informação não sofra alteração indevida.

Disponibilidade, é uma propriedade de estar acessível e utilizável quando necessário.

Procedimentos, políticas e formação são essenciais para o cumprimento do RGPD, mas a tecnologia pode auxiliar em todo o processo, desde a recolha de dados até a destruição final.

Além da implementação das medidas nos procedimentos técnicos utilizados para notificar em caso de violações e para informar os "donos" dos dados sobre os tratamentos, obter o seu consentimento e garantir que podem exercer os seus direitos (acesso, eliminação dos seus dados, portabilidade, oposição, objeção ao marketing direto e à definição de perfis,...), nesta secção iremos identificar alguns tipos de ferramentas para o ajudar a garantir a segurança dos dados pessoais e, por consequência a cumprir o RGPD.

Pode começar por fazer uma avaliação às capacidades de cibersegurança da sua empresa, com a ferramenta Ciberchecku p do CNCS é simples, pode aceder e experimentar. "Acessível no link disponibilizado nas referências" **[23]**.

Nesta matriz identificamos algumas destas ferramentas e a sua utilização:

	ÂMBITO DE APLICAÇÃO				
TIPO	**Gestão de acessos e identidade**	**Segurança no posto de trabalho**	**Segurança nas aplicações de dados**	**Segurança nos sistemas**	**Segurança na rede**
Antifraude *Anti—phishing, Anti—spam,* ferramentas de filtragem de navegação UTM, *Appliance*		✓	✓	✓	✓
Anti—malware Anti—vírus, *AntiAdware, Anti—spyware,* UTM, *Applicince*		✓	✓	✓	✓
Auditoria técnica Análise de logs e portas, vulnerabilidades, auditoria de palavras passe *(passwords)*, auditoria de sistemas e arquivos	✓		✓		✓
Certificação de acordo com as normas de SGSI, análise de risco, planos e políticas de segurança, normas de segurança		✓	✓	✓	✓
Contingência e continuidade Ferramentas de gestão de planos de contingência e continuidade, Backups, infraestrutura de *backup*, Virtualização, Nuvem *(Claud)*		✓	✓	✓	✓
Controlo de acesso e autenticação Controlo de acesso à rede, NAC, Gestão de identidade e autenticação, *Single Sign—On,* Certificados digitais, Assinatura eletrónica	✓				
Conformidade legal Ferramentas de conformidade legal (RGPD LPDP, ect.), Eliminação segura, destruição de documentos	✓	✓	✓		
Inteligência de segurança Gestão de eventos de segurança, *SIEM, Big Data,* ferramentas de monitorização e *reporting*			✓	✓	✓
Prevenção de fuga de informações Controlo de conteúdo Gestão de confidencial, ciclo de vida da informação, ferramentas de criptografia		✓	✓		✓
Proteção de comunicação *Firewall,* VPN, IDS, IPS, UTM, *Appliance,* Filtro de conteúdo, P2P, Gestão e controle de largura de banda		✓	✓	✓	✓
Segurança de dispositivo móvel Segurança de dispositivo móvel, segurança de rede sem fio, *BYOD*		✓			✓

Password segura — para ser segura tem de ter no mínimo 8 dígitos (o CNCS recomenda no mínimo 12 **[24]**) e têm que ser composta por letras Maiúsculas (A,B,C), e minúsculas (a,b,c), Números (7,8,9) e símbolos (@ # $ % ^ & *). Para facilitar a memorização da sua *Password*, relacione-a com um passatempo ou desporto favorito, Por exemplo: *Gosto de jogar badmington* poderia tornar-se GstdjgB@dm1nt()n. Escrever a *password* num "post-it" e/ou partilhá-la com os colegas de trabalho é uma regra básica de segurança. A gestão de palavras passe/ password não uma regra imposta pelo RGPD mas é recomendável.

PC portátil — Deverá garantir que o disco rígido deste está encriptado (usando, por exemplo "*Bitlocker*"). Isto garante que, em caso de roubo da máquina, mesmo removendo o disco rígido e colocando-o noutro PC, não haverá acesso aos dados. Esta ferramenta é grátis com a licença Windows.

BYOD (Bring *Your Own Device* / traga seu próprio dispositivo) Este conceito permite aumentar a mobilidade no ambiente empresarial, dando às pessoas a liberdade de usarem seus próprios dispositivos — *smartphones*, *tablets* ou *notebooks* — durante o período de trabalho para aceder a informações nos sistemas da empresa, mas para isto ser possível é fundamental estarem muito bem definidas as regras de segurança e utilização destes equipamentos.

Terminais — Quer que sejam Windows, Linux ou Apple, os terminais deverão estar preparados para que o acesso aos mesmos só possa ser efetuado através de *username* e *password*. Os terminais devem ter antivírus atualizados, bem como *firewalls* locais ativas e efetivas. Recomendamos a leitura das publicações da CNCS - Centro Nacional de Cibersegurança, boas práticas no uso de password **[24]** e boas práticas de cibersegurança **[25]**.

Acesso à internet — Os titulares não devem ter acesso a sites não fidedignos (verifique se o site que vai consultar em *HTTPS* (*Hyper Text Transfer Protocol Secure* — protocolo de transferência de hipertexto seguro ou seja se começa com: https://www.xxxx). Isto consegue-se utilizando um servidor de Proxy interno e/ou firewall para segregar a rede interna da internet e mitigar ataques.

Acesso aos sistemas da empresa do exterior — O teletrabalho veio aumentar a necessidade de acesso remoto a recursos internos da rede, para uma maior segurança use uma VPN (*Virtual Private Network*).

Uso de CRM ou ERP online — Assegure-se de que a password de acesso é forte, que a aplicação cumpre com os requisitos, como por exemplo, no caso da "portabilidade" dos dados, todos os dados do cliente podem ser exportados para um ficheiro CSV - (Comma-Separated Values) e entregues por meio digital.

Uso de base de dados simples em Access ou Excel — Deverá ser protegida por password forte, e ser guardada no servidor ou PC numa pasta privada e também ela protegida por password.

Uso de impressoras — Nunca deve imprimir um documento com dados pessoais ou confidenciais, sem ter a certeza de que estes não serão vistos ou consultados por terceiros que não deveriam ter acesso aos mesmos. Muitas impressoras centralizadas possibilitam *confidential printing*. Ao imprimir o documento, introduza um PIN. Neste caso para que o documento seja impresso é necessário ir até à impressora e introduzir este PIN.

Gestão de Newsletters — Serviços como Mailchimp possuem todos os automatismos para cumprir com o RGPD. Caso o serviço que usa não tenha um link de *Unsubscribe* ou "Remover da lista" não estará a cumprir com o RGPD, logo aconselha-se a trocar de serviço. Caso tenha um sistema de newsletter interno é absolutamente imperativo que tenha em atenção que, aquando do envio do email, por exemplo, a partir da caixa de correio da empresa, os recipientes da mensagem vão em "BCC" e não em "CC" ou "Para". Quando o envio é feito em "CC" ou "Para" os endereços dos recipientes são mostrados, e isto configura uma clara violação de conformidade do RGPD.

Transferência de informação via internet — caso tenha necessidade de transferir um grande volume de dados não deve ser usado esta forma de envio. Os ficheiros devem ser encriptados. Devemos garantir que após bom recebimento o ficheiro é apagado. Serviços como *Wetransfer* não são aconselhados, pois o link para o ficheiro online pode ser partilhado com terceiros. Serviços como *Onedrive*, permite dar acesso apenas aos destinatários, usando o seu email. Permite ainda que os ficheiros possam ser apagados após confirmação da receção.

Limitação do acesso a PC Portáteis ou terminais — Proteja o seu computador do roubo de informações. Bloqueie o seu computador através das teclas CTRL + ALT + DEL ou em alternativa **Windows + L**, mesmo que deixe o seu local de trabalho por um curto espaço de tempo.

Para minimizar todas as janelas que possam conter informação confidencial ou sensível, dever-se-á utilizar a combinação de teclas **windows + D**.

Certificação do Sistema de Gestão de Segurança e Informação (SGSI) de acordo com a norma NP ISO/IEC 27001 (Tecnologias de informação; Técnicas de segurança; Sistemas de gestão de segurança da informação).

Implementar as boas práticas Gestão de Segurança da Informação preconizadas pela ISO/IEC 27002e a Resolução do Conselho de Ministros n.º 41/2018 — Não sendo de aplicação obrigatória identifica um conjunto de orientações técnicas em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais [26].

Uma outra boa prática passa pela implementação da norma ISO/IEC 27002 — Técnicas de segurança — Guia de Boas práticas para controlos de segurança da informação.

ISO/IEC 27001 Sistema de Gestão de Privacidade da Informação (SGPI) esta é uma norma

muitas vezes associada como de suporte ao RGPD que é uma extensão da NP ISO/IEC 27001.

As Normas sobre Sistemas de Gestão de Risco tais como a NP ISO 31000:2018 — Gestão do risco ou a ISO / IEC 27005:2018, *Information technology — Security techniques — Information security risk management* são ferramentas importantes para a gestão de risco.

A norma NP EN 31010 Gestão do Risco; Técnicas de apreciação do risco, identifica um conjunto de ferramentas práticas para a avaliação de risco.

A norma NP EN ISO 2230 Sistemas de Gestão da Continuidade do Negócio define um conjunto de requisitos para as boas práticas da continuidade do negócio.

A norma ISO/TS 22317:2015 *Societal security — Business Continuity Management Systems — Guidelines for business impact analysis* (BIA) define um conjunto de ferramentas para a Análise de Impacto do Negócio (AIN/BIA).

Acesso redes WiFi públicas — Profissionalmente não deve ser permitido, e se o for, devem ser tomadas pelo menos as seguintes medidas de segurança, opte por redes protegidas por password; não guarde na rede, ou esqueça-a assim que terminar a utilização; mantenha os *softwares* atualizados, esteja ligado a estas redes o mínimo de tempo possível.

Plano de Segurança de Sistema de Informação (PSSI) e o RGPD

Para ajudar a verificar se as medidas organizacionais e tecnológicas estão implementadas corretamente e se são eficazes, ajuda ter aquilo a que chamamos Plano de Segurança de Sistema de Informação (PSSI). Ter um Plano de Segurança de Sistema de Informação (PSSI) na empresa ajuda no cumprimento do RGPD. Um dos objetivos do (PSSI) é reduzir os riscos para pessoas e empresas do uso indevido de dados pessoais.

Plano de Segurança de Sistema de Informação (PSSI), ajudará a sua empresa a ter um sistema de gestão de segurança da informação adequado à sua organização, em contínua melhoria e atualização. O RGPD obriga as empresas a analisar os riscos à privacidade e a manter registos do processamento de dados pessoais. Por este motivo, PSSI e o RGPD sobrepõem-se nas seguintes áreas: Segurança dos dados pessoais, notificação de falhas de privacidade, gestão de contratos com subcontratantes do tratamento de dados, registo das atividades de tratamento, privacidade por design e por defeito, proteger os direitos dos titulares dos dados.

Para o ajudar elaboramos a lista de verificação (*Checklist*) que identifica algumas das questões que deve ter em conta na execução do seu Plano de Segurança de Sistema de Informação e na abordagem ao RGPD em simultâneo.

LISTA DE VERIFICAÇÃO (CHECKLIST) PARA RGPD E PSSI			
	ITEM A AVALIAR	OK NC	OBSERVAÇÕES (*)
SEGURANÇA DE DADOS PESSOAIS	▸ Que tipo de dados pessoais são recolhidos, processados e armazenados? Os dados são especialmente protegidos? Protegemos os dados com pseudonimização e criptografia/cifragem?		
	▸ Os controlos e protocolos que se aplicam aos dados pessoais estão documentados? Existem controlos técnicos e organizacionais específicos para cada categoria de dados e tratamento?		
	▸ Como são determinadas as perdas de confidencialidade, integridade e disponibilidade? Realizada avaliação de risco de privacidade?		
	▸ Os dados pessoais são criptografados/Cifrados no armazenamento e quando são transmitidos? Temos a capacidade de anonimizar e pseudonimizados os dados pessoais?		
NOTIFICAÇÃO DE VIOLAÇÕES DE PRIVACIDADE	▸ Por cada processamento de dados: somos responsáveis ou subcontratantes?		
	▸ Os registos dos tratamentos, os inventários de dados pessoais e as suas métricas, permitem-nos identificar violações de dados?		
	▸ Se tivermos EPD/DPO, ele faz parte dos planos e procedimentos de gestão de incidentes?		
	▸ Em caso de incidente, temos controlos específicos para mitigar os riscos das pessoas afetadas pela violação dos dados pessoais?		
	▸ A notificação de 72 horas às autoridades de controlo (CNPD) foi incluída nos planos de resposta a incidentes?		
GESTÃO DE GERENTES / CONTROLADORES DE DADOS	▸ Temos os dados e contactos de todos os responsáveis pelo tratamento? E se somos responsáveis pelo tratamento de terceiros, temos os dados e contactos dos responsáveis por esses tratamentos?		
	▸ A nossa avaliação de risco contém perguntas sobre as medidas técnicas e organizacionais para a proteção da privacidade dirigidas aos responsáveis pelo tratamento?		
	▸ Redigimos as cláusulas contratuais que iremos incluir nos contratos com terceiros que vão atuar como subcontratantes do processamento de dados pessoais?		
	▸ Revimos os contratos existentes com responsáveis de tratamento de dados preexistentes para incluir essas cláusulas?		
	▸ Para cada tratamento pelo qual somos responsáveis, exigimos que os subcontratantes nos peçam autorização antes de subcontratarem o tratamento a terceiros?		
	▸ Para cada tratamento pelo qual somos responsáveis, as nossas políticas de segurança incluem os requisitos do artigo 32º do RGPD?		

REGISTO DE ATIVIDADES DE TRATAMENTO	▸ **Para cada tratamento de dados sabemos:**		
	▸ Que tipo de dados pessoais recolhemos?		
	▸ Como e de onde os dados foram recolhidos?		
	▸ Como e onde é realizada cada parte do tratamento?		
	▸ Como e para onde são transferidos?		
	▸ Como e onde são armazenados, protegidos e eliminados?		
	▸ Que políticas de retenção e destruição temos em vigor? Elas são acompanhadas e revistas?		
PRIVACIDADE DESDE O DESIGN E POR PADRÃO	▸ Que dados pessoais são necessários para cada tratamento que gerimos como responsáveis ou subcontratantes?		
	▸ As nossas políticas atuais limitam a quantidade de dados pessoais que podem ser recolhidos, seja pelo design dos formulários ou por outras medidas de segurança?		
	▸ Se contratarmos uma equipa de desenvolvimento ou adquirirmos novas aplicações (software), eles incorporam os princípios de privacidade nos requisitos de design das novas aplicações?		
DIREITOS DOS TITULARES DOS DADOS	▸ Atualizamos os nossos protocolos para informar os titulares dos dados e obter seu consentimento?		
	▸ Temos procedimentos para classificar e inventariar dados pessoais e para sermos capazes de responder às solicitações dos titulares sobre a sua informação pessoal?		
	▸ Os nossos procedimentos atuais, permitem que os titulares dos dados tenham acesso com segurança aos dados pessoais que temos deles? Temos outros dados pessoais que os titulares não podem ter acesso diretamente? Como são geradas as informações sobre estes últimos e como são comunicados de forma segura aos titulares dos dados que os solicitam?		
	▸ As nossas políticas incluem verificações ou outros procedimentos para rever e corrigir dados pessoais incorretos ou desatualizados?		
	▸ Temos implementados mecanismos para notificar os titulares quando os seus dados pessoais são modificados ou apagados? Art. 19º RGPD		
	▸ Utilizamos perfis ou tomadas de decisões automatizadas com base em dados pessoais e tratamos de acordo com o Art. 22º RGPD?		
	▸ Temos implementados procedimentos para não reter dados pessoais além do tempo necessário para o tratamento ou se o titular dos dados decidir exercer o seu direito de apagamento? Como se executam e reveem estes procedimentos?		
	▸ Os responsáveis pela segurança da informação têm contactos e informações atualizadas sobre os terceiros (*claud* e outros prestadores de serviços de IT) para os quais são transferidos os dados?		

(*) No campo Observações em caso de Não Conformidade (NC) ou se for necessário uma melhoria explicite o que necessita de ser corrigido ou melhorado.
Deve identificar o documento que dá suporte e/ou responde ao requisito quando ele existe e se necessita de correções ou melhorias.
Se está ok, neste campo deve identificar o documento que dá suporte e/ou responde ao requisito.

6.º

O que acontece se não cumprir o RGPD.

Qualquer cidadão da UE tem o direito de apresentar queixa individual ou colectiva se considerar que o tratamento dos seus dados pessoais viola o RGPD. Além disso, como a privacidade é um direito fundamental, terá direito a proteção judicial efetiva e a indemnização pelos danos sofridos em decorrência de uma violação do RGPD.

As autoridades poderão investigar e corrigir as infrações. Para isso, poderão ordenar ao responsável ou subcontratante que forneça informações, efetue auditorias ou obtenha acesso aos dados, instalações e equipamentos. As sanções por infração podem variar desde advertências se a infração for passível, advertências e limitações temporárias, até à proibição do tratamento, ordenando a exclusão de dados e impotação de multas.

O artigo 83º do RGPD define as Condições Gerais para a aplicação de coimas o seu valor:

- De até 10 milhões de euros, ou se for empresa o equivalente a 2% do volume total anual de negócios globais do exercício anterior, sendo aplicado o maior dos dois;
- De até 20 milhões de euros, ou se for empresa o equivalente a 4% do volume total anual de negócios do exercício anterior, sendo aplicado o maior dos dois;

A Lei da Proteção de Dados Pessoais — Lei n.º 58/2019, nos artigos 37º e 38º define a gravidade das contraordenações e o valor das coimas, embora o seu valor seja menor do que as definidas no Regulamento ainda assim são elevadas. O valor das coimas para pessoas coletivas e ou PME varia entre de 1000 (euro) a 1 000 000 (euro) ou 2 % do volume de negócios anual, a nível mundial, conforme o que for mais elevado. Varia de 500 (euro) a 250 000 (euro), no caso de pessoas singulares.

7.0

Referências.

Legislação Nacional e comunitária

[1] — Regulamento sobre identificação eletrónica e serviços de confiança (eIDAS). Decreto—Lei n.º 12/2021 assegura a execução na ordem jurídica interna do Regulamento (UE) 910/2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.
Link para o Regulamento: https://eur—lex.europa.eu/legal—content/PT/TXT/?uri=celex%3A32014R0910
Link para o Decreto—Lei: https://dre.pt/home/—/dre/156848060/details/maximized

[2] — Diretiva de Serviços de Pagamento revista — DSP2. O Decreto—Lei n.º 91/2018 estabelece o novo Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RJSPME), transpondo para o ordenamento jurídico nacional a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro, relativa aos serviços de pagamento no mercado interno (Diretiva de Serviços de Pagamento revista — DSP2).
Link para a diretiva: https://eur—lex.europa.eu/legal—content/PT/ALL/?uri=CELEX:32015L2366
Link para o Decreto—Lei: https://dre.pt/home/—/dre/116936932/details/maximized

[3] — Diretiva NIS (network and information security)/ SRI (segurança das redes e da informação) — Lei n.º 46/2018 estabelece o regime jurídico da segurança do ciberespaço, transpõe a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível de segurança das redes e da informação em toda a União.
Link para a diretiva: https://eur—lex.europa.eu/legal—content/PT/TXT/?uri=CELEX:32016L1148
Link para o Decreto—Lei: https://dre.pt/pesquisa/—/search/116029384/details/maximized

[4] — Regulamento Geral de Proteção de Dados (RGPD) — Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016:
https://eur—lex.europa.eu/legal—content/PT/TXT/?uri=celex%3A32016R0679

[5] — A Diretiva dos direitos de autor e direitos conexos no mercado único digital. Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos direitos de autor e direitos conexos no mercado único digital.
https://eur—lex.europa.eu/legal—content/PT/TXT/?uri=CELEX%3A32019L0790

[6] — Conselho Europeu adotou a Convenção para a proteção de pessoas no que diz respeito ao tratamento automatizado de dados pessoais. A Convenção 108.
https://www.coe.int/en/web/conventions/full—list/—/conventions/treaty/108?module=treaty—detail&treatynum=108

[7] — Carta dos Direitos Fundamentais da EU
https://infoeuropa.eurocid.pt/registo/000040181/documento/0001/

[8] — Proteção de Dados Pessoais e Privacidade nas telecomunicações — Lei n.º 41/2004, de 18 de Agosto. Transpõe para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas:
https://dre.pt/pesquisa/—/search/480710/details/maximized

[9] — Lei da Proteção de Dados Pessoais (LPDP) — Lei n.º 58/2019, de 08 de Agosto:
https://dre.pt/pesquisa/—/search/123815982/details/maximized

[10] — Artigo 35.º da Constituição da república:
https://dre.pt/web/guest/legislacao—consolidada/—/lc/337/201903120346/73938538/diplomaPagination/diploma/2

[26] — Resolução do Conselho de Ministros n.º 41/2018 — Define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais.
https://dre.pt/home/—/dre/114937034/details/maximized

CNPD (Comissão Nacional de Proteção de Dados)

[12] — Princípios aplicáveis aos tratamentos de dados com a finalidade de medicina preventiva e curativa no âmbito dos controlos de alcoolemia e de droga efetuados a trabalhadores
https://www.cnpd.pt/media/cxpijpa4/medicina—no—trabalho—e—controlo—alcoolemia_20_890_2010.pdf

[14] — Princípios aplicáveis aos tratamentos de dados pessoais decorrentes do controlo da utilização para fins privados das tecnologias de comunicação no contexto laboral

https://www.cnpd.pt/media/zvxmdfad/del_7680—2014_geo_laboral.pdf

[15] — Princípios aplicáveis aos tratamentos de dados no âmbito da gestão da informação dos Serviços de Segurança e Saúde no Trabalho
https://www.cnpd.pt/media/pwig2aqa/medicina—trabalho—del_840_2010_.pdf

[19] — Formulário violação de dados CNPD:
https://www.cnpd.pt:8086/databreach/?AspxAutoDetectCookieSupport=1

Registos de Atividades de Tratamento

[11] — Reprodução do Cartão de Cidadão: Lei n.º 7/2007, de 05 de Fevereiro Cartão de Cidadão — Emissão e utilização:
https://dre.pt/pesquisa/—/search/518073/details/maximized

[18] — Regulamento 1/2018 CNDP. Relativo à lista de tratamentos de dados pessoais sujeitos à avaliação de impacto sobre a proteção de dados (AIPD):
https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121818

[21] — Modelo de registo para responsáveis pelo tratamento:
https://www.cnpd.pt/media/v0jbmwqn/templatedocrgpd_resp_v1.xlsx

[22] — Modelo de registo para subcontratantes:
https://www.cnpd.pt/media/cltpq4bn/templatedocrgpd_sub_v1.xlsx

Orientações do CEPD (centro europeu de proteção de dados)

[13] — Orientações sobre o consentimento ao abrigo do RGPD:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_pt.pdf

[16] — Orientações sobre os encarregados de proteção de dados:
https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf

[17] — Orientações do CEPD relativas às avaliações de impacto sobre a proteção de dados e que determinam se o tratamento é suscetível de resultar num elevado risco:
https://www.cnpd.pt/media/f0ide5i0/aipd_wp248rev—01_pt.pdf

[20] — Orientações sobre as notificações de violações de dados:
https://www.cnpd.pt/media/zgkec1q0/data—breach—_wp250rev01_pt.pdf

CNCS (Centro Nacional de Cibersegurança)

[23] — Pode fazer uma avaliação às capacidades de cibersegurança da sua empresa, com a ferramenta Cibercheckup do CNCS é simpes, pode aceder e experimentar em ciberchеckup.cncs.gov.pt/

[24] — Boas práticas no uso de passwords:
https://www.cncs.gov.pt/pt/boas—praticas—passwords/

[25] — Boas Práticas de cibersegurança:
https://dyn.cncs.gov.pt/pt/boaspraticas/?persona=organizations

APSEI
ASSOCIAÇÃO PORTUGUESA DE SEGURANÇA

apsei.org.pt

Elaborado por:

Bureau Veritas

Cofinanciado por:

COMPETE 2020

PORTUGAL 2020

UNIÃO EUROPEIA

Fundo Europeu de Desenvolvimento Regional