Guia Prático

Proteção de Dados Pessoais – Economia Social

Imagem: Alexander Sinn em Unsplash

BPI | Fundação "la Caixa" NOVA SCHOOL OF BUSINESS & ECONOMICS

SOCIAL EQUITY INITIATIVE

KNOWLEDGE-DRIVEN PROGRESS

Base de Dados Social

Social Equity Initiative Project

NOVA SCHOOL OF BUSINESS & ECONOMICS

Data Science Knowledge Center

No contexto digital atual, caracterizado pelo ritmo acelerado de inovações tecnológicas, a gestão de dados, com destaque para a proteção de dados pessoais, assume um papel crucial que exige respostas cada vez mais complexas e abrangentes. Novos desafios emergem, obrigando as entidades a (re)pensar as suas estratégias de gestão de dados, com foco na proteção da privacidade, na segurança da informação e na tomada de decisões baseadas em dados atuais e fidedignos.

Considerando que "o tratamento, a gestão e a recolha de dados ainda não são práticas generalizadas nas entidades da economia social"[1], esses desafios são sentidos pelo setor com impactos diferenciados, conforme a dimensão, a natureza e o âmbito da intervenção das organizações que o integram.

É fundamental, por isso, promover o acesso a instrumentos e recursos adequados às especificidades do ecossistema social, capacitando as organizações para o uso estratégico de dados nos processos decisórios e de mudança social.

O presente Guia pretende, assim, apoiar as organizações sociais na implementação de práticas eficazes de proteção de dados, especialmente no que respeita aos dados pessoais. Simultaneamente, representa um convite para as organizações considerarem a gestão de dados como uma importante e necessária ferramenta estratégica para o desenvolvimento da sua missão e alcance dos seus objetivos de impacto.

"(...) para a economia social, os dados podem não ser apenas um ativo económico, mas, acima de tudo, um trunfo para apoiar a sua missão social ou ecológica, bem como um instrumento para uma governação inclusiva e democrática."[2]

[1] Comissão Europeia (2021), *Plano de Ação para a Economia Social*.

[2] Comissão Europeia (2022), *Trajetória de Transição para o Ecossistema da Economia Social e de Proximidade*.

Índice Geral

Imagem: Austris Augusts em Unsplash

Enquadramento

A gestão ética e responsável de dados é fundamental para assegurar a proteção da privacidade e dos direitos individuais, fomentando a confiança nas instituições e contribuindo para a integridade dos dados. Este cenário é particularmente relevante na economia social, dada a sua natureza marcadamente social e a sua crescente integração no mundo digital.

Beneficiários, voluntários, doadores e outras partes interessadas confiam nas organizações para gerir os seus dados com cuidado e responsabilidade, e a falha na proteção de dados pode não só prejudicar as pessoas envolvidas, mas também afetar a confiança pública na organização, por conseguinte, no setor como um todo.

Adicionalmente, o crescente volume de dados pessoais nas organizações sociais aumenta a necessidade de práticas eficazes de gestão dos dados, de forma a garantir que o seu tratamento é realizado de forma ética, segura e em conformidade com a legislação vigente.

Neste sentido, o presente Guia pretende disponibilizar um conjunto de informações e recursos úteis para a proteção de dados pessoais, reunindo orientações e recomendações de boas práticas que procuram apoiar as organizações sociais a garantir a segurança, a transparência e a responsabilidade nas várias operações de tratamento dos dados.

O Guia destina-se tanto a organizações sociais recentemente constituídas, que procuram introduzir e implementar, desde o início da sua atividade, uma cultura de gestão e de proteção de dados pessoais, como a organizações sociais estabelecidas, numa ótica de avaliação periódica e de melhoria contínua das suas práticas e procedimentos neste âmbito.

Objetivos e Metodologia

Os principais objetivos do Guia são:

- Promover a **transparência** e a **responsabilidade** na gestão de dados;
- Promover a **utilização** e a **partilha de dados** em **conformidade** com a legislação aplicável;
- Promover uma **cultura de melhoria contínua** através da **monitorização** e **atualização** regular de **práticas e procedimentos**;
- Apoiar a **implementação de medidas de segurança de dados** para prevenir acessos não autorizados, perdas, violações e potenciais ameaças;
- Promover a **confiança** junto das **partes interessadas** da economia social.

A metodologia utilizada para a elaboração do Guia centrou-se na triangulação de diversas fontes de informação, conhecimento e experiências para assegurar a pertinência e a relevância dos conteúdos apresentados.

Em particular, a experiência acumulada no âmbito do projeto Base de Dados Social revelou-se fundamental. O contacto com as organizações sociais através das iniciativas desenvolvidas pelo projeto, designadamente os *workshops* de dados, facilitou a identificação de necessidades específicas e dos desafios enfrentados pelas organizações no que diz respeito ao tratamento de dados pessoais.

De igual forma, os resultados do inquérito realizado em 2023, no âmbito da tese de mestrado "*Responsible Data Practices in the Social Economy Sector in Portugal: A Code of Conduct for Data Collection, Management, and Sharing*" da autoria de Mafalda Carvalhal e que contou com o apoio do Nova SBE Data Science Knowledge Center, permitiram aprofundar o conhecimento sobre o panorama atual da economia social em relação às práticas de recolha, gestão e partilha de dados levadas a cabo pelas organizações sociais.

Objetivos e Metodologia

Complementarmente, foram consultados documentos de referência, em particular publicações da Comissão Europeia, como o *Plano de Ação para a Economia Social* e a *Trajetória de Transição para o Ecossistema da Economia Social e de Proximidade,* para compreender o quadro estratégico das políticas comunitárias previstas para o setor, com ênfase nas iniciativas que pretendem promover a gestão de dados nas organizações sociais.

Por último, além da consulta do Regulamento Geral sobre a Proteção de Dados (RGPD) e da Lei da Proteção de Dados Pessoais (Lei n.º 58/2019, de 8 de agosto), foram também analisados documentos produzidos pelo Comité Europeu para a Proteção de Dados (CEPD), pela Comissão Nacional de Proteção de Dados (CNPD) e por autoridades nacionais de outros Estados-Membros da União Europeia (UE), para aprofundar o conhecimento sobre as regras aplicáveis e de interpretação das normas legais.

Ao longo do Guia, são utilizados três ícones para destacar as seguintes informações:

Referências ao RGPD

Exemplos ilustrativos

Informações, recomendações ou alertas relevantes

O presente Guia deve ser utilizado como um recurso adicional e complementar, não dispensando a consulta da legislação aplicável, designadamente o RGPD e a Lei da Proteção de Dados Pessoais.

Glossário

Imagem: Ryan Wallace em Unsplash

Para uma melhor compreensão dos conteúdos e temas abordados no presente Guia, apresentamos um glossário onde constam, nos termos do RGPD, os principais conceitos relacionados com a proteção de dados pessoais utilizados ao longo do documento.

Glossário

Dados Pessoais	Informação relativa a uma pessoa singular identificada ou identificável 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.
Categorias Especiais de Dados Pessoais	Dados pessoais que são protegidos pela legislação da UE e apenas podem ser tratados se existirem garantias específicas. Os seguintes dados são considerados de categorias especiais e estão sujeitos a condições de tratamento específicas: ▪ dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; ▪ filiação sindical; ▪ dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano; ▪ dados relacionados com a saúde; ▪ dados relativos à vida sexual ou orientação sexual da pessoa.
Tratamento de Dados	Operação ou conjunto de operações efetuadas sobre 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.
Titular dos Dados	Uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como, por exemplo, um nome, ou um número de identificação.
Responsável pelo Tratamento	A pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais.
Subcontratante	A pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

Glossário

Terceiro	Pessoa singular ou coletiva, autoridade pública, o serviço ou qualquer outro organismo que, não sendo o titular de dados, o responsável pelo tratamento, o subcontratante ou outra pessoa sob autoridade direta do responsável pelo tratamento ou do subcontratante, esteja autorizado a tratar os dados.
Destinatário	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.
Definição de Perfis	Qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.
Decisão de Adequação	Decisão da Comissão Europeia de que um país terceiro (qualquer país fora do Espaço Económico Europeu), um território ou um ou mais setores específicos desse país terceiro, ou uma organização internacional, assegura um nível de proteção adequado no âmbito das transferências internacionais de dados pessoais para países terceiros ou organizações internacionais.
Cláusulas Contratuais-Tipo	Cláusulas-tipo de proteção de dados normalizadas e pré-aprovadas que permitem ao responsável pelo tratamento e ao subcontratante cumprir as suas obrigações ao abrigo da legislação comunitária em matéria de proteção de dados. A Comissão Europeia tem poderes para adotar cláusulas contratuais-tipo para a relação entre responsáveis pelo tratamento e subcontratantes e para a transferência de dados pessoais para países fora do Espaço Económico Europeu.
Regras Vinculativas Aplicadas às Empresas	Regras internas de proteção de dados pessoais, aprovadas pela CNPD, aplicadas por um responsável pelo tratamento ou um subcontratante estabelecido no território de um Estado-Membro para as transferências ou conjuntos de transferências de dados pessoais para um responsável ou subcontratante num ou mais países terceiros, dentro de um grupo empresarial ou de um grupo de empresas envolvidas numa atividade económica conjunta.

Destaques do Inquérito

Imagem: Jason Coudriet em Unsplash

No âmbito da tese de mestrado "Responsible Data Practices in the Social Economy Sector in Portugal: A Code of Conduct for Data Collection, Management, and Sharing" da autoria de Mafalda Carvalhal, foi aplicado um inquérito com o objetivo de identificar e caracterizar as práticas de tratamento de dados implementadas pelas organizações sociais e avaliar a necessidade de um código de conduta no tratamento de dados pessoais.

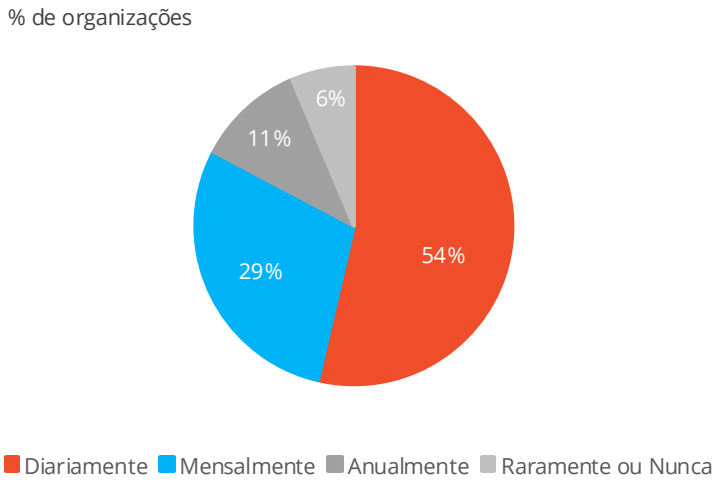
No presente capítulo, são apresentados os principais resultados do inquérito, que contou com a participação de **110 organizações sociais**.

Destaques do Inquérito

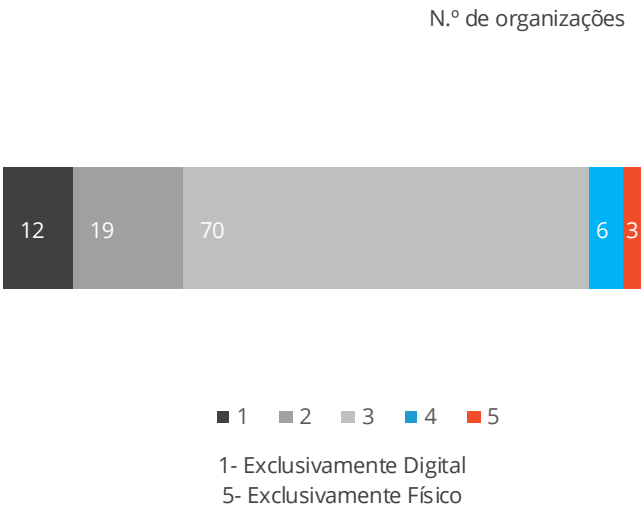
Dados nas Organizações

No que respeita à caracterização dos dados mantidos pelas organizações, verifica-se que o **tratamento de dados é uma prática frequente** e que existe um **panorama diversificado** no que respeita ao **formato** utilizado para o seu **armazenamento**.

Com que frequência as organizações procedem ao tratamento de dados?

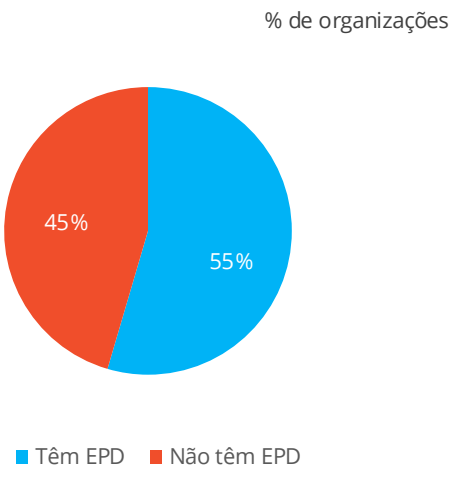


Os dados armazenados pelas organizações encontram-se num formato:



Em relação a quais entidades ou indivíduos as organizações mantêm informações?

As organizações têm um Encarregado de Proteção de Dados (EPD)?



Destaques do Inquérito

Práticas de Recolha de Dados

Quanto às práticas correntes de recolha de dados e perceção das organizações sobre a predisposição dos titulares para fornecer os seus dados, identificam-se **lacunas significativas**, particularmente no que diz respeito à **obtenção de consentimento**.

70%

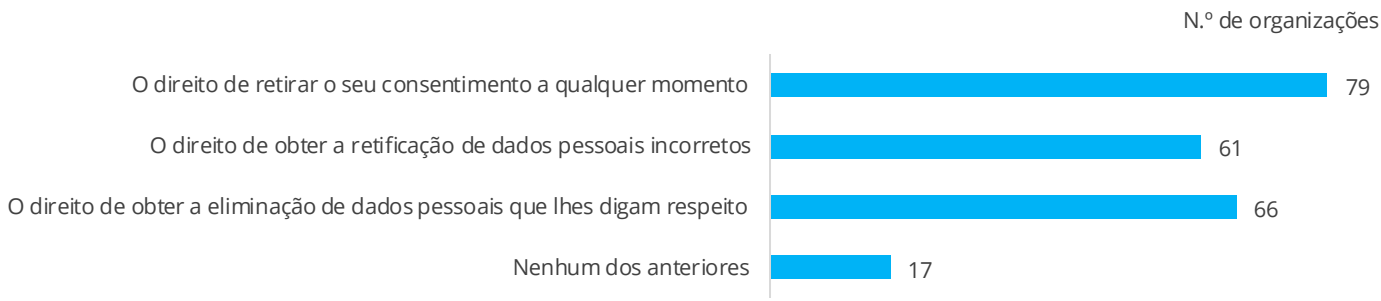
das organizações **obtêm sempre consentimento** antes de recolher dados pessoais.

8%

das organizações **validam a recolha de dados** através de **caixas de opção pré-validada**.

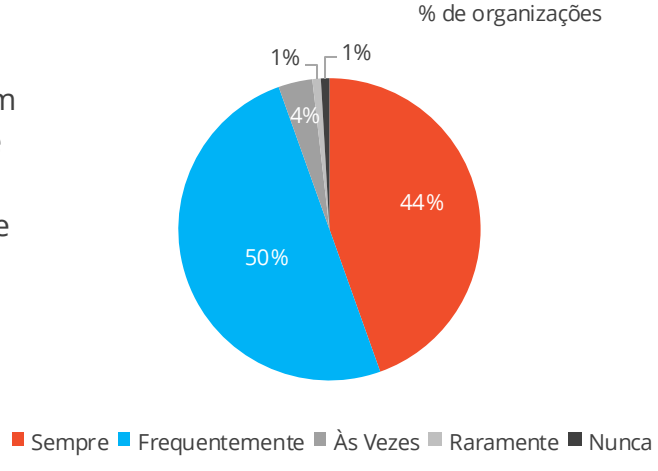
A adoção de **caixas de opção pré-validada**, onde uma opção como "Aceito" ou "Concordo" está automaticamente selecionada, **não atende aos requisitos do RGPD**. Este tipo de validação pode afetar a transparência do consentimento, colocando a organização em risco de penalidades por não conformidade.

Os titulares dos dados são informados sobre:



Os titulares dos dados partilham os seus dados pessoais sem constrangimentos?

O **elevado número de titulares que fornece os seus dados pessoais sem constrangimentos** pode refletir um **desconhecimento sobre os seus direitos**, resultante de uma eventual falta de obtenção de consentimento adequado e/ou de uma **insuficiente comunicação** sobre estes direitos, conforme evidenciado pelos dados apresentados. A ausência de avaliação crítica sobre a utilização dos dados poderá também ser um sinal de desinteresse ou de familiaridade com a constante solicitação de dados na era digital.

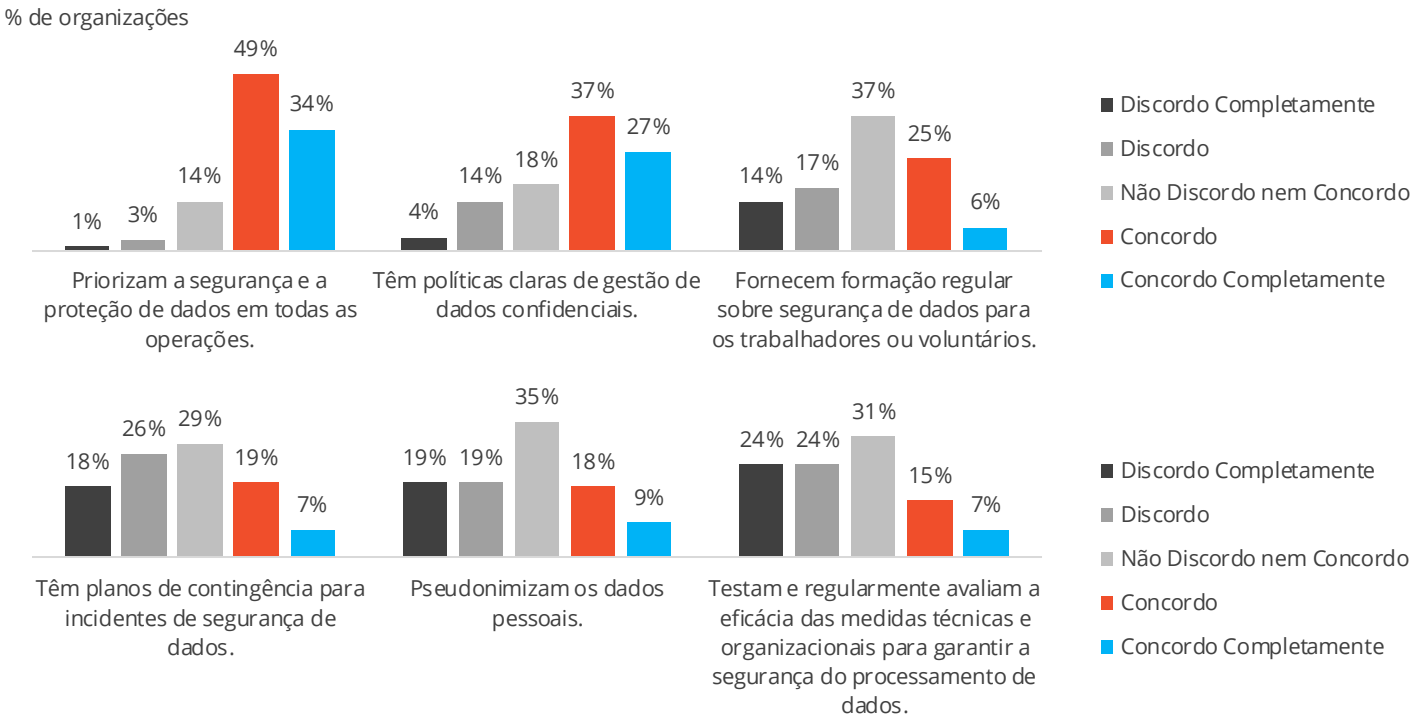


Destaques do Inquérito

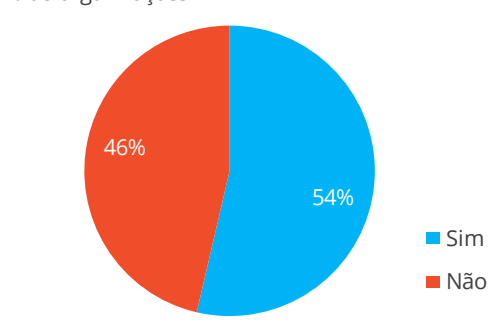
Práticas de Gestão de Dados

Relativamente às práticas correntes de gestão de dados, verifica-se **pouca evidência da adoção de práticas robustas de proteção de dados** e uma **deficiente implementação de procedimentos** para lidar com possíveis **violações de dados**.

As organizações sociais:



As organizações partilham dados com entidades externas?



As organizações lidam com obstáculos na partilha de dados e possuem procedimentos para gerir essas dificuldades?

9%

das organizações **já enfrentaram desafios** relacionados com a **partilha de dados**

41%

das organizações **não têm procedimentos** em vigor para **notificar** as **partes afetadas** no caso de **violação de dados**

Flash RGPD

Imagem: Claudio Schwarz em Unsplash

No contexto da aplicação do RGPD, verifica-se que a proteção de dados pessoais continua a ser um desafio complexo e multifacetado para muitas organizações sociais.

O presente capítulo oferece uma visão geral e sintética dos principais aspectos do RGPD, numa perspetiva de apoiar as organizações a familiarizarem-se com as exigências previstas, ou a reverem os temas-chave associados aos requisitos de conformidade.

Flash RGPD

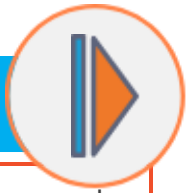
O que é o RGPD?

É um diploma da UE (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016) que define as regras para o tratamento de dados pessoais e para a livre circulação desses dados, assegurando a aplicação coerente e homogénea dessas regras em toda a UE.

Quem beneficia da proteção do RGPD?

O RGPD foi concebido para proteger a privacidade e os direitos dos cidadãos da UE, garantindo que o tratamento dos seus dados pessoais é efetuado de forma responsável e segura, reforçando, assim, os direitos fundamentais das pessoas na era digital.

Qual o âmbito de aplicação do RGPD?



O RGPD aplica-se a qualquer entidade estabelecida na UE que efetue o tratamento de dados pessoais, independentemente do local onde é realizado esse tratamento, bem como a entidades estabelecidas fora da EU, quando as atividades de tratamento estejam relacionadas com a oferta de bens ou serviços a pessoas na UE, ou com o controlo do comportamento de pessoas na UE.

Artigo 5.º

7 Princípios-Chave

Licitude
Lealdade
Transparência

Os dados pessoais são objeto de um **tratamento lícito**, **leal** e **transparente** em relação aos titulares dos dados, garantindo que estes são **informados** sobre a forma como os seus **dados** estão a ser **utilizados**.

Limitação das Finalidades

Os dados pessoais são recolhidos para **fins determinados**, **explícitos** e **legítimos** e **não devem ser tratados posteriormente** de forma **incompatível** com esses **fins**.

Minimização dos Dados

Os dados pessoais são **adequados**, **pertinentes** e **limitados** ao que é **necessário** relativamente aos **fins** para os quais são tratados.

Exatidão

Os dados pessoais são **exatos** e **atualizados**, devendo ser adotadas **medidas adequadas** para que os **dados inexatos** sejam **apagados** ou **retificados**.

Limitação da Conservação

Os dados pessoais são **conservados** de uma forma que permita a **identificação dos titulares dos dados** apenas durante o **período necessário** para os **fins** para os quais são tratados.

Integridade e Confidencialidade

Os dados pessoais são tratados de uma forma **segura**, garantindo a **proteção** contra o seu **tratamento não autorizado** ou **ilícito** e contra a sua **perda**, **destruição** ou **danificação acidental**.

Responsabilidade

O **responsável** pelo **tratamento** dos dados pessoais deve assegurar o **cumprimento** dos demais **princípios** e **comprová-lo**.

Direitos do Titular dos Dados

Informação

Artigos 13.º e 14.º

Direito de **receber informação específica** da organização, designadamente informações sobre a **finalidade da recolha de dados**, o **fundamento jurídico para o tratamento**, os **fins estabelecidos** pela organização, os **destinatários dos dados** e os **períodos de conservação dos dados**, permitindo-lhe, assim, tomar decisões informadas sobre os seus dados pessoais.

Acesso

Artigo 15.º

Direito de apresentar **pedidos de acesso** e **obter informações** da organização sobre se os seus **dados pessoais estão a ser tratados** e, se for esse o caso, de **aceder aos dados pessoais**, e de, designadamente, ser informado dos **objetivos do tratamento**, as **categorias de dados pessoais** em causa, os **destinatários dos dados**, bem como o **prazo de conservação dos dados**.

Retificação

Artigo 16.º

Direito de **exigir** da organização a **retificação dos dados pessoais inexatos sem demora injustificada**. O titular dos dados, tendo em conta as finalidades do tratamento, pode também solicitar que os **dados pessoais incompletos sejam completados**, incluindo através da apresentação de uma declaração suplementar.

Direitos do Titular dos Dados

Apagamento

Artigo 17.º

Direito a **ser esquecido**, o que permite que o titular dos dados solicite que os seus **dados pessoais sejam eliminados** se, designadamente, os **dados já não são necessários para atingir o fim para o qual foram recolhidos,** não havendo nenhuma **norma legal** que **imponha** a sua **conservação por mais tempo**, ou **retirou o seu consentimento**, no qual se baseava a legitimidade do tratamento.

Limitação do Tratamento

Artigo 18.º

Direito que permite ao titular dos dados, durante um determinado período de tempo, obter a **limitação do tratamento dos dados** por parte da **organização**, **não podendo** esta **comunicar os dados a terceiros**, **transferi-los internacionalmente**, ou **eliminá-los**, quando:

- a **exatidão dos dados estiver em causa** e a sua verificação pendente;
- houver **oposição ao tratamento**, até à **verificação** da existência da **prevalência de interesses legítimos** da organização;
- os **dados não sejam mais necessários** para a organização, mas o **titular dos dados deseja preservá-los** para efeitos de **ações legais**;
- o **tratamento for ilícito** e o titular dos dados opte pela restrição em vez do apagamento (até eventualmente instaurar uma ação judicial contra a organização).

Portabilidade

Artigo 20.º

Direito de **receber** da organização os seus **dados pessoais**, num formato estruturado, de uso corrente e de leitura automática, e de os **transmitir para outra entidade** quando o tratamento dos dados se basear no consentimento ou num contrato e for realizado por meios automatizados.

Este direito prevê que os dados sejam **transmitidos diretamente** entre entidades, sempre que tal for **tecnicamente possível**.

Direitos do Titular dos Dados

Oposição

Artigo 21.º

Direito que permite que o titular dos dados **se oponha**, a qualquer momento, ao **tratamento dos seus dados pessoais**, em determinadas situações, e dependerá da finalidade do tratamento e da base legal para o mesmo.

Nestes casos, a **organização deverá cessar o tratamento**, a menos que apresente razões imperiosas e legítimas que prevaleçam sobre os interesses, direitos e liberdades do titular, ou para efeitos de exercício de um direito num processo judicial.

Não Sujeição

Artigo 22º

Direito de **não ficar sujeito a decisões tomadas exclusivamente com base no tratamento automatizado**, incluindo a **definição de perfis**, que produza efeitos na esfera jurídica do titular dos dados ou que o afete significativamente de forma similar.

Nos casos em que se aplicam **exceções**, a organização deve implementar **medidas de proteção dos direitos** do titular dos dados.

Obrigações do Responsável pelo Tratamento

Proteção de dados desde a conceção

Artigo 25.º

A organização deve considerar a privacidade e a proteção de dados nas **fases iniciais de conceção** (***by design***) de qualquer **projeto** que envolva **dados pessoais**, bem como ao longo de todo o seu **ciclo de vida**, designadamente através:

- do **cumprimento dos princípios do RGPD** na conceção de novos produtos, serviços ou processos;
- do **desenvolvimento** e **execução** de **medidas técnicas e organizativas** adequadas;
- da **definição de políticas**, **procedimentos** e **sistemas conformes** com o **RGPD**.

Proteção de dados por defeito

Artigo 25.º

A organização deve aplicar **medidas técnicas e organizativas** para **assegurar** que, **por defeito** (***by default***), designadamente:

- só sejam **tratados os dados pessoais** que forem **necessários** para cada **finalidade específica** do tratamento;
- são **aplicadas regras rigorosas** de **proteção de dados** e **privacidade** na **aquisição** de um **produto/serviço**;
- os **dados pessoais** sejam **conservados** apenas durante o **período de tempo necessário** para **fornecer** o **produto/serviço**.

As **medidas** devem **assegurar** que, **por defeito**, os **dados pessoais não sejam disponibilizados sem intervenção humana** a um **número indeterminado de pessoas singulares**.

Obrigações do Responsável pelo Tratamento

Garantias do subcontratante

Artigo 28.º

A **organização**, quando o **tratamento dos dados** for **efetuado por sua conta**, **recorre** apenas a **subcontratantes** que **apresentem garantias suficientes** de execução de **medidas técnicas e organizativas** adequadas de uma forma que o tratamento satisfaça os **requisitos do RGPD** e assegure a **defesa dos direitos** do titular dos dados.

Para assegurar as referidas garantias, deve ser **celebrado** nos termos da lei um **contrato** entre a organização e o subcontratante, que, designadamente:

- **vincule o subcontratante** ao responsável pelo tratamento;
- **estabeleça o objeto e a duração** do tratamento;
- **defina a natureza e finalidade** do tratamento;
- **defina o tipo de dados pessoais** e as **categorias** dos titulares dos dados;
- **estabeleça as obrigações e direitos** do responsável pelo tratamento;
- **preveja outras estipulações** presentes no RGPD.

Registo de atividades de tratamento

Artigo 30.º

A **organização** deve **manter e conservar** um **registo** das **atividades de tratamento** sob a sua responsabilidade, no qual devem constar:

- **nome** e **contactos** do **responsável pelo tratamento** e, caso aplicável, do **EPD**;
- **finalidades** do tratamento dos dados;
- **descrição das categorias** de titulares de dados e de dados pessoais;
- **categorias de destinatários** a quem os dados pessoais foram ou serão divulgados;
- **transferências** de dados pessoais para **países terceiros ou organizações internacionais**;
- **prazos** previstos para o **apagamento** dos dados pessoais;
- **descrição geral** das **medidas técnicas e organizativas** no domínio da **segurança**.

A CNPD, no âmbito de verificações de conformidade, pode solicitar à organização, a qualquer momento, a disponibilização dos registos das atividades de tratamento.

Obrigações do Responsável pelo Tratamento

Cooperação com a CNPD

Artigo 31.º

A **organização** deve **cooperar** com a **CNPD**, a pedido desta, na **prossecução das suas atribuições**.

Segurança do tratamento

Artigo 32.º

A **organização** deve **aplicar as medidas técnicas e organizativas** adequadas para **garantir um nível de segurança adequado ao risco**, incluindo, consoante o que for adequado:

- a **pseudonimização** e a **encriptação** dos dados pessoais;
- a capacidade de **assegurar** a **confidencialidade**, **integridade**, **disponibilidade** e **resiliência permanentes** dos **sistemas** e dos **serviços de tratamento**;
- a **capacidade de restabelecer** a **disponibilidade** e o **acesso** aos **dados pessoais atempadamente** no caso de um **incidente** físico ou técnico;
- um **processo** para **testar, apreciar e avaliar regularmente** a **eficácia das medidas técnicas e organizativas** para assegurar a **segurança do tratamento**.

Gestão do Risco

Artigo 32.º

Na **avaliação do nível de segurança adequado**, a **organização** deve **considerar**, designadamente, os **riscos** apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas e à divulgação ou acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

A **gestão do risco prepara a organização** para os **potenciais problemas futuros de proteção de dados pessoais** associados a um determinado projeto, com benefícios para a sua **conceção e desenvolvimento** e para a **comunicação com as partes interessadas** sobre os riscos associados.

Obrigações do Responsável pelo Tratamento

Notificação de violações

Artigo 33.º

A **organização**, em caso de **violação de dados pessoais**, e sempre que essa violação seja suscetível de resultar num **risco para os direitos e liberdades** dos titulares dos dados, deve **notificar a CNPD**, sem demora injustificada e, sempre que possível, **até 72 horas após ter tido conhecimento** da mesma. Se este prazo não for cumprido, a organização deve apresentar com a notificação os motivos do atraso.

A **notificação** referida deve, pelo menos:

- descrever **a natureza** da **violação dos dados pessoais** incluindo, se possível, as **categorias** e o **número aproximado** de **titulares de dados afetados**, bem como as **categorias** e o **número aproximado de registos** de **dados pessoais** em causa;
- comunicar o **nome e os contactos do EPD** ou de **outro interlocutor** onde possam ser obtidas mais informações;
- descrever as **consequências prováveis** da violação de dados pessoais;
- descrever as **medidas adotadas ou propostas** para **reparar** a violação de dados pessoais, inclusive, se for caso disso, **medidas para atenuar** os seus **eventuais efeitos negativos**.

A **organização** está, ainda, **obrigada** a dar **conhecimento** aos **titulares dos dados** da ocorrência de uma **violação** de dados pessoais, quando essa violação **for suscetível de implicar um elevado risco** para os seus **direitos e liberdades**.

Obrigações do Responsável pelo Tratamento

Avaliação de impacto (AIPD)

Artigos 35.º e 36.º

Quando determinado **tipo de tratamento**, em particular que utilize **novas tecnologias** e tendo em conta a sua **natureza**, **âmbito**, **contexto** e **finalidades**, for suscetível de implicar um **elevado risco** para os **direitos e liberdades** dos titulares dos dados, a **organização deve**, **antes de iniciar o tratamento**, realizar uma **avaliação de impacto sobre a proteção de dados** das operações de tratamento previstas.

A **AIPD** deverá **incluir**, 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 fazer face aos 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**.

Quando a **avaliação de impacto indicar** que o **tratamento** de dados que se pretende efetuar, apesar das medidas mitigadoras a adotar, resulta ainda num **elevado risco** para os **direitos e liberdades** dos titulares dos dados, a **organização** deve **submeter** o tratamento de dados em causa a **consulta prévia da CNPD**.

Consulte aqui os casos em que a realização de uma AIPD é obrigatória nos termos do Regulamento 798/2018 da CNPD!

Consulte aqui as Orientações do CEPD relativas à AIPD e que determinam se o tratamento é suscetível de resultar num elevado risco!

Obrigações do Responsável pelo Tratamento

Designação EPD

Artigo 37.º

A **organização** só está **obrigada** à **designação de um EPD** se **tratar categorias especiais de dados pessoias** ou **dados relativos a condenações penais e infrações**, em **larga escala**, ou se realizar **tratamentos em larga escala** relativos ao **controlo regular e sistemático** dos titulares dos dados.

Nestes casos, a organização deve:

- **assegurar** que o **EPD seja envolvido**, de forma adequada e em tempo útil, **em todas as questões relacionadas** com a **proteção de dados pessoais**;
- **apoiar** o **EPD** no **exercício das suas funções**, fornecendo-lhe os **recursos necessários** ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como dando-lhe **acesso aos dados pessoais** e às **operações de tratamento**;
- **assegurar** que o **EPD**, ao nível da proteção de dados, **exerce as suas funções** com a **máxima independência**.

O **EPD não pode ser destituído**, **nem penalizado** pela organização pelo facto de **exercer as suas funções**.

Adicionalmente, a **designação de um EPD é obrigatória** para **entidades públicas**, assegurando a conformidade com as normas de proteção de dados.

Consulte aqui as Orientações do CEPD sobre os EPD!

Nos casos em que o EPD não é obrigatório, a organização pode decidir designar um interlocutor responsável pela matéria da proteção de dados, considerando as vantagens associadas!

Artigo 83.º

Sanções

O **RGPD** prevê um **regime sancionatório** que define **coimas avultadas**, aliado a uma **maior fiscalização** por parte da **CNPD**, que deve **assegurar** que a **aplicação das coimas** seja **efetiva**, **proporcionada** e **dissuasiva**.

1

Coimas até €10.000.000 ou, no caso de uma **empresa**, **até 2% do seu volume de negócios anual**, a nível mundial, correspondente ao exercício financeiro anterior, **consoante o montante que for mais elevado**, estando em causa, designadamente, **violações** dos **princípios** do tratamento, dos **direitos dos titulares dos dados** e das **regras sobre transferências**.

2

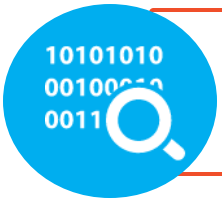
Coimas até €20.000.000 ou, no caso de uma **empresa**, **até 4% do seu volume de negócios anual**, a nível mundial, correspondente ao exercício financeiro anterior, **consoante o montante que for mais elevado**, para, designadamente, situações de **incumprimento de obrigações da organização**.

Além das coimas, podem ser aplicadas outras sanções de acordo com a legislação em vigor, designadamente responsabilidade criminal, responsabilidade civil e responsabilidade disciplinar!

Sanções

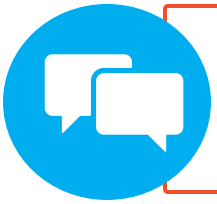
Na Europa...

De acordo com a 5.ª edição do Relatório *GDPR Enforcement Tracker Report* [3]:



2.086 corresponde ao **número total de coimas** aplicadas pelas Autoridades de Controlo da UE

4.48 mil milhões de euros corresponde ao **valor total** de coimas aplicadas pelas Autoridades de Controlo da UE



Media, Telecomunicações e Radiodifusão representa o **setor** com o maior número de coimas aplicadas

Base jurídica insuficiente para o tratamento constituiu o **principal motivo** para a maioria das coimas aplicadas

[3] CMS, *GDPR Enforcement Tracker Report*, 2024 (dados do período compreendido entre 2018 e 1 de março de 2024)

Sanções

Na Europa...

De acordo com o *GDPR Enforcement Tracker*, em 2024[4]:

€16.000

Valor da **coima** aplicada pela **Autoridade de Controlo Francesa** a uma **associação** pelo **tratamento de dados pessoais sem suficiente base legal**.

€15.000

Valor da **coima** aplicada pela **Autoridade de Controlo Francesa** a uma **associação** devido à **falta de segurança dos dados**, ao **incumprimento do princípio da minimização dos dados** e ao **incumprimento das suas obrigações de informação**.

Top 3 das maiores coimas aplicadas pelas Autoridades de Controlo da UE em 2023:

Meta Platforms Ireland Limited
1.2 mil milhões de Euros: tratamento de dados pessoais sem suficiente base legal

Meta Platforms Ireland Limited
390 milhões de Euros: não conformidade com os princípios gerais de tratamento de dados pessoais

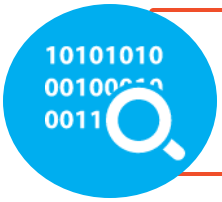
TikTok Limited
345 milhões de Euros: não conformidade com os princípios gerais de tratamento de dados pessoais

[4] CMS, *GDPR Enforcement Tracker*, 2024

Sanções

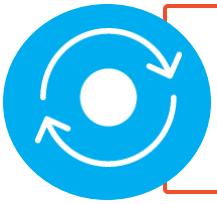
Em Portugal...

De acordo com o *Relatório de Atividades* 2023 da CNPD[5]:



48 corresponde ao **número total de coimas** aplicadas pela CNPD ao abrigo do RGPD

360 mil euros corresponde **ao valor total de coimas** aplicadas pela CNPD ao abrigo do RGPD



7 medidas corretivas aplicadas pela CNPD ao abrigo do RGPD

197 deliberações adotadas pela CNPD nos processos de **violação de dados pessoais**

[5] CNPD, *Relatório de Atividades 2023*

Benefícios

A **conformidade com o RGPD** oferece um conjunto de **benefícios** à sua **organização**. O **cumprimento** das obrigações legais deve ser encarado como uma **oportunidade** para introduzir **mudanças** e implementar **práticas adequadas** e **transparentes** de **gestão de dados**.

Proteção

Transparência

Segurança

Confiança

Controlo

Conformidade Legal

Inovação

Ética

Responsabilidade

Tratamento de Dados Pessoais

Imagem: Jakub Żerdzicki em Unsplash

Os princípios e os direitos fundamentais consagrados no RGPD devem ser rigorosamente assegurados e cumpridos no âmbito do tratamento dos dados pessoais. A sua aplicação é essencial para assegurar a conformidade e a proteção da privacidade dos titulares dos dados.

No presente capítulo, pretendemos apresentar como os princípios e os direitos podem traduzir-se em práticas organizacionais conformes, designadamente ao nível da definição de procedimentos internos de tratamento de dados pessoais. Destacamos os processos de recolha, gestão, partilha e violação de dados pessoais e a implementação de ações de proteção.

Recolha de Dados Pessoais

Artigos 5.º/1/a) e 6.º

Licitude do Tratamento

Qual a razão ou o fundamento para a minha organização recolher dados pessoais?

Esta reflexão deve constituir o ponto de partida de qualquer atividade de tratamento de dados pessoais por parte da organização!

Nos termos do **RGPD**, e de acordo com o **princípio da licitude**, o tratamento de dados pessoais apenas é possível se se verificar um **fundamento legítimo**. Considera-se que o **tratamento** é **lícito** quando se verifique a existência de pelo menos uma das seguintes situações[6]:

Consentimento

Quando o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas

Execução de um contrato

Quando o tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte ou no âmbito de diligências pré-contratuais a pedido do titular dos dados

Interesses vitais

Quando o tratamento é necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular

[6] Quando esteja em causa o tratamento de categorias especiais de dados pessoais, será ainda necessário identificar uma condição específica de entre as definidas no artigo 9.º do RGPD, como, por exemplo, consentimento explícito, cumprimento de obrigações em matéria de legislação laboral, interesse público no domínio da saúde pública.

Recolha de Dados Pessoais

Artigos 5.º/1/a) e 6.º

Licitude do Tratamento

Interesse público

Quando o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investida a organização

Interesses legítimos

Quando o tratamento for necessário para prosseguir interesses legítimos da organização ou de terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular dos dados que exijam a proteção dos seus dados pessoais, em especial se for uma criança

A organização deve, assim, **definir o fundamento legal** que garanta que qualquer **tratamento** de dados pessoais **cumpre o princípio da licitude** e que cada **operação de tratamento assenta no fundamento** mais adequado às **circunstâncias específicas**.

Não existe uma hierarquia ou preferência de fundamento legal associadas à licitude do tratamento!
O consentimento não constitui o único fundamento legal para o tratamento, ou o mais adequado em determinadas operações de tratamento!

Recolha de Dados Pessoais

Artigos 5.º/1/b) e 6.º/4

Limitação das Finalidades

Uma associação, que desenvolve respostas sociais, recolhe dados pessoais dos beneficiários para efeitos da sua intervenção social. No âmbito de um novo projeto, cujo objetivo é criar uma rede de apoio integrado para prestar serviços de formação e capacitação, a organização deverá informar os beneficiários sobre a nova finalidade, obter o seu consentimento, atualizar a documentação relevante e, revelando-se necessário, implementar medidas de segurança adicionais.

A organização deve apenas efetuar o **tratamento** dos dados pessoais para **fins determinados**, **explícitos** e **legítimos**, **definidos previamente** à sua **recolha**. Os **dados não podem ser tratados posteriormente** de uma **forma incompatível** com essas **finalidades**.

Considerando que só após **conhecida a finalidade do tratamento** é possível apurar se os **dados pessoais recolhidos são necessários e não excessivos**, o **princípio da limitação das finalidades** assume uma importância fundamental no âmbito do tratamento de dados pessoais.

Qualquer **tratamento adicional** para além dos fins inicialmente especificados é **permitido** tendo em consideração:

- o **consentimento** do titular dos dados
- os fins de **arquivo de interesse público**, **de investigação científica** ou **histórica**, ou **estatísticos**, que sejam considerados **compatíveis** com as **finalidades iniciais**

Recolha de Dados Pessoais

Artigos 5.º/1/b) e 6.º/4

Limitação das Finalidades

Quando o **tratamento para fins diferentes** daqueles para os quais os dados pessoais foram **inicialmente recolhidos** não for realizado com base no anteriormente referido, a organização, a fim de verificar a **compatibilidade** de um **tratamento posterior** com a **finalidade inicial**, deve ter em conta:

qualquer **ligação** entre a **finalidade inicial** e o **tratamento futuro** previsto

o **contexto** da recolha dos dados pessoais, especificamente, a **relação** entre a **organização** e o **titular dos dados**

a **natureza** dos dados pessoais

as possíveis **consequências** da **alteração da finalidade** para os titulares dos dados

a existência de **garantias adequadas**, por exemplo, **encriptação** ou **pseudonimização**

Recolha de Dados Pessoais

Artigos 5.º/1/b) e 6.º/4

Limitação das Finalidades

Ao **definir** se o **novo fim** é **compatível** com os **fins inicialmente estabelecidos**, a organização poderá, assim, ter em atenção as seguintes **questões**:

- **A nova finalidade está completamente dissociada da finalidade inicial?**
- **O novo fim é inesperado?**
- **Quais os efeitos do tratamento adicional dos dados pessoais nos titulares dos dados?**
- **A organização consegue assegurar a proteção dos dados pessoais no âmbito da nova finalidade?**

A **organização** deve ser, desde o início, **clara e transparente** sobre o tratamento dos dados pessoais e assegurar que as **finalidades** estão em **conformidade** com as **expectativas** dos **titulares dos dados**.

Os dados pessoais devem ser utilizados apenas para os fins para os quais foram inicialmente recolhidos!

Recolha de Dados Pessoais

Artigo 5.º/1/c)

Minimização de Dados Pessoais

Para comunicação das atividades e projetos que desenvolve, uma misericórdia divulga mensalmente uma newsletter digital aos seus subscritores. Nesse âmbito, e mediante consentimento, recolhe unicamente o correio eletrónico dos subscritores, não se revelando necessário, para esse fim, recolher outros dados pessoais, como o nome, morada e/ou o contacto telefónico.

A organização deve garantir que, relativamente aos **fins do tratamento**, os dados pessoais que estão a ser recolhidos são:

- **adequados**
- **relevantes**
- **limitados ao necessário**

Os **fins** do tratamento determinam, assim, as **categorias de dados pessoais** que são necessárias recolher, exigindo que a organização considere a **quantidade mínima de dados** necessária para atingir essas finalidades.

No âmbito da **minimização de dados**, a organização poderá considerar as seguintes **questões**:

- **Qual o fim subjacente ao tratamento de dados pessoais?**
- **Que categorias de dados são necessárias para o fim definido?**
- **É possível atingir o fim definido com menos categorias de dados pessoais?**

Recolha de Dados Pessoais

Artigo 5.º/1/c)

Minimização de Dados Pessoais

Como parte da minimização dos dados, a organização deve também garantir o cumprimento do **princípio da limitação da conservação**, para assegurar a **conservação dos dados pessoais** durante e somente pelo **tempo necessário** para **cumprir os fins** para os quais os dados pessoais são tratados. Com o objetivo de garantir que os dados pessoais não são conservados mais tempo do que o necessário, a organização deve estabelecer **prazos** para o seu **apagamento** ou **anonimização**.

Não devem ser recolhidos dados excessivos ou irrelevantes!
Caso se verifique que a organização recolhe dados excessivos, o tratamento passará a ser ilícito!

Recolha de Dados Pessoais

Artigos 4.º/11 e 7.º

Consentimento para o Tratamento

Uma fundação que desenvolve atividades na área da proteção ambiental, recolhe dados pessoais dos seus doadores individuais para fins de realização de campanhas de angariação de fundos. Para esse efeito, solicitou o consentimento dos doadores mediante a disponibilização de um formulário no qual constam informações claras e completas sobre os dados que serão recolhidos e os fins do tratamento, obtendo consentimento através de uma caixa de seleção que inclui uma declaração de concordância da disponibilização dos dados pessoais para os fins descritos, bem como autorização para o seu tratamento.

O **consentimento** deve ser dado de forma **clara**, **afirmativa**, **voluntária** e **informada** para o tratamento dos dados pessoais. O consentimento poderá ser dado, designadamente, mediante:

uma **declaração escrita**, inclusive em formato eletrónico

uma **declaração oral** (gravada)

a **validação de uma opção** ao visitar um *website*

a **seleção dos parâmetros técnicos** para os serviços da sociedade da informação[7] ou através de **outra declaração**, **ou conduta** que indique claramente, neste contexto, a aceitação dos titulares dos dados ao tratamento proposto

[7] Nos termos da Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho de 9 de Setembro de 2015, serviços da sociedade da informação constituem qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços.

Recolha de Dados Pessoais

Artigos 4.º/11 e 7.º

Consentimento para o Tratamento

No âmbito do **consentimento** para o tratamento dos dados pessoais, a organização poderá ter em conta as seguintes **questões**:

- **Os mecanismos de recolha de consentimento garantem que este é dado livremente, de forma específica e informada e que é uma indicação expressa de que o titular concordou com o tratamento dos seus dados através de uma declaração ou de uma ação afirmativa clara?**
- **Se os dados pessoais foram mantidos com base no consentimento, cumprem o exigido pelo RGPD ou, se necessário, procurou novamente o consentimento do titular para garantir a conformidade com o RGPD?**
- **Existem evidências que demonstrem que o titular deu o seu consentimento?**
- **Existem procedimentos que permitam ao titular retirar o seu consentimento?**

O consentimento não deve ser presumido e deve ser obtido antes do início do tratamento dos dados. O silêncio, opções pré-validadas ou inatividade não constituem consentimento nos termos do RGPD!

Recolha de Dados Pessoais

Artigos 4.º/11 e 7.º

Consentimento para o Tratamento

Para garantir a conformidade com o RGPD[8], o consentimento deve ser uma **manifestação de vontade**:

Livre

O consentimento deve ser concedido de **forma voluntária**, sem qualquer tipo de coerção ou influência externa.

Como garantir?

Demonstrar que **é possível recusar ou retirar o consentimento** sem que o titular dos dados sofra prejuízos, como fraude, intimidação, coação ou outras consequências negativas significativas.

Informada

O titular dos dados deve receber todas as **informações necessárias** para tomar uma decisão consciente:

- identificação do responsável pelo tratamento
- fim de cada uma das operações de tratamento para as quais se pretende o consentimento
- (tipo de) dados que serão recolhidos e utilizados
- direito de retirar o consentimento
- prazo de conservação dos dados pessoais ou os critérios usados para definir esse prazo
- direitos do titular dos dados
- direito de apresentar reclamação junto da CNPD
- se a disponibilização de dados é uma obrigação legal, contratual ou condição para celebrar um contrato e as consequências no caso de incumprimento
- existência de decisões automatizadas e implicações desse tratamento

[8] Para mais informações, consultar Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679, Versão 1.1, adotadas em 4 de maio de 2020 pelo CECP,

Recolha de Dados Pessoais

Artigos 4.º/11 e 7.º

Consentimento para o Tratamento

Caso seja aplicável, o titular dos dados deve receber, ainda, **informações** sobre:

- os contactos do EPD
- os interesses legítimos do responsável pelo tratamento ou de um terceiro
- os destinatários dos dados pessoais
- se a organização pretende transferir os dados para outro país ou organização internacional

Como garantir?

É possível apresentar informações válidas por vários meios, tais como **declarações escritas ou orais**, **mensagens áudio ou vídeo**.
Em todos os casos, as informações devem ser transmitidas através de uma **linguagem clara e informal**.

Específica

O titular dos dados deve consentir para uma **finalidade específica**, de modo a prevenir a imposição de consentimento para múltiplas finalidades de forma agrupada.

Como garantir?

Separar o consentimento para cada finalidade específica, garantindo que o titular dos dados tem a opção de consentir separadamente para cada uma.

Recolha de Dados Pessoais

Artigos 4.º/11 e 7.º

Consentimento para o Tratamento

Inequívoca

O consentimento exige da parte do titular dos dados uma **autorização clara e direta**, sem ambiguidade ou dúvida sobre a sua intenção.

Como garantir?

Declaração Escrita

Carta ou E-mail: O titular dos dados escreve uma carta ou mensagem de e-mail à organização detalhando exatamente com o que concorda.

Formulário Eletrónico: O titular dos dados pode preencher um formulário online disponibilizado pela organização ou enviar por e-mail um documento digitalizado.

Declaração Oral Gravada

Conversa Telefónica: Obter consentimento através de uma chamada telefónica, garantindo que a informação seja clara e que o titular confirme a sua escolha (por exemplo, pressionando uma tecla ou confirmando oralmente).

Métodos Alternativos

O consentimento pode ser indicado por **outras ações** como, por exemplo, deslizar o dedo numa barra no ecrã, desde que as instruções sejam claras e a ação indique concordância com um pedido específico.

A organização pode certificar-se de que a declaração escrita é assinada pelo titular dos dados, por forma a eliminar todas as dúvidas possíveis e evitar uma potencial falta de provas no futuro!

Recolha de Dados Pessoais

Artigo 6.º/1/b)

Execução de um Contrato

No âmbito da prestação de serviços de saúde, uma mutualidade efetua o tratamento dos dados pessoais dos seus utentes com base no contrato de prestação de serviços celebrado entre ambas as partes. Os dados pessoais tratados incluem dados de saúde, contactos e histórico médico, que constituem informações necessárias para garantir a continuidade e a qualidade dos serviços de saúde prestados.

Este fundamento legal serve de base para **o tratamento de dados necessário à execução de um contrato celebrado** entre a **organização** e o **titular dos dados** ou para **medidas tomadas antes da celebração do contrato** (pré-contratual) **a pedido do titular dos dados**.

A **utilização do contrato** para fundamentar o tratamento está sujeita a **três condições**:

1. **existência de uma relação contratual ou pré-contratual entre a organização e o titular dos dados**: caso em que o **contrato já foi celebrado** ou quando o tratamento de dados é necessário para preparar o contrato - **fase pré-contratual** (por exemplo, troca de informações antes da assinatura do contrato, desde que o titular dos dados tenha solicitado este processo)

2. **validade jurídica do contrato**: o contrato entre o titular dos dados e o responsável pelo tratamento, ou o contrato que se pretende celebrar entre as partes, deve **ser legal ao abrigo da lei portuguesa** (por exemplo, deve cumprir os requisitos do direito contratual que constitui a sua base)

3. **o tratamento deve ser objetivamente necessário para a execução do contrato**: o tratamento deve apenas **permitir à organização o cumprimento das obrigações contratuais**, ou seja, fornecer o produto ou o serviço pretendido pelo titular dos dados, e **não deve visar outro objetivo**, como, por exemplo, a prossecução de objetivos distintos ou interesses exclusivos da organização

Recolha de Dados Pessoais

Artigo 6.º/1/b)

Execução de um Contrato

Para determinar se o **tratamento dos dados pessoais é necessário** para o fornecimento do produto ou serviço, a organização poderá ter em conta as seguintes **questões**:

- **Qual o objetivo do contrato?**
- **Quais as expectativas de ambas as partes do contrato?**

A organização, ao efetuar o tratamento de dados pessoais sob o fundamento da execução de um contrato, deve disponibilizar ao titular dos dados informações claras e transparentes sobre como os seus dados pessoais estão a ser tratados!

Recolha de Dados Pessoais

Artigo 6.º/1/f)

Interesse Legítimo

Uma cooperativa comunica mensalmente com os seus cooperadores por e-mail para efeitos de marketing direto. Estas comunicações mensais incluem uma revista, uma newsletter e a promoção de eventos/formações que apoiam os cooperadores. Esta atividade está alinhada com a missão e objetivos da cooperativa, no âmbito da sua relação com os seus cooperadores.

O **interesse legítimo** constituiu outro **fundamento jurídico** previsto no **RGPD** no qual a organização pode basear o tratamento de dados pessoais. Este fundamento prevê **três requisitos cumulativos** para que o **tratamento de dados pessoais** seja **lícito:**

1. **a prossecução de interesses legítimos pela organização ou por terceiros**: a organização deve identificar a finalidade/ objetivo do tratamento e verificar se é um interesse legítimo - **teste da finalidade**

Neste âmbito, a organização poderá considerar as seguintes **questões**:

- **Qual é o objetivo do tratamento?**
- **O tratamento é necessário para atingir um ou mais objetivos organizacionais específicos?**
- **Porque é que a atividade de tratamento é importante para organização?**

Artigo 6.º/1/f)

Interesse Legítimo

2 **a necessidade do tratamento dos dados pessoais para a realização do interesse legítimo prosseguido**: a organização deve verificar se o tratamento é necessário para esse fim – **teste da necessidade**

Neste âmbito, a organização poderá ter em conta os seguintes **aspectos**:

- **Há uma forma alternativa de atingir a finalidade sem realizar esta operação de tratamento?**
- **A organização consegue atingir a sua finalidade sem tratar os dados ou tratar menos dados?**

3 **a não prevalência sobre os interesses ou direitos e liberdades fundamentais dos titulares dos dados**: o tratamento não deve entrar em conflito com os direitos e liberdades dos titulares dos dados, tendo em conta as suas expectativas razoáveis – **teste do equilíbrio**

Neste âmbito, a organização poderá ter em atenção as seguintes **questões**:

Recolha de Dados Pessoais

Artigo 6.º/1/f)

Interesse Legítimo

- **É expectável por parte do titular dos dados que o tratamento ocorra?**
- **O tratamento é suscetível de ter um impacto negativo nos direitos e/ou liberdades do titular dos dados?**
- **Qual a natureza dos dados que serão alvo de tratamento (categorias especiais de dados, dados de crianças)?**

A organização pode realizar este **exercício** (três testes) no âmbito do fundamento do tratamento de dados pessoais com base no **interesse legítimo**[9], exigindo-se, para este efeito, uma **avaliação cuidada**, que deve ser efetuada **antes da atividade de tratamento**.

Caso, a partir deste exercício, a organização conclua que:

i. o **tratamento** dos dados **não é razoável**;
ii. os titulares dos dados **não esperariam um tratamento adicional**; ou
iii. o **tratamento** causa **danos injustificados**,

o **fundamento do interesse legítimo não pode servir de base** para o **tratamento de dados pessoais**.

Quando o tratamento se baseia em interesses legítimos, a organização deve também informar os titulares dos dados do seu direito de se oporem a esse tratamento!

[9] Os Considerandos 47 a 50 do RGPD apresentam exemplos de quando um responsável pelo tratamento pode ter um interesse legítimo no tratamento de dados pessoais.

Artigos 12.º e 15.º

Acesso a Dados Pessoais

Uma fundação que desenvolve atividades culturais e recreativas, para facilitar a comunicação e responder de forma efetiva aos pedidos de acesso aos dados pessoais por parte dos beneficiários das suas iniciativas, disponibiliza um endereço de correio eletrónico específico para ser utilizado pelos titulares dos dados para esse efeito, que consta da página de Política de Privacidade do seu site institucional.

O **direito de acesso** atribui ao titular dos dados o direito de **obter uma cópia dos seus dados pessoais**, bem como outras informações a que tem direito ao abrigo do RGPD. Neste sentido, constituiu **obrigação da organização assegurar o acesso** do titular dos dados aos seus dados pessoais.

O **RGPD não exige a utilização de um formulário específico** para efetuar um pedido de acesso, no entanto, a organização deve dispor de **medidas técnicas e organizativas** que permitam uma gestão de dados conforme, designadamente ao nível do controlo do alcance do tratamento e da quantidade de dados relacionados com o titular dos dados.

A existência de medidas técnicas e organizativas adequadas facilita a **verificação de todos os dados pessoais tratados** sobre o titular em causa, permitindo à organização estar **devidamente preparada para responder a pedidos de acesso**.

Na sequência de um **pedido de acesso** e caso o tratamento de dados pessoais do titular ocorra, a **organização deve**:

1

Confirmação do tratamento

Confirmar que, no momento da receção do pedido, efetuava o **tratamento dos dados pessoais** do titular dos dados e, se tiver sido efetuado um pedido de dados específico, que trata efetivamente os dados pessoais em questão.

Gestão de Dados Pessoais

Artigos 12.º e 15.º

Acesso a Dados Pessoais

2

Acesso aos dados pessoais

Facultar o acesso aos **dados pessoais solicitados** tal como se encontravam no momento em que o pedido foi apresentado.

Disponibilizar o acesso às seguintes **informações**:

- as **finalidades** do tratamento;
- as **categorias** dos dados pessoais;
- os **destinatários** da divulgação dos dados pessoais;
- os **prazos de conservação**, ou os **critérios** usados para a sua determinação;
- os vários **direitos** do titular dos dados;
- o **direito de apresentar uma reclamação** junto da **CNPD**;
- a **origem dos dados** tratados;
- a existência de **decisões automatizadas**;
- as **garantias vigentes** se os dados forem **transferidos** para um **país terceiro** ou uma **organização internacional**.

3

Informações sobre o tratamento

4

Cópia dos dados pessoais

Disponibilizar uma cópia dos dados pessoais solicitados que estavam a ser tratados no momento em que o pedido foi efetuado.
Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário, a informação é fornecida num formato eletrónico de uso corrente.

Artigos 12.º e 15.º

Acesso a Dados Pessoais

A organização deve **fornecer** ao titular dos dados as **informações** solicitadas, **sem demora injustificada** e no **prazo** de **um mês** a contar da **data de receção do pedido**. Este prazo pode ser **prorrogado até dois meses**, quando for necessário, tendo em conta a **complexidade** e o **número de pedidos** de acesso.

Se os pedidos apresentados por um titular de dados forem **manifestamente infundados ou excessivos**, nomeadamente devido ao seu **caráter repetitivo**, a organização pode:

- **Exigir o pagamento de uma taxa razoável**, tendo em conta os custos administrativos associados ao fornecimento das informações;
- **Recusar-se** a dar **seguimento** ao pedido.

O tempo para o cumprimento do prazo começa a contar a partir do dia em que o pedido é recebido pela organização, independentemente dessa solicitação ter sido apresentada junto de um outro contacto da organização ou de um diferente departamento/área da organização.

Cabe à organização demonstrar o caráter manifestamente infundado ou excessivo do pedido.

Gestão de Dados Pessoais

Artigos 5,º/1/d), 16.º e 19.º

Retificação de Dados Pessoais

Na sequência do acesso aos seus dados pessoais tratados por uma cooperativa que promove programas de formação, um formando verifica que as suas habilitações literárias não estão atualizadas. Neste sentido, apresenta junto da organização um pedido de retificação dos dados pessoais, fornecendo o documento comprovativo correspondente, de forma a ter essa informação atualizada.

A **exatidão dos dados** que a organização detém sobre os seus beneficiários, trabalhadores, financiadores e outras partes interessadas é fundamental no âmbito da gestão dos dados. Se a informação detida for inexata ou incompleta, não pode ser considerada uma fonte confiável para a tomada de decisões com base nos dados tratados pela organização.

O **direito de retificação** decorre do **princípio da exatidão**, concedendo ao titular dos dados o **direito de obter** a **retificação de dados pessoais inexatos**, ou de **obter** a **completude**, no caso da organização **tratar dados pessoais incompletos**.

Na sequência da **receção de um pedido válido de retificação** de dados pessoais, a organização deve:

1. **proceder à retificação** dos dados pessoais em relação aos quais o direito é exercido, no **prazo máximo de um mês** a **contar da data de receção do pedido** e enviar uma **comunicação ao titular dos dados** sobre o resultado da retificação

2. **comunicar a cada destinatário** a quem os dados pessoais tenham sido transmitidos da **retificação efetuada**, desde que isso não implique um esforço desproporcional, para que estes também possam efetuar as correções adequadas

Artigos 5,º/1/d), 16.º e 19.º

Retificação de Dados Pessoais

Na eventualidade de concluir que **não é possível dar seguimento** total ou parcial às **retificações** solicitadas, a organização deve **comunicar** essa **situação fundamentadamente**, no **prazo máximo de um mês após a receção do pedido**, a fim de, no caso de ser necessário, o **titular dos dados apresentar reclamação à CNPD**.

A organização deve implementar as medidas necessárias para garantir a exatidão dos dados pessoais tratados, designadamente para fazer face a eventuais desafios neste âmbito, relacionados, por exemplo, com a fonte dos dados, a periodicidade de atualização da informação e respostas a pedidos de retificação!

Artigos 17.º e 19.º

Eliminação de Dados Pessoais

Uma voluntária que deixou de colaborar com uma misericórdia no âmbito do desenvolvimento de atividades de voluntariado, solicita a eliminação de todos os seus dados pessoais tratados pela organização, designadamente as suas informações de contacto. A organização, verificando que não se aplicam exceções ao direito da titular dos dados, procede à eliminação dos seus dados pessoais.

O RGPD consagrou o **direito a ser esquecido**, que permite ao titular dos dados obter da organização o **apagamento dos seus dados pessoais**, mitigando, assim, os riscos associados ao armazenamento de longo prazo dos dados, como, por exemplo, acessos indevidos ou não autorizados, ou perdas acidentais.

A organização tem a **obrigação de apagar os dados pessoais**, sem demora injustificada, quando se aplique um dos seguintes **motivos**:

- Os dados pessoais **deixaram de ser necessários** para a **finalidade** que motivou a sua recolha ou tratamento
- O titular dos dados **retira o consentimento** em que se baseia o tratamento dos dados e não existe outro fundamento jurídico para o referido tratamento
- O titular dos dados **opõe-se** ao tratamento dos seus dados pessoais, nos termos definidos pelo RGPD

Eliminação de Dados Pessoais

Os dados pessoais **foram tratados ilicitamente** pela organização

Os dados pessoais têm de ser eliminados para o **cumprimento de uma obrigação jurídica** decorrente do direito da UE ou de um Estado-Membro a que a organização esteja sujeita

Os dados pessoais foram recolhidos no contexto da **oferta de serviços da sociedade da informação**

O **direito a ser esquecido não se aplica**, e a organização não tem a obrigação de proceder à eliminação dos dados, se o tratamento de dados pessoais for necessário:

- ao exercício da **liberdade de expressão e de informação**;
- ao cumprimento de uma **obrigação legal** a que a organização esteja sujeita, ao **exercício de funções de interesse público** ou ao **exercício da autoridade pública** de que esteja investida a organização;
- por motivos de **interesse público no domínio da saúde pública**, para fins de **arquivo de interesse público**, para fins **de investigação científica ou histórica** ou para **fins estatísticos**;
- para efeitos de **declaração**, **exercício** ou **defesa** de um **direito** num **processo judicial**.

Artigos 17.º e 19.º

Eliminação de Dados Pessoais

Após a receção de um **pedido válido de eliminação de dados pessoais**, a organização deve:

1. **proceder ao apagamento** dos dados pessoais em relação aos quais o direito é exercido, no **prazo máximo de um mês** a **contar da data de receção do pedido** e enviar uma **comunicação ao titular dos dados** sobre o resultado da eliminação

2. **comunicar a cada destinatário** a quem os dados pessoais tenham sido transmitidos da **eliminação efetuada**, desde que isso não implique um esforço desproporcional, de modo a que estes também possam realizar a eliminação adequada

Na eventualidade de concluir que **não é possível dar seguimento** total ou parcial ao **apagamento** dos dados, a organização deve **comunicar essa situação fundamentadamente**, no **prazo máximo de um mês após a receção do pedido**, a fim de, no caso de ser necessário, o **titular dos dados apresentar reclamação à CNPD**.

O processo de eliminação de dados pessoais deve ser rigorosamente documentado pela organização, não só para garantir a conformidade com as exigências legais, mas também para demonstrar transparência e responsabilidade perante os titulares dos dados e a CNPD!

Artigos 6.º, 13.º, 14.º, 26.º, 32.º e 35.º

Partilha de Dados Pessoais

Duas associações de desenvolvimento local, que trabalham em áreas complementares, partilham dados pessoais dos beneficiários para coordenar os serviços prestados. A partilha de dados foi efetuada com base no consentimento dos titulares, tendo sido adotadas medidas técnicas e organizativas para proteger os dados pessoais dos beneficiários.

A **partilha de dados pessoais** no contexto do RGPD é um processo que requer conformidade com as normas estabelecidas para **proteger os direitos e liberdades dos titulares dos dados**. Tal como referido no âmbito da licitude do tratamento, a partilha de dados pessoais entre organizações deve ocorrer apenas com **base num fundamento legítimo** previsto no **RGPD**.

Além disso, são igualmente necessárias **medidas técnicas e organizativas** que assegurem e comprovem a proteção dos dados pessoais contra, por exemplo, acessos não autorizados e usos indevidos.

A **transparência** e o **respeito pela privacidade** dos titulares dos dados são princípios fundamentais que devem guiar todas as operações de partilha de dados pessoais, assegurando que os direitos e liberdades dos titulares sejam preservados em todas as etapas desse processo.

A existência de **acordos de partilha de dados pessoais** bem definidos é uma forma de demonstrar a **conformidade** e de garantir que todos os envolvidos na partilha de dados compreendem e cumprem as suas **obrigações** no âmbito do RGPD, assegurando a **proteção** dos **direitos** dos titulares dos dados e **minimizando** os **riscos** de violações de privacidade.

Artigos 6.º, 13.º, 14.º, 26.º, 32.º e 35.º

Partilha de Dados Pessoais

No âmbito da partilha de dados pessoais, a **gestão do risco ou a AIPD** podem ajudar a **identificar** e **mitigar** riscos associados a esse processo, constituindo ferramentas fundamentais para assegurar que a **transferência de dados pessoais** é realizada de forma **segura** e em **conformidade com o RGPD**.

Cada organização tem o dever de assegurar que os dados pessoais não são tratados posteriormente de uma forma incompatível com as finalidades para as quais foram originalmente recolhidos pela organização que partilha os dados!

Artigos 45.º e seguintes

Transferência Internacional de Dados Pessoais

Para coordenar operações locais de forma eficaz, uma organização não governamental para o desenvolvimento (ONGD), que desenvolve programas de ajuda humanitária em países fora da UE, necessita de transferir dados pessoais dos seus voluntários e doadores para os seus escritórios regionais em alguns desses países terceiros. Para garantir a conformidade com o RGPD, a organização adotou cláusulas contratuais-tipo, procedeu à avaliação de riscos adicionais, para eventual adoção de medidas adicionais de segurança e obteve o consentimento dos seus voluntários e doadores, informando-os sobre a transferência dos seus dados para fora da UE e os potenciais riscos associados.

A **transferência internacional de dados pessoais** para **países terceiros** e **organizações internacionais** ao abrigo do **RGPD** está sujeita a **regras rigorosas** para **garantir** que os **direitos à privacidade e proteção de dados** dos cidadãos da UE sejam devidamente **respeitados e cumpridos**.

O RGPD estabelece que os dados pessoais só podem ser transferidos para fora do Espaço Económico Europeu se garantirem um **nível de proteção adequado**, equivalente ao oferecido dentro da UE. Esta adequação pode ser reconhecida através de uma **decisão de adequação** emitida pela **Comissão Europeia**, **atestando** que o **país de destino oferece garantias de proteção suficientes**.

Na **ausência de uma decisão de adequação**, o RGPD, designadamente através da apresentação de **garantias adequadas**, permite a transferência de dados com base em **instrumentos específicos**, como:

cláusulas contratuais-tipo, aprovadas pela Comissão Europeia

regras vinculativas aplicáveis às empresas, aprovadas pela CNPD

acordos internacionais celebrados entre a UE e países terceiros

Artigos 45.º e seguintes

Transferência Internacional de Dados Pessoais

A respeito da transferência internacional de dados pessoais para países terceiros e organizações internacionais, o **CEPD** adotou um conjunto de **recomendações** relativas às **medidas complementares aos instrumentos de transferência** para **assegurar o cumprimento do nível de proteção** dos dados pessoais da UE[10].

Neste âmbito, o CEPD definiu as seguintes **etapas** a serem consideradas pelas organizações:

1. **Conhecer as transferências**
2. **Identificar os instrumentos de transferência utilizados**
3. **Avaliar se o instrumento de transferência utilizado é eficaz tendo em conta todas as circunstâncias da transferência**
4. **Identificar e adotar medidas complementares**
5. **Adotar todas as medidas processuais formais exigidas pelas medidas complementares**
6. **Reavaliar com frequência adequada**

A CNPD tem o poder de suspender ou pôr termo às transferências de dados pessoais para o país terceiro se a proteção dos dados transferidos exigida pela legislação da UE, em especial o 46.º do RGPD e a Carta dos Direitos Fundamentais, não estiver assegurada.

[10] CEPD, Recomendações 01/2020, Versão 2.0, Adotado em 18 de junho de 2021

Artigos 4.º/12, 33.º, 34.º e 35.º

Violação de Dados Pessoais

Uma instituição particular de solidariedade social (IPSS) que presta apoio a vítimas de violência doméstica envia, por lapso, um email com dados pessoais de vários beneficiários para um destinatário incorreto, que não tem autorização para aceder a essas informações. O erro pode expor os beneficiários da organização a riscos de segurança e privacidade, e configura uma violação de dados pessoais. A organização notificou a CNPD no prazo de 72 horas após ter detetado a violação e informou as pessoas afetadas, em cumprimento das orientações fornecidas pela CNPD.

Nos termos do RGPD, uma **violação de dados pessoais** corresponde a *"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"*.

Considerando a **gravidade das consequências** para os direitos e liberdades dos titulares dos dados, **evitar** e **prevenir** eventuais **violações de dados pessoais** representam **desafios** consideráveis no âmbito da proteção e segurança dos dados pessoais.

Neste sentido, o RGPD exige que as organizações **apliquem medidas técnicas e organizativas** apropriadas para **assegurar** um **nível de segurança adequado ao risco** referente aos dados pessoais que estão a ser tratados.

A organização, logo após ter tido conhecimento de uma violação, deve procurar não só **conter o incidente**, mas também **avaliar o risco** que dele pode resultar. Ao avaliar o risco para os titulares dos dados na sequência de uma violação de dados pessoais, a organização deve considerar, assim, as **circunstâncias específicas da violação**, incluindo **a gravidade do impacto potencial** e **a probabilidade da sua ocorrência**.

Artigos 4.º/12, 33.º, 34.º e 35.º

Violação de Dados Pessoais

Nos termos das *"Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679"* (RGPD), elaboradas pelo Grupo de Trabalho sobre a proteção das pessoas no que diz respeito ao tratamento de dados pessoais[11], a **avaliação do risco** deve considerar os seguintes **critérios**:

1. **Tipo de violação** (integridade, confidencialidade ou disponibilidade dos dados)
2. **Natureza, sensibilidade e volume dos dados pessoais**
3. **Facilidade de identificação de pessoas singulares**
4. **Gravidade das consequências para as pessoas**
5. **Características especiais das pessoas singulares** (crianças ou outras pessoas vulneráveis)
6. **Características especiais do responsável pelo tratamento de dados** (natureza, função, atividades)
7. **Número de pessoas afetadas**
8. **Elementos gerais: combinação da gravidade do impacto potencial do risco sobre os direitos e liberdades dos titulares e da probabilidade de ocorrência do risco**

[11] Grupo de Trabalho, Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679, Adotadas em 3 de outubro de 2017, Revistas e adotadas pela última vez em 6 de fevereiro de 2018

Artigos 4.º/12, 33.º, 34.º e 35.º

Violação de Dados Pessoais

A organização, no âmbito da avaliação do risco, poderá elaborar uma **matriz de riscos**, que atribui uma **classificação aos riscos** com base na **interação entre a probabilidade e o impacto**, permitindo visualizar os riscos de forma mais clara e priorizar as ações necessárias para mitigá-los.

Riscos de **alta probabilidade** e de **alto impacto** podem, por exemplo, requerer **ações imediatas**, enquanto riscos de **baixa probabilidade** e de **impacto moderado** podem ser apenas alvo de **monitorização**.

Existem duas **obrigações principais** para a organização ao abrigo do regime da violação de dados pessoais:

1. **notificação de qualquer violação de dados pessoais à CNPD**, a menos que possa demonstrar que não é provável que resulte num risco para os titulares dos dados
2. **comunicação dessa violação aos titulares dos dados**, sempre que a violação seja suscetível de resultar num elevado risco para os próprios

O RGPD exige que a organização **notifique** a violação sem demora injustificada e, sempre que possível, **até 72 horas após ter tido conhecimento** da mesma. Este requisito de notificação visa encorajar a organização a **agir rapidamente em caso de violação**, **contê-la** e, se possível, **recuperar os dados pessoais afetados**, bem como obter a **orientação relevante por parte da CNPD**, designadamente sobre a decisão de comunicar ou não comunicar a violação aos titulares dos dados.

A organização deve garantir, em conformidade com o princípio da responsabilidade, que documenta toda e qualquer violação de dados pessoais, incluindo os factos relacionados com a violação, os seus efeitos e as medidas de mitigação implementadas - isto permitir-lhe-á demonstrar perante a CNPD o cumprimento do regime de notificação de violação de dados pessoais!

Medidas de Segurança

Imagem: FlyD em Unsplash

A organização deve implementar - desde a conceção e por defeito - medidas técnicas e organizativas que assegurem a segurança dos dados pessoais e a proteção dos direitos e liberdades dos titulares dos dados.

No presente capítulo apresentamos, de forma não exaustiva, exemplos de medidas[12], incentivando-se à implementação e/ou adaptação de outras soluções, tendo em consideração, designadamente, o contexto específico das atividades desenvolvidas pela organização, a natureza e volume de dados pessoais tratados, as finalidades do tratamento, bem como os recursos disponíveis.

[12] Para mais medidas, consultar a Diretriz/2023/1 da CNPD

Medidas de Segurança

Medidas Técnicas

Palavra-passe de acesso

Os trabalhadores devem ter um **identificador único**, como uma palavra-passe, **individual e intransmissível**, para permitir o acesso a dados pessoais. Uma palavra-passe forte deve incluir um mínimo de doze caracteres e deve conter um ou mais caracteres de letras (maíscula e minúscula), números, símbolos e pontuação.

Exemplo: **PrAtyCIeFArOs#1!**

As palavras-passes devem ser alteradas periodicamente, designadamente a cada 180 dias.

Autenticação multifator

O software de autenticação multifator poderá ser utilizado pela organização para reforçar a segurança. Em vez de utilizar apenas uma palavra-passe à sua escolha, o trabalhador pode ter um segundo fator, como um **código de acesso** enviado para o endereço de correio eletrónico, número de telefone ou dispositivo secundário.

Encriptação

A encriptação é o processo de **codificação da informação armazenada** num dispositivo e acrescenta um nível de segurança adicional.

A chave de encriptação deve cumprir as **regras de complexidade** exigidas para as palavras-passe.

Medidas de Segurança

Medidas Técnicas

Software anti-vírus

A utilização pela organização de um *software* antivírus é importante não só para **evitar ameaças** a partir da *Internet* (por correio eletrónico ou por fontes *Web*), mas também para **evitar a introdução de vírus** a partir de dispositivos portáteis.

É essencial que o software seja **atualizado regularmente**.

Firewalls

A organização deve dispor de dispositivos de segurança que efetuem a **monitorização do tráfego de rede** de entrada e saída e que **permitam ou bloqueiem tráfegos específicos** de acordo com um conjunto definido de regras de segurança, constituindo uma ferramenta fundamental no combate às tentativas de acesso não autorizado.

É fundamental que a *firewall* seja **atualizada regularmente**.

VPN

A organização deve assegurar a utilização de **Redes Privadas Virtuais** (VPN) para garantir que as comunicações sejam seguras, especialmente para os trabalhadores que realizam **trabalho remoto**.

Medidas de Segurança

Medidas Técnicas

Pseudonimização

A pseudonimização dos dados pessoais é recomendada para reduzir os riscos de exposição dos titulares e fornecer segurança adicional à organização. Embora não remova completamente as informações de identificação, a pseudonimização **dificulta a vinculação dos dados à identidade original**.

Para ser eficaz, as **informações adicionais devem ser armazenadas separadamente** e protegidas por medidas técnicas que impeçam a identificação dos titulares.

Anonimização

A anonimização dos dados pessoais é uma prática recomendada para **eliminar totalmente a possibilidade de identificação dos titulares**, garantindo a privacidade absoluta. Diferente da pseudonimização, a anonimização remove todos os identificadores, tornando os dados irreversíveis e impossíveis de serem associados a uma pessoa específica.

É importante que o processo de anonimização seja realizado de forma rigorosa, garantindo que não haja **risco de reidentificação**, mesmo quando combinados dados com outras informações.

Medidas de Segurança

Medidas Técnicas

Cópias de segurança

A criação de um **sistema de cópias de segurança** (*back-up*) atualizado, seguro e testado, totalmente separado das bases de dados principais e sem acessibilidade externa, garante a proteção contra perda de dados devido a falhas técnicas, ataques cibernéticos ou erros humanos.

Segurança física

A organização deve também considerar as medidas de segurança física necessárias para garantir a proteção dos dados pessoais num ambiente físico.
Alguns exemplos de **medidas práticas** de segurança física:

- ativar protetores de ecrã, exigindo uma palavra-passe para restabelecer o acesso;
- manter os escritórios e os armários fechados à chave;
- manter as salas ou os armários dos servidores fechados à chave e com restrições de acesso;
- aplicar políticas de secretárias limpas;
- assegurar que o equipamento TIC é eliminado de forma segura no fim da sua vida útil;
- assegurar a eliminação segura de registos em papel.

Medidas de Segurança

Medidas Organizativas

Política de recolha e conservação

A organização deve saber sempre **quais os dados pessoais que recolhe**, **onde são guardados** e **como circulam na organização**, pelo que devem ser definidas medidas claras sobre a sua recolha, prazos de conservação e os procedimentos para a sua eliminação segura quando não forem necessários.

Política de acesso

A implementação de medidas de acesso aos dados pessoais é essencial para garantir a segurança e a privacidade dos dados na organização, pelo que devem ser **definidas regras de permissão**, **as circunstâncias e as condições de acesso**, garantindo que apenas trabalhadores autorizados e qualificados possam aceder aos dados pessoais.

A definição de **procedimentos para a revisão regular dos acessos concedidos** deverá igualmente ser assegurada pela organização, nomeadamente através de **auditorias periódicas** e da **monitorização contínua** das atividades de acesso, para identificar/prevenir eventuais acessos não autorizados ou suspeitos.

Como medida adicional de reforço da segurança e privacidade no acesso aos dados pessoais, poderão ser celebrados Acordos de Confidencialidade entre a organização e os trabalhadores e/ou outras partes interessadas.

Medidas de Segurança

Medidas Organizativas

Planos de resposta a incidentes de segurança

A organização deve desenvolver planos de resposta a incidentes que incluam **regras para lidar com violações de dados**, como a **identificação de incidentes**, a **aplicação de medidas corretivas** e os **requisitos de comunicação obrigatória** ao abrigo do RGPD.

Auditorias e avaliações periódicas

As auditorias e avaliações periódicas são fundamentais para assegurar que a organização está a agir em conformidade com o RGPD e demais regulamentação de proteção de dados. Estas práticas permitem **identificar vulnerabilidades**, **avaliar a eficácia das medidas de segurança** implementadas e garantir que as **políticas, processos e procedimentos estão alinhados com as exigências legais**.

A identificação de eventuais **desconformidades**, **vulnerabilidades** ou **áreas de melhoria** deverão constar de **relatórios**, bem como devem ser apresentadas propostas de **ações corretivas** para colmatar falhas e fortalecer a proteção e a segurança dos dados pessoais.

A organização deve, ainda, **monitorizar a implementação das ações corretivas** para garantir que as alterações necessárias são efetivamente implementadas e asseguram a conformidade.

Medidas de Segurança

Medidas Organizativas

Política de privacidade

A organização deve estabelecer as **diretrizes e os procedimentos** adotados para proteger os dados pessoais, bem como **informar os titulares** sobre o **tratamento** que realiza, sobre os seus **direitos** e como **assegura o cumprimento das obrigações**. Ao definir claramente os princípios de proteção dos dados e as responsabilidades organizacionais, a política de privacidade ajuda a criar uma **cultura de conformidade** e a garantir que todos os trabalhadores e as demais partes interessadas estão alinhados neste âmbito, contribuindo para a **transparência** e a **confiança** dos titulares de dados.

A política de privacidade deve ser **revista periodicamente** e **constar do *website*** da organização.

Medidas de Segurança

Medidas Organizativas

Formação dos trabalhadores e de outras partes interessadas

A formação regular contribui para a criação de uma **cultura organizacional orientada para a segurança e privacidade dos dados**. Ao garantir que todos os trabalhadores e outras partes interessadas compreendem a importância da proteção dos dados pessoais e sabem como **agir em conformidade**, a organização fortalece a segurança e mantém a confiança dos titulares dos dados e das partes interessadas.

A formação e ações de capacitação e/ou de sensibilização a desenvolver pela organização poderão abranger os seguintes **temas**:

- Princípios básicos de proteção de dados;
- Políticas e procedimentos internos;
- Identificação e resposta a incidentes;
- Boas práticas de cibersegurança.

A sua organização pode aproveitar o Dia da Proteção de Dados, que se celebra anualmente a 28 de janeiro, como uma oportunidade para sensibilizar os trabalhadores e outras partes interessadas para a importância da privacidade e segurança dos dados pessoais, designadamente através da divulgação de folhetos, brochuras, vídeos ou podcasts alusivos ao tema, ou através da realização de uma ação de sensibilização!

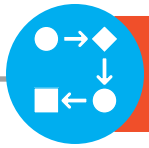
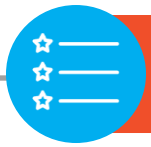
Checklist

Imagem: Glen Carstens-Peters em Unsplash

Apresentamos, no presente capítulo, uma *checklist* que tem como principal objetivo apoiar no cumprimento das principais exigências previstas no RGPD.

De acordo com a realidade e as necessidades específicas da sua organização, esta ferramenta poderá ser ajustada, com a inclusão de novos requisitos ou o aprofundamento dos requisitos apresentados.

Checklist

- [ ]  Identifique e mapeie os dados pessoais tratados pela sua organização, o fundamento legal de licitude do tratamento, bem como as finalidades associadas a cada operação de tratamento.
- [ ]  Defina um procedimento com regras e responsabilidades de resposta ao exercício de direitos dos titulares dos dados.
- [ ]  Designe, de acordo com a dimensão e a natureza das atividades de tratamento de dados da sua organização, um EPD ou um interlocutor responsável.
- [ ]  Informe os beneficiários e outras partes interessadas sempre que for necessário recolher os seus dados pessoais e obtenha o seu consentimento válido, nos casos aplicáveis.
- [ ]  Defina e implemente medidas técnicas e organizativas adequadas de proteção e segurança dos dados pessoais.
- [ ]  Conserve um registo de todas as atividades de tratamento sob a responsabilidade da sua organização. De modo a facilitar o cumprimento desta obrigação, a CNPD disponibiliza este modelo de registo.
- [ ]  Realize AIPD para atividades de tratamento de dados de alto risco.
- [ ]  Defina procedimentos para lidar com situações de violações de dados. Em caso de violação de dados pessoais deve notificar a CNPD através do preenchimento deste formulário.
- [ ]  Promova a capacitação dos trabalhadores sobre os temas do tratamento e proteção de dados. Como boa prática desenvolva sessões informativas junto dos beneficiários e de outras partes interessadas.

Referências

Imagem: Kimberly Farmer em Unsplash

- Regulamento Geral sobre a Proteção de Dados
- Lei de Proteção de Dados Pessoais
- Orientações e recomendações da Comissão Nacional de Proteção de Dados
- Orientações e recomendações do Comité Europeu para a Proteção de Dados
- Orientações e recomendações da Autoridade Espanhola de Proteção de Dados
- Orientações e recomendações da Autoridade Francesa de Proteção de Dados
- Orientações e recomendações da Autoridade Irlandesa de Proteção de Dados

Ficha Técnica

Título | Guia Prático: Proteção de Dados Pessoais – Economia Social

Autoria | Cátia Cohen e Mafalda Carvalhal

Revisão | Lénia Mestrinho

Edição | Nova School of Business and Economics | Novembro 2024

Design | Nova SBE Data Science Knowledge Center

Agradecimentos | Este projeto foi desenvolvido no âmbito da Iniciativa para a Equidade Social, uma parceria entre a Fundação "la Caixa", o BPI e a Nova SBE.
Agradecemos os contributos de Sandra Barbosa e Sara Rocha (DPO – Universidade Nova de Lisboa) e de Alice Caetano e Susana Lavado (Nova SBE Data Science Knowledge Center).

Citação recomendada:
Nova SBE (2024). Guia Prático: Proteção de Dados Pessoais – Economia Social. Nova School of Business & Economics (Social Equity Initiative), Carcavelos

NOVA SBE DATA SCIENCE KNOWLEDGE CENTER
Campus de Carcavelos
Rua da Holanda, 1
2775-405 Carcavelos

Sobre

Base de Dados Social
Social Equity Initiative Project

A Base de Dados Social é uma plataforma de dados abertos que disponibiliza informação sobre as organizações da economia social portuguesas. O projeto pretende, assim, promover o conhecimento do setor e contribuir para uma melhor e mais esclarecida tomada de decisão por parte de investidores sociais, empresas, voluntários, colaboradores, entre outras partes interessadas e, ainda, fomentar e permitir mais e melhores estudos sobre estas organizações.

bd.social@novasbe.pt

NOVA Data Science Knowledge Center
NOVA SCHOOL OF BUSINESS & ECONOMICS

O Nova SBE Data Science Knowledge Center tem como objetivo desenvolver conhecimento sobre o processo de tomada de decisão baseado em data e respetiva aplicação na sociedade. A posição que ocupamos dentro de uma escola de negócios e a forma como compreendemos ciências sociais, tecnologia, programação e métodos estatísticos permite-nos colmatar a lacuna entre organizações e tecnologia que gera, processa e usa data para criar impacto.

datascience@novasbe.pt

BPI | Fundação "la Caixa" NOVA SCHOOL OF BUSINESS & ECONOMICS

SOCIAL EQUITY INITIATIVE
KNOWLEDGE-DRIVEN PROGRESS

Em 2019, a Fundação "la Caixa", o BPI e a Nova School of Business & Economics (Nova SBE) juntaram-se para lançar a Iniciativa para a Equidade Social, uma parceria que visa impulsionar o setor social em Portugal com uma visão de longo prazo, traçando um retrato do setor social em Portugal e desenvolvendo programas de investigação e capacitação para apoiar organizações sociais.

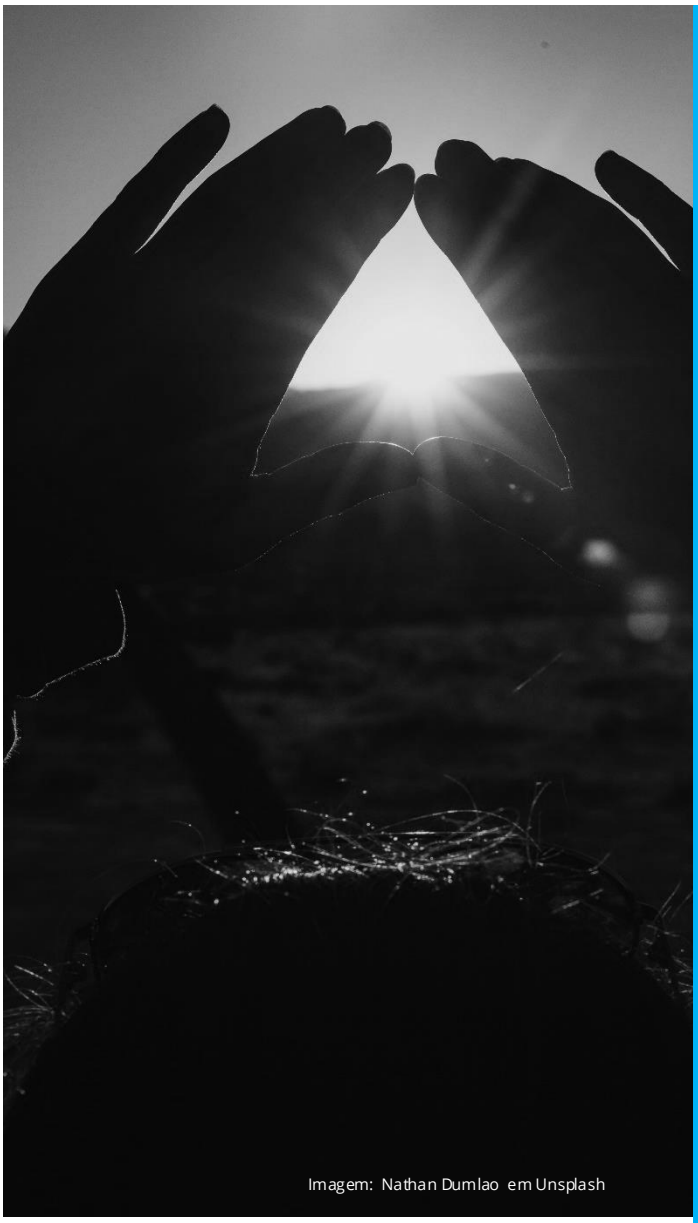


Imagem: Nathan Dumlao em Unsplash

BPI | Fundação "la Caixa" NOVA SCHOOL OF BUSINESS & ECONOMICS

SOCIAL EQUITY INITIATIVE

KNOWLEDGE-DRIVEN PROGRESS

Base de Dados Social

Social Equity Initiative Project

NOVA SCHOOL OF BUSINESS & ECONOMICS

Data Science Knowledge Center