RGPD

Disposições iniciais

NOÇÕES ESSENCIAIS

O RGPD tem como principal objetivo eliminar as assimetrias existentes nos diferentes regimes de proteção de dados em vigor nos diferentes países da União Europeia que representavam um obstáculo ao funcionamento do Mercado Único.

Verificando-se a necessidade de uniformizar o regime de proteção de dados pessoais nos países que integram o Espaço Europeu, o RGPD apresenta um conjunto de direitos dos titulares de dados pessoais e de obrigações de tratamento de dados que se impõem aos Responsáveis pelo Tratamento e Subcontratantes.

Atualmente, a maior parte dos dados pessoais processados pelas empresas recorrem a ferramentas informáticas que deverão ser adequadas a garantir uma boa aplicação do RGPD, no sentido de assegurar a confidencialidade, integridade e segurança dos dados.

Deste modo, no que respeita ao tratamento informático dos dados devem respeitar-se essencialmente duas características de segurança essenciais:

- Segurança no acesso à aplicação ou sistema pela utilização de *password* ou outro método de autenticação ou identificação;
- A possibilidade de rastreamento dos acessos.

Não obstante estes dois requisitos sejam essenciais para garantir a segurança do acesso aos dados, a aplicação do RGPD tem um alcance maior.
Para garantir os direitos do titular dos dados e os princípios de tratamento do RGPD é importante considerar a rastreabilidade da informação produzida e processada.

Conceito de dados pessoais

Nos termos e para os efeitos do artigo 4º, 1) consideram-se dados pessoais, toda a informação relativa a uma pessoa singular identificada ou identificável.

O RGPD aplica-se apenas aos dados das pessoais singulares, não abrangendo os dados das pessoas coletivas nem os dados das pessoas já falecidas, com exceção dos dados sensíveis.

Consideram-se dados pessoais toda a informação relativa à identificação do seu titular ou que possam levar à sua identificação de forma direta ou indireta, 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, religiosa ou social.

Exemplos de dados pessoais:

- Nome
- Número de identificação
  - BI, NIF, carta de condução, Passaporte.
- Endereços de identificação e localização
  - Físicos como por exemplo a morada
  - Eletrónicos: endereço de *email,* página *web*, página de Facebook, etc…

- Biométricos
  - Altura, peso, conotações físicas diversas
  - Genética
- Saúde
  - Síndromas, doenças
  - Desempenho físico oumental
  - Dados de diagnósticos como pressão arterial ou ECG
- Económicos
- Culturais
- Religiosos
- Sociais
- Políticos

Distinção entre segurança informática, sigilo profissional e RGPD

Antes de abordar a aplicação do RGPD no seu negócio é de extrema importância fazer uma distinção clara entre segurança informática e da Informação, sigilo profissional e RGPD.

No que diz respeito à segurança informática ou segurança da informação a base para uma implementação assenta sobre os seguintes pilares:

- Segurança, controlo e registo de acessos às instalações ou zonas sensíveis das instalações.
- Segurança, controlo e registo de acessos à rede ou dispositivos do negócio
  - Internamente (*Log-on* noscomputadores)
  - A partir do exterior (da internet a um recurso interno)
- Segurança, controlo e registo de acessos a recursos da rede ou de dispositivos isolados
- Utilização de *passwords* ou outros métodos de acesso de segurança.
- Formação adequada dos operadores.

Por exemplo, escrever a *password* num "post-it" e/ou partilhá-la com os colegas de trabalho é uma regra básica de segurança e não uma regra imposta pelo RGPD. Caso haja exista uma fuga de informação por causa deste comportamento, então estaremos sim a falar de uma não conformidade abrangida pelo RGPD.

Já o sigilo profissional consubstancia um dos deveres de todos os trabalhadores. O dever de sigilo será um dever prévio e anterior ao respeito pelo RGPD que não podendo ser com este confundido, dele faz parte integrante. De facto, as questões de ética são anteriores e sobre- põem-se a qualquer outro princípio.

Em resumo:

- As regras básicas da segurança dos dados digitais e físicos devem ser cumpridas de raiz, independentemente do RGPD.
- Os comportamentos éticos são basilares também para a aplicação do RGPD, porém nunca se deve sobrepor a este.

» O RGPD é uma lei composta por um conjunto de regulamentos que confere aos residentes europeus um maior controlo sobre os seus dados pessoais e requer que as empresas mantenham um nível de segurança apropriada para a proteção destes mesmos dados.

Princípios básicos de aplicação

A aplicação da lei numa empresa passa pelos seguintes passos:

» Levantamento: identificação dos dados pessoais que são processados na empresa e da legitimidade para proceder ao seu tratamento;

» Proteção: estabelecimento de controlos de segurança e rastreabilidade, ao nível da segurança informática e da segurança física dos dados;

» Controlo: monitorização dos acessos e operações de tratamento dos dados;

» Relatório: documentação das solicitações por parte dos titulares dos dados e do procedimento de resposta.

Responsável pelo tratamento e subcontratante

O RGPD aplica-se a todas as pessoas singulares ou coletivas, de natureza pública ou privada, que no âmbito da sua atividade comercial ou profissional tratam dados pessoais.

O responsável pelo tratamento é uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais.

Subcontratante é a pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

Razões pelas quais foi criado o regulamento

O RGPD tem como maior desiderato uniformizar o regime de tratamento de dados no espaço da União Europeia, considerado como requisito essencial para o bom funcionamento do Mercado Único e com a consequente proteção da privacidade dos titulares de dados e criação de uma cultura de respeito pelos dados pessoais.

Enquadramento legal

Regulamento Geral de Proteção de Dados, Código do Trabalho, Estatuto Deontológico, legislação nacional e comunitária no domínio da proteção de dados.

Direitos do titular dos dados

O titular dos dados tem os seguintes direitos:

» O direito a ser informado

» O direito de acesso aos seus dados

» O direito à retificação dos seus dados

- O direito a ser esquecido / apagado
- O direito à restrição de processamento
- O direito à portabilidade dos dados
- O direito de oposição
- Decisões individuais automatizadas, incluindo a definição de perfis.

Exercício dos direitos

O exercício dos direitos passa pela ação do DPO ou então através de automatização, exceção feita no caso dos direitos relacionados com o processamento automático, por óbvias razões.

No caso específico dos direitos de acesso, retificação, esquecimento, restrição e portabilidade, todos estes direitos podem ser proporcionados de forma automática, através, por exemplo de uma plataforma de gestão de identidade dos clientes. Caso a empresa possua um *website* funcional pode desenvolver ou aplicar uma plataforma para que os seus clientes, através de um painel de controlo, exerçam os seus direitos. Empresas como a Google, o Facebook, a Microsoft, etc. possuem este tipo de automatização.

Exemplo de *email* para pedido de consentimento, informação a os titulares e contacto.

Exmos. Srs.

Por forma a cumprir com o novo Regulamento Geral de Proteção de Dados, vimos por este meio, na qualidade de Responsáveis pelo Tratamento dos seus dados pessoais solicitar o seu consentimento, nos termos e para os efeitos dos arts. 4.º, 11), 6.º, n.º 1, a) e 7.º do RGPD. Deste modo, para que os seus dados pessoais possam continuar a ser objeto de tratamento torna-se necessário recolher o seu expresso consentimento nesse sentido.

Agradecemos, pois, que caso continue a manter interesse no tratamento dos seus dados pessoais responda a este *email* para confirmar o processamento, utilizando para tal os botões de voto acima ou, se o seu sistema não for compatível, responda apenas "sim, dou o meu consentimento para o processamento dos meus dados" a este *email*.

Se, pelo contrário, não desejar que os seus dados continuem a ser tratados, procederemos ao apagamento dos seus dados e cessaremos qualquer tratamento em curso.

Os seus dados, na nossa empresa são processados da seguinte forma:

- Publicidade;
- Comunicação institucional;
- Aconselhamento financeiro e fiscal.

Cabe-nos também informar que a partir de dia 25 de maio poderá solicitar-nos a aplicação dos seguintes direitos:

- O direito a ser informado
- O direito de acesso aos seus dados

- O direito à retificação dos seus dados
- O direito a ser esquecido / apagado
- O direito à restrição de processamento
- O direito à portabilidade dos dados
- O direito à objeção
- Direitos relacionados com o processamento automático.

A partir do momento em que este *email* seja enviado o titular dos dados terá toda a informação necessária para ativar os seus direitos.

Será necessário agora garantir que os procedimentos internos e as ferramentas, de facto permitem o cumprimento destes direitos.

Responsável pelo exercício dos direitos

Para que o RGPD possa ser facilmente implementado é necessário garantir que haverá um responsável por analisar os pedidos dos titulares dos dados para o exercício dos seus direitos e assume a responsabilidade de responder a tais pedidos. Importa aqui ter em atenção que estas respostas deverão ser dadas no prazo máximo de 30 dias.

Limitação ao exercício dos direitos

O exercício dos seus direitos por parte dos titulares dos dados poderá ser limitado por medida legislativa interna ou comunitário que sobreponham outros interesses superiores aos direitos dos titulares, desde que seja respeitada a essência dos direitos e obrigações previstos nos arti- gos 12.º a 22.º do RGPD.

Neste elenco de interesses e direitos que podem por em causa o exercício dos direitos dos titulares dos dados elencam-se, designadamente:

- Segurança do Estado;
- Defesa;
- Segurança pública;
- Prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública;
- Objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social;
- Defesa da independência judiciária e dos processos judiciais;
- Prevenção, investigação, deteção e repressão de violações de deontologia de profissões regulamentadas;
- Missão de controlo, de inspeção ou de regulamentação associada, ainda que ocasionalmente, ao exercício da autoridade pública;
- Defesa do titular dos dados ou dos direitos e liberdades de outrem;
- Execução de ações cíveis.

Estas medidas legislativas devem, contudo, incluir quando for relevante, disposições explícitas relativas, pelo menos:

» Finalidades do tratamento ou às diferentes categorias de tratamento;

» Categorias de dados pessoais;

» Alcance das limitações impostas;

» Garantias para evitar o abuso ou o acesso ou transferência ilícitos;

» Especificação do responsável pelo tratamento ou às categorias de responsáveis pelo tratamento;

» Os prazos de conservação e às garantias aplicáveis, tendo em conta a natureza, o âmbito e os objetivos do tratamento ou das categorias de tratamento;

» Riscos específicos para os direitos e liberdades dos titulares dos dados; e

» Direito dos titulares dos dados a serem informados da limitação, a menos que tal possa prejudicar o objetivo da limitação.

Princípios de proteção e tratamento de dados

Não existindo, presentemente, certificação neste domínio, impõem-se ao Responsável pelo Tratamento e Subcontratante o respeito pelos seguintes princípios:

» Princípio da responsabilidade pelo tratamento dos dados em conformidade com o RGPD

Compete ao Responsável pelo Tratamento ou Subcontratante aplicar as medidas técnicas e organizativas adequadas para assegurar e poder comprovar que o tratamento de dados é realizado em conformidade com o Regulamento. O pedido de autorização e a notificação feitos anteriormente à CNPD são agora substituídos pela autorresponsabilização do Responsável pelo Tratamento e Subcontratantes.

Cabe assim aos responsáveis pelo tratamento e subcontratantes assumirem a responsabilidade de respeito pelo RGPD e deterem as provas documentais de tal tratamento.

» Princípio da segurança do tratamento

Garantia de, tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, âmbito, contexto e finalidades do tratamento, bem como os riscos para os direitos e liberdades das pessoais singulares, o responsável pelo tratamento e subcontratante deve aplicar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, nomeadamente:

- Pseudonimização e a cifragem dos dados pessoais;
- Capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência per- manentes dos sistemas e dos serviços de tratamento;
- Capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempa- da no caso de um incidente físico ou técnico;
- Processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

›› Princípio da licitude, lealdade e transparência

A licitude para tratamento de dados encontra-se numa das alíneas do art.º 6.º do RGPD.

O consentimento é uma das causas de legitimidade do tratamento dos dados, mas este, deve agora ser um consentimento expresso, mediante um ato positivo do qual resulte a clara e informada autorização do titular para o tratamento dos seus dados.

Não é, contudo, a uma fonte de legitimidade para o tratamento de dados pessoais, podendo este ter outros fundamentos também previstos no art.º6.º, como por exemplo:

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

Será este o fundamento para o tratamento dos dados pessoais dos trabalhadores – existência de um contrato de trabalho – clientes – existência de contrato de prestação de serviços – ou outro titular dos dados com os quais exista um contrato ou se esteja a diligenciar nesse sentido.

c) o tratamento seja necessário para cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

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

e) o tratamento seja necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;

f) o tratamento seja necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os direitos e liberdades fun-damentais do titular que exijam a proteção dos dados pessoais, como sucede com o caso das crianças.

O tratamento dos dados deverá ainda ser leal – respeitar a finalidade para a qual os dados fo- ram recolhidos e não se desviar desta sem o consentimento dos titulares – e transparente – o titular dos dados deve conhecer o tratamento a que foram sujeitos os seus dados pessoais.

›› Princípio da limitação das finalidades e da conservação

Os dados pessoais deverão ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados para finalidades distintas a menos que exista um claro interesse superior que o preveja (v.g. fins de arquivo de interesse público).

O período de conservação dos dados deve ser o prazo estritamente necessário, devendo neste aspeto conhecer-se e respeitar-se os prazos de conservação e arquivo previstos na lei.

›› Princípio da minimização dos dados

O responsável pelo tratamento e o subcontratante devem orientar o momento da recolha de dados pelo princípio da minimização, devendo recolher apenas os dados pessoais que considere adequados, pertinentes e limitados ao tratamento que pretende fazer.

›› Princípio da exatidão

Decorre deste princípio o dever de os dados estarem permanentemente exatos e atualizados sempre que necessário, devendo ser adotados mecanismos para garantir a exatidão e atualização permanentes.

- **Princípio da integridade e confidencialidade**

Os dados deverão ser tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental.

Compete ao responsável pelo tratamento e subcontratante não só cumprir todos estes princípios como também ser capaz de demonstrar – por evidências – tal respeito.

Operações de tratamento de dados: exemplos

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

- *Email*
- Processamento de texto
- Bases de dados
- Folhas de cálculo
- *Software* de ERP ou CRM
- Processamento salarial
- Página de *Facebook* ou *website* com divulgação de informações com dados pessoais
- *Newsletter* com dados pessoais

Qualquer operação que seja executada nestes sistemas ou ferramentas e que envolva dados pessoais necessita de cumprir as normas do RGPD.

As operações podem ser tão simples como:

- Envio de um *email* com informações pessoais;
- Introdução de informação pessoal num documento Word ou Excel;
- Alteração de dados num ERP ou CRM;
- Aquisição de um novo cliente e introdução dos dados no ERP, CRM ou *software* de salários;
- A remoção de dados de um cliente do sistema.

Ou mais complexas como:

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

Exemplo de tratamento simples:

Caso prático:

Um cliente necessita de receber uma folha de Excel com um resumo dos salários dos trabalhadores da sua empresa. Este documento tem campos como:

- Nome do trabalhador
- Número de Segurança Social
- Salário e descontos

Riscos inerentes a este tratamento:

- Se o ficheiro for enviado para o cliente errado este poderá ter acesso a dados sensíveis.
- Se o ficheiro for capturado por "*hackers*" os dados poderão ser utilizados de forma maliciosa.

Para cumprir o RGPD devem ser adotadas as medidas para garantir que:

- Estamos a utilizar uma ferramenta apropriada para o envio
- Em caso de interceção dos dados somente o destinatário poderá abri-los
- Apenas os dados necessários de facto estão a ser transmitidos

Princípios básicos:

- Antes de proceder ao envio do ficheiro este deverá ser protegido por *password* usando o próprio Excel ou mesmo adicionando-o a um ficheiro ZIP encriptado e protegido por *password* longa e complexa.
- Esta *password* deve ser enviada ao cliente separadamente e por método distinto. Caso o ficheiro seja enviado por *email*, por exemplo, a *password* deverá ser transmitida por telefone.
- Caso o ficheiro tenha um tamanho superior ao permitido para um envio por *email*, este poderá ser colocado num serviço de *download* ou Cloud. Porém é necessário garantir que APENAS o destinatário terá acesso ao *download*. Um serviço protegido por *password* ou identidade (Partilha por *OneDrive* ou *Goole Drive*) é aceitável. Serviços gratuitos como "*Wetransfer*" não garantem que o *link* não possa ser partilhado e utilizado por outras pessoas.

Exemplo de execução:

- Exportar o ficheiro Excel a partir do *software* de salários para uma localização segura, na rede, para garantir a centralização dos dados e remoção simplificada em caso de necessidade.
- Usar o Excel para configurar uma *password* ou usar uma ferramenta ZIP que permita a encriptação.
- Adicionar o ficheiro protegido ao *email* e enviá-lo.
- Garantir através de recibos de leitura ou envio que o *email* foi bem recebido.

- Transmitir a *password* por telefone ao cliente

- Apagar o ficheiro da localização de rede para prevenir acessos não controlados.

- Para garantir que de facto não há qualquer cópia adicional dos dados para além das necessárias (no software de salários e do lado do cliente), podemos adicionalmente apagar o *email* dos itens enviados. Caso seja necessário um comprovativo de envio os *emails* de entrega e de leitura são geralmente validos, mas poderá ser solicitado uma resposta do cliente para validar a entrega.

Exemplo de aplicação complexa com envolvimento técnico de IT.

Caso prático:

Um cliente pede-nos para ser esquecido. Legalmente não existe qualquer problema, logo podemos cumprir com o direito.

Risco inerente a este tratamento:

- Não conseguir cumprir com o pedido

- Caso algum dado do cliente não for apagado e houver fuga de informação o cliente pode processar-nos por danos e podemos ser multados.

Considerações:

Esta execução depende de como os processos estão implementados na aquisição e armazenamento dos dados. Caso existam dados do cliente guardados nos computadores dos trabalhadores da nossa empresa muito dificilmente teremos capacidade de cumprir com este direito.

Principio:

A remoção do cliente da base de dados deverá ser executada quanto antes será necessário fazer prova não apenas da remoção dos dados da base de dados bem como de dados pessoais constantes em documentação interna da rede, salvaguardando as disposições legais que se sobreponham ao direito ao esquecimento.

Execução:

- No *software* de CRM, ERP ou base de dados de clientes será necessário aceder ao registo do cliente e proceder à remoção do registo.

- No sistema de ficheiros de rede é necessário verificar se existem documentos com dados do cliente em questão e apagar, na medida do possível e do legal, estes documentos (Word, Excel, CSV, XML, etc…)

- No sistema de *email*, é necessário assegurar, na medida do possível e do legal, que não há *emails* enviados ou recebidos com dados pessoais (daí a necessidade de apagar os *emails* enviados com dados pessoais como no exemplo anterior.

Boas práticas

Algumas boas práticas de operação e tratamento de dados:

- Nunca partilhar *passwords* de acesso ao PC ou outros acessos como *email*, serviços de *Cloud*
  - Em caso de necessidade de partilha de dados, utilizar meios que permitam uma rastreabilidade dos acessos
- Apagar dados que não sejam estritamente necessários
  - Por exemplo, apagar *emails* dos "enviados" quando tratam dados pessoais
- Manter os dados o mais centralizados possível para poder cumprir com os direitos de forma ágil
- Criar registos dos tratamentos dos dados ou aderir a ferramentas e plataformas que possuam tais registos
- Guardar em local seguro e confidencial todo e qualquer documento e suporte físico com dados pessoais
- Controlar os acessos aos documentos com dados pessoais.

Recolha dos dados

No momento da recolha dos dados é importante garantir dois requisitos: a licitude para o tratamento (cfr. art.º 6.º RGPD) e o cumprimento do dever de informação (cfr. arts. 13.º e 14.º do RGPD).

Embora nem sempre seja necessário recolher o consentimento do titular dos dados para o seu tratamento – porquanto não é necessário quando se verifica um dos requisitos das alíneas b), c), d), e) e f) do n.º 1 do art.º 6.º - sempre que tal for necessário, o consentimento terá que consubstanciar uma manifestação de vontade expressa, informada e voluntária (ato positivo inequívoco).

Com a entrada em vigor do RGPD – a 25 de maio de 2018 – dispomos de mais seis meses para recolher o consentimento para o tratamento de dados pessoais que já se encontrem na posse do Responsável pelo Tratamento e Subcontratante e que tenham sido recolhidos sem que o consentimento para o seu tratamento tenha sido expresso ou se verifique um dos requisitos do art.º 6.º, n.º 1, alíneas b), c), d), e) e f) do RGPD.

Para tal, o pedido de consentimento poderá ser efetuado utilizando os contactos atuais dos titulares dos dados para que estes manifestem de forma expressa, voluntária e informada – preenchendo um formulário específico, fazendo *reply* do *email* enviado ou adotando uma conduta da qual resulte clara a sua autorização para o tratamento dos dados.

O envio de um simples *email* como já mostrado acima deverá ser suficiente, porém é necessário que exista uma **resposta afirmativa à pergunta** – ato positivo inequívoco - se o titular autoriza o processamento e tratamento dos dados.

O consentimento também pode ser pedido através de assinatura, em adenda ao contrato.

Do exercício do dever de informação

Dispondo o titular dos dados do direito à informação e à transparência das informações, comunicações e regras para o exercício dos direitos, deve o responsável pelo tratamento ou sub-contratante garantir que aquando da recolha dos dados são facultadas ao titular dos dados as informações constantes do art.º 13.º ou, no caso de os dados não serem recolhidos na presença do titular as informações constantes do art.º 14.º , informação que pode ser prestada no momento do preenchimento do formulário *online* – mediante o acesso a um documento *word* como requisito essencial para que o formulário seja submetido – ou o envio do documento por *email* no prazo máximo de 30 dias.

Este dever apenas deixa de existir quando o titular dos dados já tenha conhecimento de todas estas informações ou, no caso de dados recolhidos na ausência do titular dos dados, quando o titular já tenha conhecimento das informações, se comprove a impossibilidade de disponibilizar a informação, a obtenção ou divulgação dos dados esteja expressamente prevista na lei ou os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional.

DO RESPONSÁVEL PELO TRATAMENTO DE DADOS

Garantir que presta todas as informações ao candidato a emprego e ao trabalhador, tanto no que respeita aos seus direitos como aos seus deveres como no que diz respeito à utilização das ferramentas informáticas ao seu dispor bem como nos comportamentos do dia-a-dia inclusive no cuidado com os documentos físicos que contenham dados pessoais (*v.g*. dossiers no arquivo, em cima da secretaria, documentos com dados pessoais que se encontrem a ser tratados em suporte físico).

Boas práticas de base:

- Não partilhar o utilizador nem a *password* de acesso ao PC
- Sempre que se afasta do PC bloqueá-lo (*ctrl+alt+del* + "Bloquear" no caso de *Win- dows*)
- Não tirar "*screenshots*" ou fotografias quando há dados sensíveis no ecrã.
- Não guardar dados sensíveis localmente no PC. Utilizar apenas as localizações e métodos aprovados pelos procedimentos conformes com o RGPD.
- Encriptar dados sensíveis aquando do envio por *email* ou partilha pública e removê-los imediatamente após a transferência.
- Guardar todas as pastas com dados pessoais em local seguro e de acesso condicionado (idealmente um local de arquivo onde o acesso não seja livre, podendo também optar-se por armários com portas fechadas à chave e guardadas em sitio seguro).
- Implementar uma política de segurança documental na qual cada trabalhador assuma a responsabilidade pelos documentos que lhe são confiados, não os deixando em cima da secretária sem vigilância ou noutro local onde não consiga garantir o sigilo.
- Não utilizar o verso de fotocópias com dados pessoais como folhas de rascunho.
- Não fornecer qualquer informação com dados pessoais pelo telefone, a menos que seja possível certificar a identidade da pessoa que solicita a informação.

DO SUBCONTRATANTE

O art.º 28.º do RGPD estabelece que sempre que o tratamento dos dados for efetuado por sua conta, o responsável pelo tratamento 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 dos titulares dos dados.

Para garantir que os nossos subcontratantes cumprem com o RGPD é necessário solicitar algumas informações relevantes como as que constam do documento anexo . Tal carta deverá ser enviada ou entregue, com comprovativo de entrega, antes do dia 25 de maio de 2018.

Inexistindo, de momento, uma certificação de *compliance* com o RGPD a garantia de respeito pelo RGPD deverá assentar na apresentação de ferramentas e elementos que evidenciem essa conformidade, nomeadamente:

- Contacto do DPO? Este é interno ou externo? Se não existe, qual é a razão?
- Manual de normas de conformidade com RGPD?
- Que *software* é utilizado para armazenar os dados pessoais dos clientes.
- Os dados estão guardados todos no mesmo *software* ou existem espalhados por mais aplicações?
- Os utilizadores tem *user* / *password* para aceder aos PC?
- Que sistema de *email* utilizam?
- Tem capacidade ou conhecimento para proceder à encriptação de dados?
- Possuem servidor interno ou estão assentes em *cloud* ou serviços internos distribuídos (partilha de ficheiros entre PC)?
- Os trabalhadores estão sensibilizados para o RGPD?
- O que consideram um "incidente"?
- Quais são os procedimentos utilizados em caso de incidente?

Algumas destas respostas são chave para compreender a conformidade de um subcontratante.

Se, por exemplo, o subcontratante não tiver DPO, é necessário compreender se tal sucede por não ser legalmente exigida a nomeação de DPO ou, pelo contrário, por não estar *compliance* com o RGPD.

A inexistência de um Código de Conduta ou Manual de Procedimentos evidenciam, por si só, o incumprimento do Regulamento ou a dimensão da empresa não o justifica.

Caso os utilizadores não tenham *user/password* ou outro método de identificação não há for- ma de aplicar a rastreabilidade dos acessos, logo não estarão conforme.

Caso tenham um sistema distribuído, será mais difícil cumprir com todos os direitos e muito mais complexo proceder a uma proteção eficaz dos dados.

Boas práticas de proteção de dados

EM SUPORTE FÍSICO

Importa antes de mais, enumerar todos os dados que se encontram em suporte físico (v.g. toda a informação que diz respeito aos alunos, professores, formadores, funcionários e outros) e garantir que os mesmos se encontram guardados num local que garante a sua segurança e integridade.

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

EM SUPORTE DIGITAL

O acesso aos documentos tratados em suporte informático deve ser condicionado a todos aqueles que em função das suas funções, a eles devam ter acesso.

O princípio da minimização dos acessos determina que deve ser selecionado criteriosamente o acesso aos dados por forma a impedir a sua dispersão por um grande número de pessoas e com isso se ponha em causa a sua confidencialidade.

O acesso aos dados deve ser feito mediante a credenciação com nome de utilizador e palavra passe – os quais são pessoais e intransmissíveis.

Deve garantir-se a existência de *firewalls* centrais, antivírus atualizados.

Os trabalhadores deverão ser informados – por escrito – da importância de manter sigilo sobre a sua palavra passe e de que não poderão deixar os computadores desbloqueados.

Boas práticas de tratamento de dados

EM SUPORTE FÍSICO

Os *dossiês* e documentos que contenham dados pessoais não poderão ser arquivados em local de fácil acesso, ou expostos em secretárias ou locais de fácil acesso por parte de terceiros ou de trabalhadores que não devam ter acesso a essa informação.

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

EM SUPORTE DIGITAL

O tratamento de dados pessoais em suporte digital deve garantir que os mesmos se encontram confidenciais.

Incidentes

DEFINIÇÃO DE INCIDENTES

Do ponto de vista de IT um incidente pode ser:

- Acesso malicioso ou não autorizado à rede
- Acesso malicioso ou não autorizado a um dispositivo
- Um acesso indevido aos dados (causado ou não por um acesso malicioso ou não autorizado)
- Uma divulgação em massa de dados pessoais por causa de um acesso indevido ou um incidente
- Envio de dados pessoais ao titular errado
- Roubo de um PC (encriptado ou não)
- Alteração de dados pessoais sem autorização do titular dos dados.

Tratamento de dados em suporte físico:

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

Deve existir um mecanismo que permita detetar a existência de um destes incidentes no mais curto prazo de tempo, devendo existir um procedimento de comunicação à Comissão Nacional de Proteção de Dados (CNPD) num prazo máximo de 72 horas e a cada um dos titulares de da- dos, se a violação de dados implicar um risco grave para os seus direitos, liberdades e garantias.

A comunicação aos titulares de dados pode ser feita por email, carta ou pelo *website* da empresa, caso não seja possível fazê-lo por nenhuma das outras vias. Pode, caso o número de titulares envolvidos e a dimensão do incidente o justifique, ser feita mediante comunicado de imprensa ou o dependendo da dimensão do incidente.

Plano de minimização de riscos

- Documentação de todas as operações de tratamento;
- Preenchimento das *check-lists* e implementação das medidas corretivas e de melhoria.

Reação e mitigação dos riscos

Nomeação dos responsáveis pela deteção de incidentes e definição de procedimento de comunicação à CNPD e aos titulares de dados em caso de risco elevado para os seus direitos, liberdades e garantias.

Definição dos riscos e das medidas que minimizam e atenuam os seus efeitos.

Responsabilidades e deveres dos trabalhadores

SIGILO PROFISSIONAL

Todos os trabalhadores, sem exceção, de acordo com o Código do trabalho, devem guardar segredo profissional sobre os factos e documentos de que tomem conhecimento no exercício das suas funções, dele só podendo ser dispensados por decisão judicial.

DEVERES NO ÂMBITO DO RGPD

Qualquer pessoa/entidade que, no âmbito e em virtude das funções que exerce, tenha acesso a dados pessoais de terceiros, está obrigado ao dever de sigilo e confidencialidade em relação aos dados pessoais que lhe tenham sido confiados. O incumprimento deste dever, muito mais vasto do que o dever de sigilo tal como consta do Código de Trabalho, é passível de responsabilidade disciplinar.

CLÁUSULAS CONTRATUAIS

Aquando da contratação dos novos trabalhadores o contrato de trabalho deverá acautelar o respeito pelo dever de sigilo e confidencialidade e facultar ao trabalhador todas as informações do artigo 13.º. Os trabalhadores com contrato anterior deverão assinar uma declaração que garanta o conhecimento dos seus direitos e deveres.

Responsabilidade de terceiros

Todos aqueles que tenham acesso aos dados pessoais recolhidos pelo Responsável pelo Tratamento e que não tenham a qualidade de subcontratantes, trabalhadores e outros com qual- quer vínculo contratual formalizado por escrito, deverão assinar uma declaração como Responsável do dever de sigilo e confidencialidade a que se obrigam.

Responsabilidade do subcontratante

DEMONSTRAÇÃO DE “COMPLIANCE”

Deve ser enviada a todos os subcontratantes uma carta a solicitar que estes prestem as garantias técnicas e organizativas de *compliance* com o RGPD. O cumprimento do art.º 28.º exige que a carta seja registada com aviso de receção ou outra forma que evidencie que a escolha ou continuidade do subcontratante se baseou na comprovação de *compliance* .

Contrato de prestação de serviços

Idêntico aos restantes trabalhadores.

A função do DPO

EXIGÊNCIA LEGAL

Para além das entidades públicas que, independentemente da dimensão, estão obrigadas a nomear um Encarregado de Proteção de Dados, no que respeita às entidades privadas essa obrigatoriedade existe sempre que a atividade privada desenvolvida, a título principal, implique:

a) Operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam **um controlo regular e sistemático dos titulares dos dados em grande escala**; ou

b) Operações de tratamento em grande escala das categoriais especiais de dados nos

termos do artigo 9.º do RGPD, ou de dados pessoais relacionados com condenações penais e contra ordenacionais nos termos do artigo 10.º do RGPD.

Inexistindo uma definição clara do que consiste grande escala para efeitos da alínea a) parece-nos que os CC que exerçam a sua atividade numa empresa de média dimensão e que pro- cedam ao tratamento de dados de forma regular e sistemático deverão nomear um DPO ou, caso entendam que tal não será necessário, ser apoiados por quem tenha conhecimentos no domínio do direito e das práticas de proteção de dados. Caso a opção do CC seja de não nomeação, parece-nos importante – para evidenciar o esforço de *compliance* – que se faça uma ata ou documento que evidencie a análise feita e os fundamentos da opção de não nomear um DPO.

Esta nomeação poderá recair sobre um trabalhador da entidade ou um prestador de serviços com o qual seja celebrado um contrato neste domínio.

Funções e Responsabilidades

Integram o elenco de funções do DPO, sem prejuízo de outras que se considerem necessárias para assegurar a *compliance* com o RGPD as seguintes funções:

» Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como todos os trabalhadores que tratem os dados, a respeito das suas obrigações no que respeita ao trata- mento de dados pessoais;

» Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal, bem como a necessidade de proceder a auditorias (periódicas ou não);

» Coopera com a autoridade de controlo;

» Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia, e consulta a autoridade de controlo sobre qualquer outro assunto;

» Sensibiliza os utilizadores para importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança, sempre que for detetado código malicioso;

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

Caso o DPO se encontre vinculado ao Responsável pelo Tratamento ou Subcontratante por um

vínculo de contrato de trabalho a sua responsabilidade pelo incumprimento do RGPD, apenas terá implicações a nível disciplinar. Distintamente, um DPO com contrato de prestação de ser- viços pode implicar a responsabilidade contratual e financeira daquele.

Perfil

Não obstante a referência legal recaia sobre uma pessoa com conhecimentos especializados na área do direito e da proteção de dados, o DPO deverá ser apoiado por uma equipa multidisciplinar que reúna competências nas mais diversas áreas, como a financeira, os recursos humanos, a tecnológica e arquivo, entre outras.

Assim, para além do exigido no domínio dos conhecimentos jurídicos o DPO dever conhecer as ferramentas utilizadas para o processamento dos dados, por forma a poder garantir que existe conformidade técnica e tecnológica das mesmas, sem descurar a segurança física dos dados.

Regime legal do incumprimento

CONDIÇÕES ATENUANTES E AGRAVANTES

Compete ao Responsável pelo Tratamento e Subcontratante reunir as evidências de *compliance* com o RGPD, evidencias essas que, em caso de violação de dados e incumprimento do Regulamento, serão passiveis de afastar a sua responsabilidade nos termos do Consideran- do 146.

O titular de dados que sofra prejuízos em virtude do incumprimento deste regulamento pode recorrer a uma autoridade de controlo – em Portugal a CNPD – ou requerer uma indemnização nos termos do art.º 82.º do RGPD.

As sanções aplicadas pela CNPD podem ser as seguintes:

As sanções a aplicar pela Autoridade de Controlo poderão ser:

- Coimas;
- Correção de comportamento;
- Advertência para que sejam respeitadas as indicações da Autoridade de Controlo; ou
- Repreensão;

No que às coimas respeita, estas deverão ser efetivas, proporcionadas e dissuasivas.
Na definição do montante das coimas serão ponderados os seguintes fatores:

- Natureza;
- Gravidade e duração da infração;
- Carácter doloso da infração;
- Medidas tomadas para atenuar os danos sofridos;
- Grau de responsabilidade ou eventuais infrações anteriores;
- Via pela qual a infração chegou ao conhecimento da autoridade de controlo;
- Cumprimento das medidas ordenadas contra o responsável pelo tratamento ou subcontratante;
- Cumprimento de um código de conduta ou quaisquer outros fatores agravantes ou atenuantes.

Portanto, a documentação das atividades de tratamento, a existência de um Código de Conduta e a comunicação à CNPD de qualquer violação no mais curto prazo de tempo são claramente fatores que minimizarão o grau de responsabilidade do Responsável pelo Tratamento ou Sub-contratante.