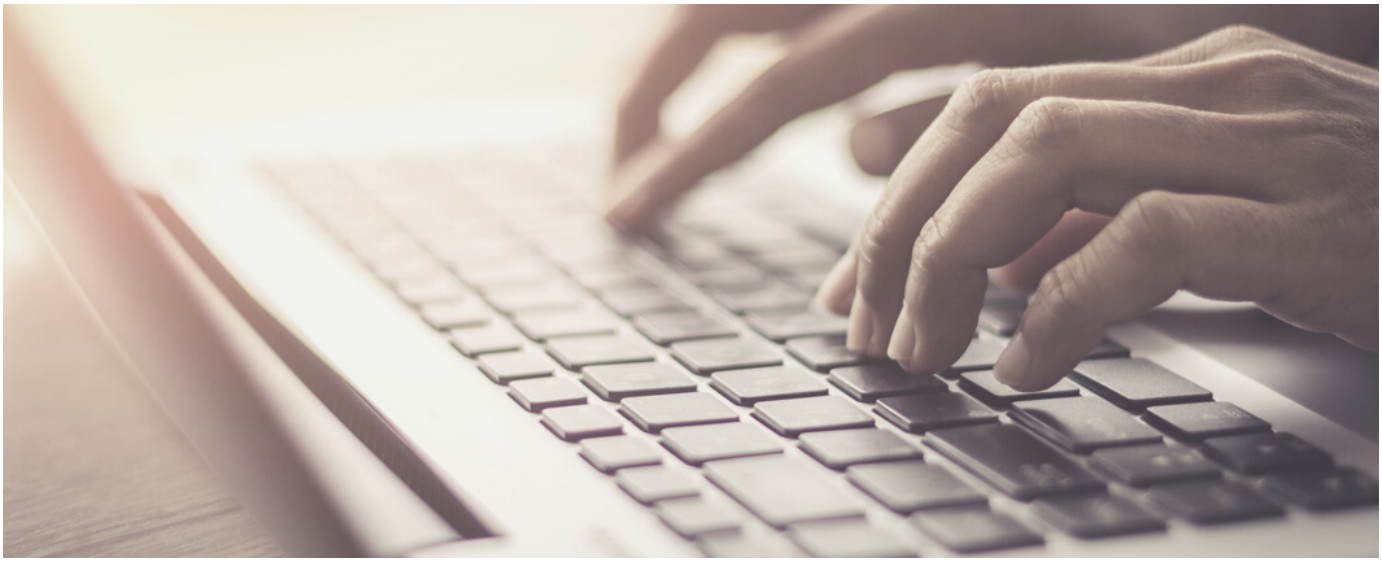


Medidas organizativas e de segurança na protecção de dados pessoais

NOTÍCIAS, NOVIDADES, TÓPICOS ACTUAIS

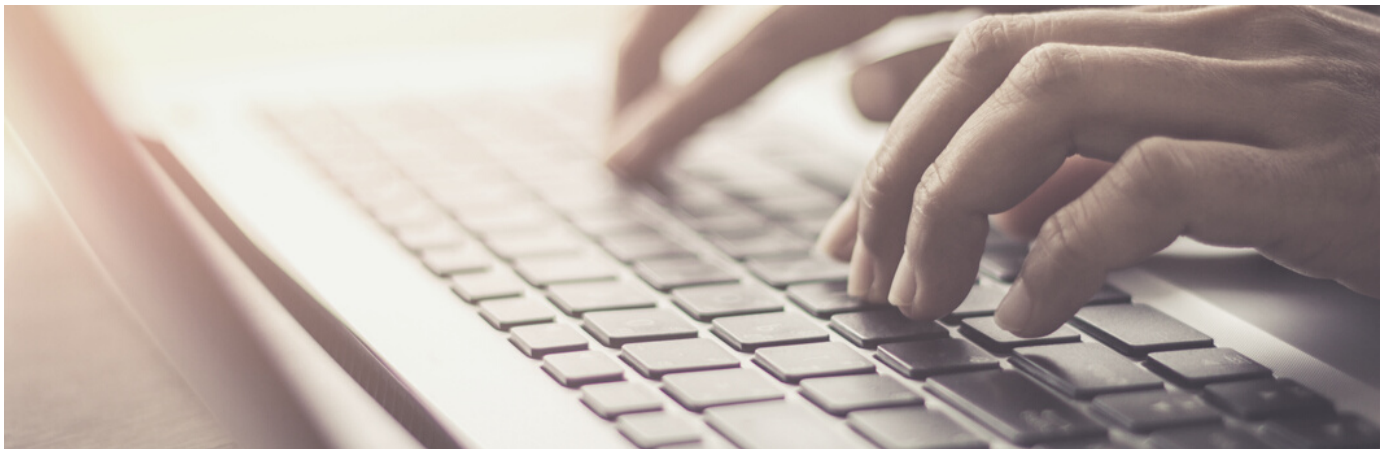
AUTORES

LÍDIA SILVESTRE
ADVOGADA

CATARINA BERNARDINO PEREIRA
ADVOGADA ESTAGIÁRIA

No âmbito das suas atribuições, e na sequência do aumento do número de ataques a sistemas de informação, a 10 de Janeiro de 2023, a CNPD aprovou a **Directriz/2023/1, sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais**, a qual se destina a sensibilizar os responsáveis pelo tratamento de dados pessoais, e aos subcontratantes, para as suas obrigações legais no domínio da segurança dos tratamentos e para a necessidade de adoptarem medidas de segurança que minimizem as consequências de eventuais ataques a sistemas de informação.

Indica a CNPD que, nos ataques ocorridos, tem sido detectada *"a exploração das vulnerabilidades das infraestruturas, a falta de formação dos utilizadores para*



detectarem campanhas de phishing que permitem depois a distribuição de malware, com especial relevância para os ataques de ransomware [e] a ausência de consciencialização dos responsáveis pelos tratamentos quanto aos riscos para os direitos dos titulares dos dados que a falta de investimento em mecanismos de segurança acarreta".

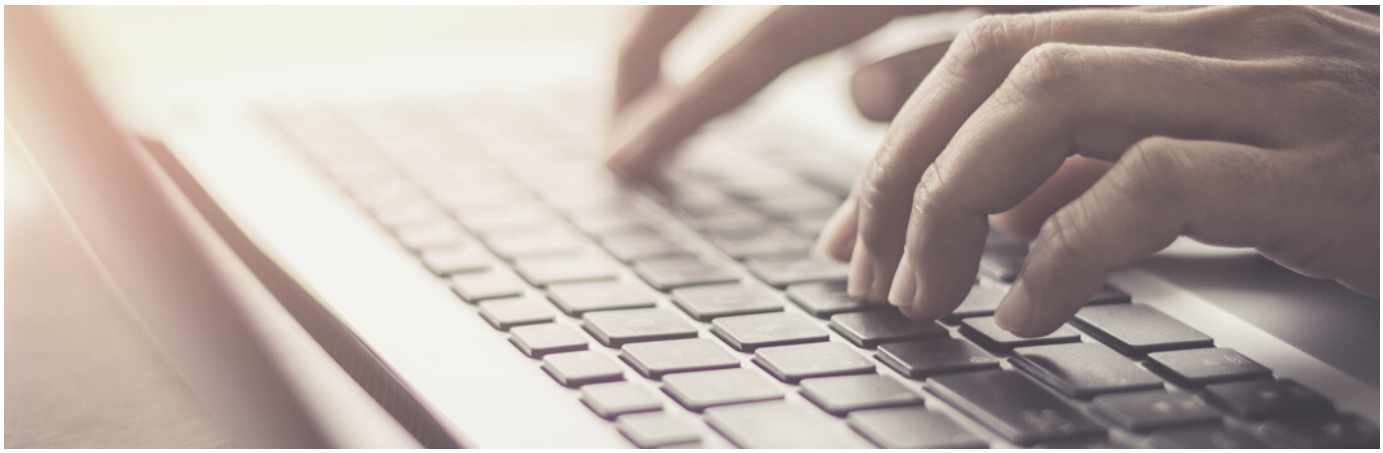
Devendo o responsável pelo tratamento adoptar uma política interna que lhe permita detectar e gerir incidentes de segurança com impacto na protecção de dados pessoais, são exemplificadas, na Directriz, medidas de segurança que deverão ser aplicadas no âmbito do tratamento de dados pessoais, as quais estarão, naturalmente, sujeitas a actualização, em virtude da sua directa dependência do desenvolvimento tecnológico.

1. Medidas técnicas e organizativas a adoptar pelo responsável pelo tratamento e pelo subcontratante:

Como corolário da obrigação do responsável pelo tratamento e do subcontratante de aplicar medidas técnicas e organizativas adequadas para assegurar um nível de segurança apropriado ao risco – tendo, para o efeito, em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento e os riscos para os direitos e liberdades das pessoas singulares -, prevê a CNPD que devem ser consideradas as seguintes medidas de segurança, consoante o que for adequado às características e sensibilidade de cada tratamento de dados pessoais efectuado e às especificidades da concreta organização:

A. Organizativas:

1) Definir e exercitar regularmente o plano de resposta a incidentes e recuperação do desastre, prevendo os mecanismos necessários para garantir a segurança da informação e a resiliência dos sistemas e serviços, bem como assegurar que a disponibilidade dos dados é restabelecida atempadamente após um incidente;
2) Classificar a informação de acordo com o nível de confidencialidade e sensibilidade e adoptar as medidas organizativas e técnicas adequadas à classificação;
3) Documentar as políticas de segurança;
4) Adoptar procedimentos de análise para a monitorização dos fluxos de tráfego na rede;
5) Definir políticas de gestão de palavras-passe seguras, impondo requisitos para o tamanho, a composição, o armazenamento e a frequência com que uma palavra-passe precisa de ser alterada;
6) Criar uma política de gestão de ciclo de vida dos utilizadores, para garantir que cada trabalhador tem acesso apenas aos dados necessários para executar as suas funções e rever, com frequência, as permissões dos



vários perfis de utilizadores, se possível, bem como a desactivação de perfis inactivos;
7) Adoptar alarmística que permita identificar situações de acesso, tentativas ou utilização indevida;
8) Definir, numa fase inicial, as melhores práticas de segurança de informação a adoptar, considerando, em particular, os princípios de protecção de dados desde a concepção e por defeito, análises de risco do tratamento e do ciclo de vida dos dados, métodos de pseudonimização e anonimização dos dados;
9) Realizar auditorias de segurança de tecnologias de informação ("TI") e avaliações de vulnerabilidade sistemáticas;
10) Verificar se as medidas de segurança definidas estão em prática, garantindo que são eficazes e actualizando-as regularmente, (incluindo as que são implementadas pelos subcontratantes nos tratamentos de dados);
11) Documentar e corrigir, rapidamente, as vulnerabilidades de segurança detectadas;
12) Tomar as medidas necessárias para garantir o pleno cumprimento dos deveres de notificação de uma violação de dados pessoais à CNPD, em conformidade com o artigo 33.º do RGPD, em particular no que diz respeito ao desenvolvimento de uma política interna para lidar e documentar eventuais violações de dados pessoais;
13) Fomentar, junto dos colaboradores, uma cultura de privacidade e segurança da informação, para que cada colaborador esteja capacitado para reconhecer potenciais ameaças e agir em conformidade, reduzindo a ocorrência e o impacto do erro humano;
14) Informar os trabalhadores do dever de confidencialidade a que estão sujeitos pelo facto de tratarem dados pessoais;
15) Avaliar periodicamente as medidas de segurança, técnicas e organizativas, internas e proceder à sua actualização e revisão sempre que necessário.

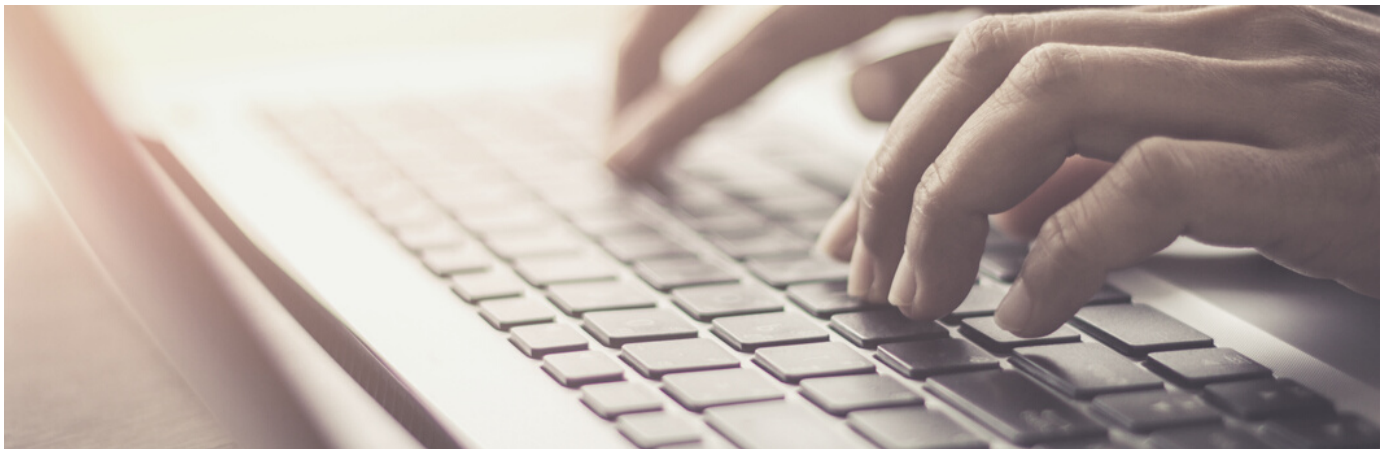
B.Técnicas:

B.1. Autenticação:

1) Utilizar credenciais fortes com palavras-passe longas (pelo menos 12 caracteres), únicas, complexas e com números, símbolos, letras maiúsculas e minúsculas, alterando-as com frequência;
2) Equacionar, designadamente face à sensibilidade da informação, aos privilégios dos utilizadores ou à forma de acesso (v.g. remota), a aplicação de autenticação *multifactor*;

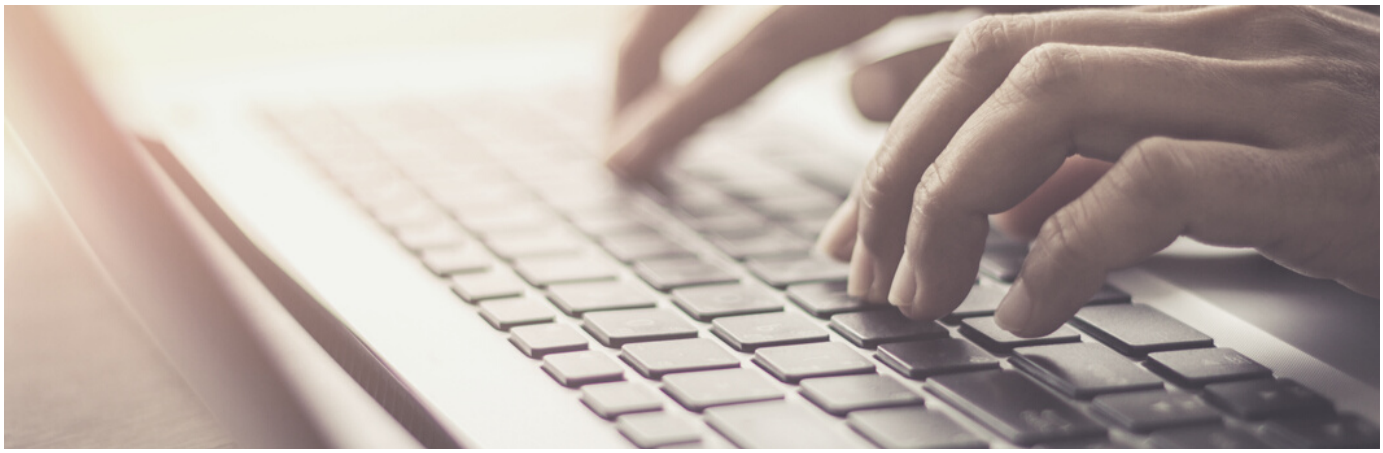
B.2. Infra-estrutura e sistemas:

3) Garantir que os sistemas operativos de servidores e terminais se encontram actualizados, bem como todas as aplicações (por exemplo, *browser* e *plugins*);
4) Manter o *firmware* dos equipamentos de rede actualizado;
5) Desenhar e organizar os sistemas e a infra-



estructura por forma a segmentar ou isolar os sistemas e as redes de dados para prevenir a propagação de *malware* dentro da organização e para sistemas externos;
6) Robustecer a segurança dos postos de trabalho e servidores, nomeadamente:
a) bloquear o acesso a sítios que sejam susceptíveis de constituir um risco para a segurança;
b) bloquear os redireccionamentos suspeitos através de motores de busca;
c) bloquear de imediato os ficheiros e aplicações infectadas com *malware*;
d) realizar inspecção periódica do estado e utilização dos recursos do sistema;
e) monitorizar a utilização do software instalado;
f) activar e conservar os registos de auditoria (log);
g) validar os acessos por IP aos servidores que estão expostos ao público;
h) alterar o porto configurado por omissão para o protocolo de acessos remotos (“RDP”).

B.3. Ferramenta de correio electrónico:
7) Definir de forma clara e inequívoca políticas e procedimentos internos sobre o específico envio de mensagens de correio electrónico contendo dados pessoais, que introduzam as verificações adicionais necessárias, no sentido de:
a) garantir a inserção dos endereços de correio electrónico dos destinatários no campo 'Bcc:', nos casos de múltiplos destinatários;
b) prevenir erros na introdução manual de endereços de correio electrónico;
c) assegurar que os ficheiros enviados em anexo contêm apenas os dados pessoais que se pretendem comunicar;
8) Equacionar a criação de listas de distribuição ou grupos de contacto, com o objectivo de prevenir a divulgação dos endereços dos destinatários em operações de envio massivo de mensagens de correio electrónico;
9) Equacionar a criação de regras com o objectivo de adiar/atrasar a entrega de mensagens de correio electrónico contendo dados pessoais, mantendo-as na ‘Caixa de Saída’ por um tempo determinado, permitindo verificações de conformidade, após clique em 'Enviar’;
10) Encriptar com código, ao qual só o destinatário tenha acesso, os e-mails e/ou anexos enviados que contenham dados pessoais;
11) Confirmar com o destinatário, antes de envio de e-mail contendo dados pessoais, o endereço de e-mail preferencial para contacto;
12) Realizar acções de formação no sentido de capacitar os trabalhadores a operar os mecanismos de envio de mensagens de correio electrónico de acordo com os procedimentos definidos, sensibilizando-os para os erros mais comuns e incentivando-os à dupla verificação;
13) Reforçar o sistema de alerta da ferramenta de alarmística utilizada pela entidade, para



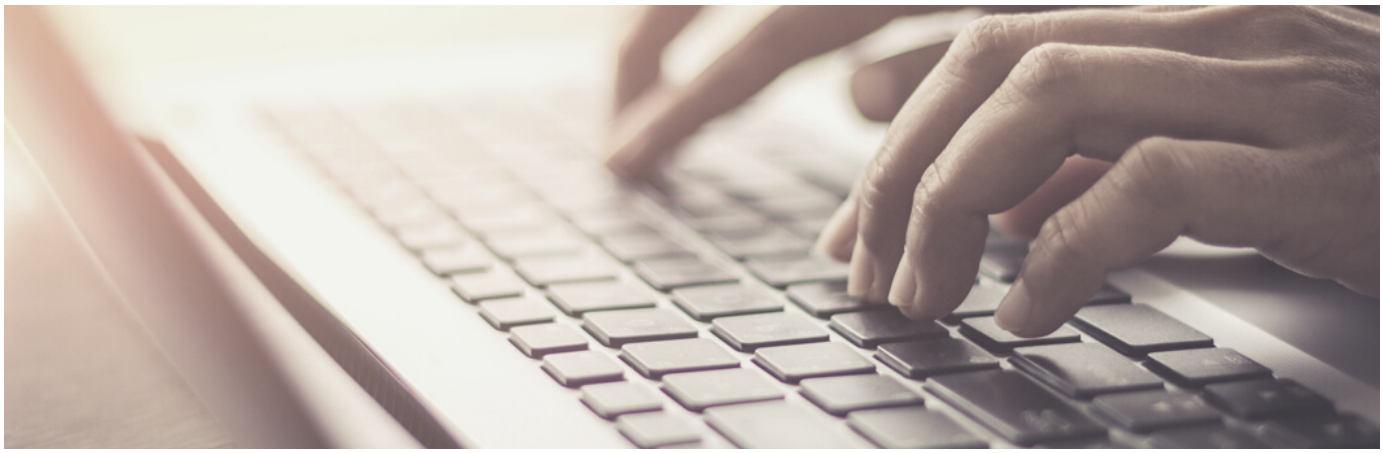
assegurar visibilidade imediata sobre a criação por utilizadores de regras de encaminhamento automático de e-mails para contas externas;
14) Reforçar o sistema com ferramentas *antiphishing* e *antispam*, que permitam bloquear ligações e/ou anexos com código malicioso;
15) Adoptar controlos de segurança que permitam classificar e proteger as mensagens de correio electrónico sensíveis.

B.4. Protecção contra *malware*:
16) Utilizar encriptação segura, especialmente no caso de credenciais de acesso, de dados especiais, de natureza altamente pessoal ou financeiros;
17) Criar um sistema de cópias de segurança (*backup*) actualizado, seguro e testado, totalmente separado das bases de dados principais e sem acessibilidade externa;
18) Reforçar o sistema com ferramentas *antimalware* que inclua a capacidade de o verificar e detectar, bem como o bloqueio em tempo real de ameaças do tipo *ransomware*.

B.5. Utilização de equipamentos em ambiente externo:
19) Armazenar dados em sistemas internos, protegidos com medidas de segurança apropriadas, e acessíveis remotamente através mecanismos de acesso seguro (VPN);
20) Permitir acessos apenas por VPN;
21) Bloquear as contas após várias tentativas inválidas de login;
22) Activar a autenticação *multifactor* para os utilizadores dos equipamentos;
23) Aplicar cifragem dos dados no sistema operativo;
24) Sempre que for aplicável, activar a funcionalidade de *"remote wipe"* e *"find my device"*;
25) Efectuar cópias de segurança automáticas das pastas de trabalho, quando o equipamento se encontra ligado à rede da entidade;
26) Definir regras claras e adequadas para a utilização de equipamentos em ambiente externo.

B.6. Armazenamento de documentos em papel que contenham dados pessoais:
27) Utilizar papel e impressão que seja durável;
28) Conservar documentação em local com controlo de humidade e temperatura;
29) Armazenar os documentos que contêm dados pessoais sensíveis em local fechado, resistente ao fogo e inundação, devidamente organizados;
30) Controlar os acessos, com registo das respectivas data e hora, de quem acede e do(s) específico(s) documento(s) acedido(s);
31) Destruir os documentos através de equipamento específico que garanta a destruição "segura".

B.7. Transporte de informação que integre dados pessoais:

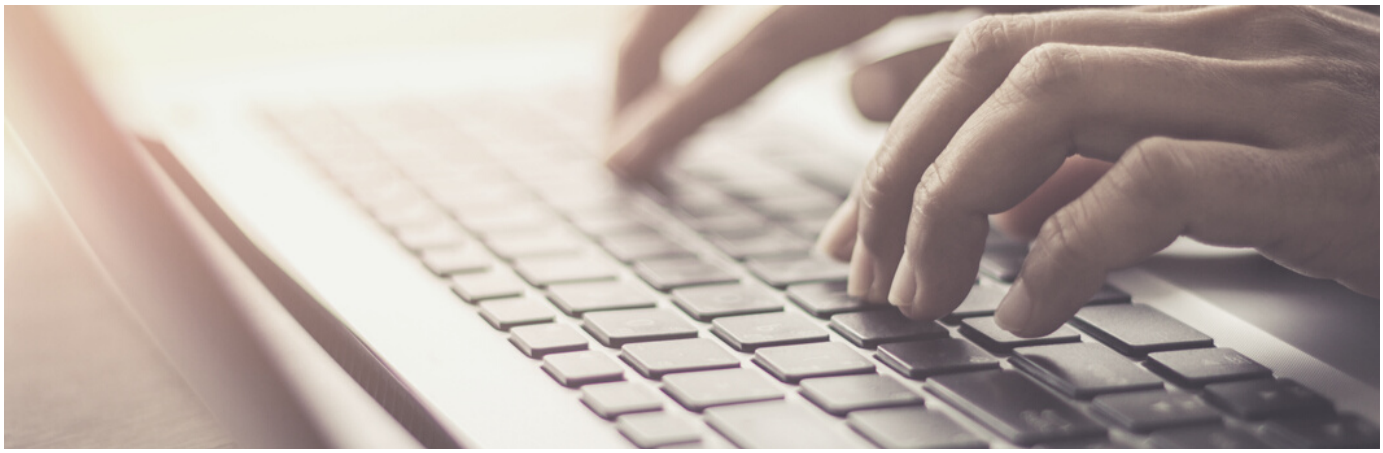


32) Adoptar medidas para impedir que, no transporte de informação com dados pessoais, estes possam ser lidos, copiados, alterados ou eliminados de forma não autorizada;
33) Utilizar encriptação segura no transporte, em dispositivos de massa ou arquivo potencialmente permanente (CD/DVD/PEN USB).

Tais medidas baseiam-se nas obrigações previstas no RGPD, entre as quais destacamos as seguintes:

2. Sobre a notificação de violação de dados pessoais:

a. Cabendo ao **responsável pelo tratamento de dados pessoais assegurar o respeito pelos direitos e interesses dos titulares de dados**, sobre ele recai o dever de verificar e demonstrar, antes de realizar um tratamento, se cumpre todas as regras de protecção de dados e se os concretos tratamentos de dados estão em conformidade com os princípios relativos ao tratamento de dados elencados no n.º 1 do artigo 5.º do RGPD.
Para o efeito, deverá o responsável adaptar o seu modelo de negócio ou de gestão pública, e os respectivos meios técnicos e organizativos, de forma a assegurar o efectivo cumprimento da lei e a devida protecção dos dados pessoais e da esfera de interesses, direitos e liberdades dos seus titulares, através da regular avaliação das operações de tratamento e do impacto das das tecnologias no funcionamento das suas organizações, bem como dos riscos para os direitos e liberdades das pessoas singulares.
b. Entendendo-se como **«violação de dados pessoais»** uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, perda, alteração, divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, nas **situações em que a violação seja susceptível de resultar num risco para os direitos e liberdades das pessoas singulares, tal violação deverá ser notificada à CNPD**, sempre que possível, até 72 horas, seguidas, após ter tido conhecimento da mesma.
c. Ainda que o responsável pelo tratamento considere que não é exigível a notificação à CNPD, estará sempre **obrigado a documentar quaisquer violações de dados**.
d. O responsável pelo tratamento está ainda obrigado a **dar conhecimento aos titulares dos dados da ocorrência de uma violação de dados, quando a violação de dados for susceptível de implicar um elevado risco para os direitos e liberdades das pessoas singulares**, logo que seja razoavelmente possível – de forma a prestar informações específicas acerca das medidas que devem tomar para se protegerem de tal violação.



3. Subcontratação:

A CNPD esclarece que o recurso à subcontratação não altera o facto de o responsável pelo tratamento deter a responsabilidade global pela protecção dos dados pessoais – actuando os subcontratantes apenas por conta do responsável, e impondo o RGPD que, no que diz respeito ao tratamento de dados pessoais, a actuação dos subcontratantes resulte estritamente do que lhes for prescrito pelo responsável pelo tratamento, mediante as suas instruções. Contudo, caso, no seu entender, alguma instrução violar o RGPD ou outras disposições legais em matéria de protecção de dados, o subcontratante deve informar imediatamente o responsável pelo tratamento de tal facto.

Sendo o tratamento de dados realizado por subcontratantes, deve o responsável pelo tratamento implementar mecanismos de controlo eficazes quanto à actuação dos subcontratantes, assegurando que estes não prejudicam o cumprimento das obrigações que recaem sobre o responsável neste domínio.

Não pode, destarte, o responsável eximir-se de cumprir as suas obrigações legais, eventualmente diferindo para subcontratantes as suas responsabilidades.

É, portanto, neste contexto que a CNPD define algumas orientações para que os responsáveis pelo tratamento e os subcontratantes (com as devidas adaptações) possam, através da adopção de medidas técnicas e organizativas adequadas, garantir a segurança adequada dos dados pessoais, incluindo a protecção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental.