O Tratamento de Dados Pessoais em Portugal

Breve Guia Prático

apdsi
associação para a
promoção e desenvolvimento
da Sociedade da Informação

Edição de 2014

O Tratamento de Dados Pessoais em Portugal

O Grupo de Trabalho Permanente "Segurança na Sociedade da Informação" (o "GSSI") foi constituído com o intuito de permitir à APDSI acompanhar em permanência e emitir, com oportunidade e rigor, comentários e sugestões públicas sobre as principais questões de "Proteção e Segurança da Informação e Privacidade" que se colocam no âmbito da promoção e desenvolvimento da Sociedade da Informação e do Conhecimento, em variados domínios.

No âmbito das linhas de ação a considerar pelo GSSI, ressaltam, entre outros, aspetos económicos, culturais e estratégicos transversais aos mais variados sectores de atividade, bem como a necessidade de contribuir para o reforço do nível de cumprimento das regras aplicáveis no domínio da privacidade e da proteção de dados pessoais.

Neste sentido, o GSSI tem vindo a trabalhar para que as empresas coloquem na sua agenda as questões de privacidade. Este guia procura ser mais um contributo nesse sentido.

VIEIRA DE ALMEIDA & Associados Sociedade de Advogados, R.L.

apdsi associação para a promoção e desenvolvimento da sociedade da informação

Índice

1. Importância das questões de Privacidade e Proteção de Dados Pessoais

O presente guia tem como objetivo disponibilizar algumas informações genéricas sobre as condições a que se encontra sujeito o tratamento de dados pessoais em Portugal.

Algumas empresas não estão ainda conscientes das consequências que o incumprimento da legislação relativa ao tratamento de dados pessoais[1] pode ter na sua atividade e para os seus responsáveis. Tais consequências, embora facilmente evitáveis, são bastante gravosas, podendo fazer incorrer os gestores das organizações em responsabilidade criminal.

O respeito pelas regras de proteção de dados e privacidade não é importante apenas por uma questão de "*compliance*". As bases de dados pessoais e tratamento de dados associado assumem um papel absolutamente fundamental na boa gestão de qualquer empresa e/ou entidade pública, com particular relevância no domínio do relacionamento com os seus clientes/potenciais clientes e, no caso das entidades públicas, com os utentes dos serviços públicos.

A informação veiculada no presente guia não é exaustiva e não pretende espelhar o quadro detalhado de procedimentos a adotar no domínio do tratamento de dados pessoais.

[1] *Em Portugal, o regime jurídico de proteção de dados pessoais encontra-se consagrado, em termos genéricos, na Lei n.º 67/98, de 26 de outubro (Lei de Proteção de Dados Pessoais), que resultou da transposição da Diretiva Comunitária n.º 95/46/CE. Existe também legislação específica para determinadas áreas, como é o caso da lei que regula o tratamento de dados pessoais no contexto das redes e serviços de comunicações eletrónicas acessíveis ao público (Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto).*

VIEIRA DE ALMEIDA & Associados Sociedade de Advogados, R.L.

apdsi associação para a promoção e desenvolvimento da sociedade da informação

2. Regras Gerais do Tratamento de Dados Pessoais

a) Qual a entidade competente neste domínio?

A Comissão Nacional de Proteção de Dados ("CNPD") é a autoridade nacional que controla e fiscaliza o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, competindo-lhe em especial autorizar ou registar, consoante os casos, os tratamentos de dados pessoais e emitir pareceres sobre disposições legais ou legislação em preparação com impacto nesta matéria.

Para mais informações sobre a atividade da CNPD e conhecimento das suas decisões/deliberações sugerimos a consulta do site da CNPD em www.cnpd.pt

b) Que entidades estão abrangidas?

Qualquer pessoa, singular ou coletiva que recolha, registe, organize, conserve, adapte, altere, recupere, consulte, transmita ou realize qualquer tipo de operação que envolva dados pessoais. Tal significa que todas as entidades, públicas ou privadas, que tratem dados pessoais estão abrangidas.

Em princípio, apenas estão sujeitas à lei as entidades que residam/tenham o seu estabelecimento no território português. No entanto, esta lei também pode ser aplicável ao tratamento de dados por empresas/pessoas com residência/sede fora deste território em determinadas situações específicas e previstas na lei.

c) Que tipos de dados estão abrangidos?

Todos e quaisquer dados relativos a pessoas singulares identificadas ou identificáveis – como por exemplo o nome, morada, e-mail, idade, estado civil, situação patrimonial – em qualquer tipo de suporte – seja em papel, eletrónico, informático, som e imagem, etc.

As imagens relativas a pessoas, recolhidas através dos sistemas de videovigilância, a gravação de chamadas

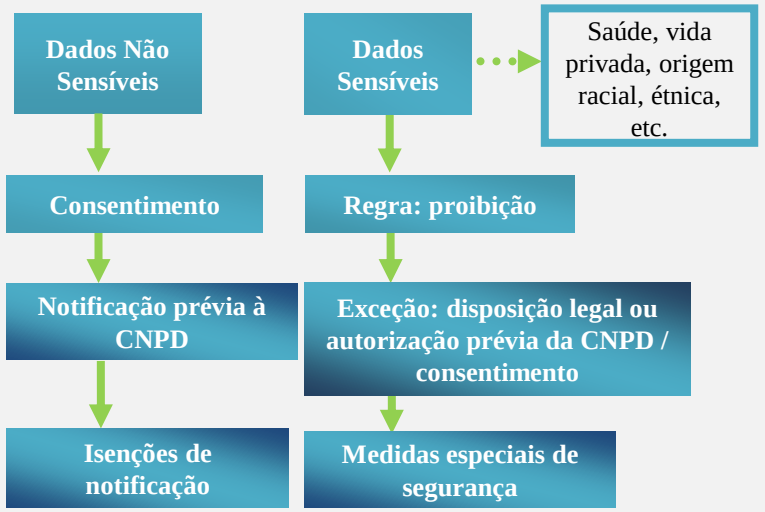
Vieira de Almeida & Associados Sociedade de Advogados, R.L.
apdsi associação para a promoção e desenvolvimento da sociedade da informação

Todas as entidades públicas e privadas que tratem de dados pessoais estão sujeitas ao cumprimento de várias obrigações em matéria de privacidade

telefónicas, os endereços de IP, os dados de tráfego e dados de localização recolhidos no âmbito das comunicações eletrónicas e ainda a informação relativa à localização de determinadas pessoas (por exemplo através de sistemas de geolocalização) também constituem dados pessoais.

Os dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como os dados relativos à saúde e à vida sexual, incluindo os dados genéticos, são considerados "dados sensíveis" e o seu tratamento é apenas autorizado em casos excecionais.

d) O que fazer antes de dar início ao tratamento de dados?



Previamente ao início de qualquer tratamento de dados, a empresa deve obter o consentimento do titular dos dados (i.e. da pessoa a quem os dados dizem respeito), exceto nos casos em que tal consentimento é dispensado nos termos da lei.

A empresa deve ainda, enquanto responsável pelo tratamento, proceder à notificação do tratamento de dados à CNPD. Tal notificação pode consistir num mero registo (caso em que a empresa pode iniciar imediatamente o tratamento de dados) ou num

pedido de autorização (caso em que a empresa deverá aguardar pela emissão da respetiva autorização para dar início ao tratamento).

O que determina se a notificação assumirá a forma de uma mera notificação ou de um pedido de autorização serão os tipos de dados tratados e os tipos de operações que se pretendem efetuar com os dados pessoais recolhidos. Por exemplo, os tratamentos de dados sensíveis estão sujeitos a autorização prévia da CNPD, pelo que a empresa deve não só notificar a CNPD como aguardar pela autorização da mesma antes de dar início ao tratamento.

Por Deliberação da CNPD, algumas operações de tratamento de dados estão isentas de notificação prévia.

e) Quais as obrigações em matéria de proteção de dados pessoais?

A empresa ou organização que individualmente ou em conjunto com outra determine as finalidades e os meios dos tratamentos dos dados é o "responsável pelo tratamento" e deve, nessa medida, entre outros aspetos, assegurar que:

- Os dados pessoais são recolhidos para finalidades determinadas, explícitas e legítimas e não sejam posteriormente tratados de forma incompatível com as finalidades da recolha;
- Apenas são recolhidos os dados pessoais adequados, pertinentes e não excessivos relativamente às finalidades da recolha;
- Os dados pessoais recolhidos são exatos e atualizados;
- Os dados pessoais apenas são conservados durante o período necessário para a prossecução das finalidades da recolha/tratamento (garantindo o cumprimento das Deliberações da CNPD aplicáveis e da legislação específica aplicável a determinados sectores de atividade);

Os dados devem ser tratados para as finalidades para que foram recolhidas e conservadas apenas durante o período necessário à prossecução das mesmas

O incumprimento da lei pode acarretar responsabilidade e ter um impacto negativo na imagem das empresas e organizações

- São postas em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais;
- São disponibilizadas ao titular dos dados todas as informações relacionadas com o tratamento efetuado, concedendo-lhe o direito de acesso, retificação e eliminação dos seus dados, bem como a oposição ao seu tratamento, nos termos da lei;
- É obtido o consentimento do titular para o tratamento dos dados, nos casos em que tal é exigível;
- O tratamento dos dados se encontra devidamente notificado à CNPD e, quando legalmente exigido, é obtida a respetiva autorização prévia.

f) Consequências do incumprimento

O desrespeito por algumas das regras constantes da lei pode acarretar responsabilidade civil, criminal ou contraordenacional, existindo ainda a possibilidade de aplicação, pela CNPD, de sanções acessórias, como a proibição, temporária ou definitiva, do tratamento de dados pessoais, ou a publicidade da sentença condenatória.

O incumprimento da lei tem ainda outros custos associados que podem ter um impacto negativo, muito significativo para a empresa/organização: os custos de imagem e de reputação.

3. Implementação de Medidas de Segurança

a) Quais as obrigações em matéria de segurança?

O responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra:

- a destruição, acidental ou ilícita;
- a perda acidental;
- a alteração;
- a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede; e
- qualquer outra forma de tratamento ilícito.

Sempre que esteja em causa o tratamento de dados sensíveis devem ainda ser adotadas medidas especiais de segurança com vista ao controlo de entradas nas instalações, do acesso aos dados e suportes de dados, ao controlo da utilização dos sistemas de tratamento automatizados por pessoas não autorizadas ou ao controlo da transmissão dos dados.

As medidas de segurança deverão garantir, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado aos riscos que o tratamento apresenta e à natureza dos dados a proteger.

b) Quais os passos a adotar para assegurar o seu cumprimento?

Para a adoção das adequadas medidas de segurança, será necessária a identificação das principais potenciais vulnerabilidades do sistema, bem como uma previsão do impacto que essas falhas de segurança possam causar, de modo a proceder a uma análise e avaliação de risco corretas e realistas que conduzam a uma eficaz definição das medidas de segurança que melhor poderão dar resposta às necessidades da empresa.

Vieira de Almeida & Associados Sociedade de Advogados, R.L.
apdsi associação para a promoção e desenvolvimento da sociedade da informação

O responsável pelo tratamento deve adotar medidas de segurança adequados para proteger os dados pessoais tratados

As falhas de segurança podem verificar-se com maior probabilidade em dois momentos: na comunicação de dados e no recurso à subcontratação.

A comunicação de dados é a operação que se traduz na transmissão de dados pessoais a um terceiro, que pode ser qualquer pessoa singular ou coletiva, autoridade pública, serviço ou qualquer outro organismo que, não sendo o titular de dados, o responsável pelo tratamento, o subcontratado ou outra pessoa sob autoridade direta do responsável pelo tratamento ou do subcontratado, esteja habilitado a tratar os dados.

As empresas deverão adotar particulares cuidados nesta operação, tendo em atenção se os dados foram recolhidos efetivamente com o propósito de serem posteriormente comunicados a terceiros e se para tal foi obtido o consentimento do seu titular.

A comunicação de dados deverá apenas ser possível quando:

- O titular dos dados consentiu na comunicação dos mesmos, aquando da sua recolha;
- A comunicação se processa de acordo com os legítimos interesses da empresa ou do terceiro, não causando prejuízos aos direitos do seu titular;
- A comunicação decorre de uma obrigação legal ou estatutária;
- A comunicação constitui exigência de execução de um contrato;
- A comunicação é necessária para proteger os interesses vitais do titular dos dados.

Tendo em conta o frequente recurso à subcontratação por parte das empresas, torna-se essencial identificar os riscos que esta acarreta para a proteção de dados. Na maior parte dos casos, o outsourcing permite o acesso a dados relativos aos trabalhadores e aos clientes da empresa, pelo que há a possibilidade de ocorrência de falhas de segurança no decurso destas operações.

Assim, quando o responsável pretenda recorrer aos serviços de subcontratados, deverá assegurar-se, em primeiro lugar, que o subcontratado oferece as garantias suficientes em relação ao tratamento a realizar, devendo este último comprometer-se a zelar pelo cumprimento dessas mesmas medidas. Para esse efeito, deverá ser celebrado, nos termos da lei, um contrato escrito entre o responsável pelo tratamento e o subcontratado, o qual poderá consistir num acordo de subcontratação autónomo ou na inclusão de cláusulas especificamente dirigidas à proteção de dados no contrato de prestação de serviços, onde o subcontratado se obrigue a tratar os dados de acordo com as instruções do responsável pelo tratamento e a adotar as medidas de segurança técnicas e organizativas adequadas.

É importante definir uma estratégia de *compliance* como forma de prevenir violações de dados pessoais

VIEIRA DE ALMEIDA & Associados Sociedade de Advogados, R.L.

apdsi associação para a promoção e desenvolvimento da sociedade da informação

4. O futuro Regulamento Europeu

O novo Regulamento Geral sobre a Proteção de Dados (que após aprovação terá aplicação direta a todas as entidades públicas e privadas que tratem dados pessoais), não alterará significativamente as obrigações descritas neste guia. Vem definir, no entanto, novas obrigações e alguns aspetos que modificam e vão seguramente alterar a forma como as empresas tratam as matérias de proteção de dados e privacidade.

Em termos gerais, destacamos algumas das alterações mais significativas:

- ***Data Breaches***: em caso de ocorrência de violações de dados pessoais (ex.: acesso indevido ou perda de dados), as entidades passarão a ter de notificar imediatamente a autoridade nacional de proteção de dados e, em alguns casos, também os titulares dos dados (i.e. as pessoas afetadas);
- ***Data Privacy Officer***: na maioria dos casos, passará a ser obrigatória a existência de um *Data Privacy Officer* independente (desde logo, em empresas com mais de 250 trabalhadores ou em empresas dedicadas ao tratamento de dados pessoais);
- **Sanções**: o Regulamento prevê novas sanções para as violações de dados pessoais e o agravamento do valor das coimas existentes, que podem ascender a 5% do volume anual global de negócios das empresas;
- **Responsabilidade das entidades subcontratadas**: as entidades subcontratadas passarão a poder ser diretamente responsabilizadas em caso de incumprimento das instruções do responsável pelo tratamento.

Apesar do conteúdo do Regulamento ainda estar em discussão no seio da União Europeia, é essencial que as empresas e organizações coloquem a privacidade e proteção de dados pessoais na sua agenda. Este é seguramente um investimento que compensará.

VIEIRA DE ALMEIDA & Associados Sociedade de Advogados, R.L.
apdsi associação para a promoção e desenvolvimento da sociedade da informação

5. Boas Práticas

As empresas e entidades públicas podem facilmente reduzir o risco de incumprimento da lei em matéria de proteção de dados pessoais através da implementação de um programa de "*compliance*" adequado, que lhes permita identificar quais as operações de tratamento de dados normalmente efetuadas no seio da empresa e instituir mecanismos de controlo do cumprimento da lei.

Uma vez que cada entidade tem necessidades próprias, decorrentes das suas características, estrutura e mercado em que atua, o programa de "*compliance*" deverá ser "desenhado" à sua medida.

Em todo o caso, uma das principais medidas destinadas a reduzir o risco de incumprimento da lei será a nomeação de um responsável da empresa pelas matérias de privacidade (um "*Data Privacy Officer*"). Uma outra medida igualmente importante será a de alertar os responsáveis de cada departamento para as questões relacionadas com a privacidade e a aposta na formação dos trabalhadores. Numa organização em que existe consciência das questões de privacidade, os riscos de incumprimento da lei são significativamente menores. Por outro lado, e perante os reais riscos de perda e divulgação indevida de dados pessoais, é essencial que as empresas adotem políticas de gestão de "*data breaches*", que contenham medidas claras de prevenção e reação perante a ocorrência destas situações.

As empresas que pretendam instituir boas práticas em matéria de privacidade devem ainda dispor de uma política interna de tratamento de dados pessoais, acompanhada por uma avaliação regular que lhes permita assegurar uma planificação das necessidades de tratamento de dados pessoais da empresa.

O controlo regular do cumprimento das regras da legislação em matéria de privacidade e dados pessoais é imprescindível para avaliar se, em cada momento, estão a ser respeitadas as finalidades determinantes da recolha, os prazos de conservação dos dados e todas as demais obrigações a que as entidades se encontram sujeitas neste domínio.

VIEIRA DE ALMEIDA & Associados Sociedade de Advogados, R.L.
apdsi associação para a promoção e desenvolvimento da sociedade da informação

6. Avaliação do cumprimento da Lei de Proteção de Dados Pessoais

Para que as entidades possam verificar o seu nível de cumprimento das regras de proteção de dados pessoais, poderá ser utilizada uma breve checklist, tendo como exemplo a que se segue:

- ❑ Existem bases de dados pessoais (de clientes, fornecedores, colaboradores ou outros) e/ou câmaras de videovigilância na sua entidade?
- ❑ Os instrumentos de recolha dos dados, designadamente os contratos, contêm informações detalhadas sobre a finalidade da recolha e outras informações relevantes?
- ❑ Foi obtido o consentimento dos titulares dos dados?
- ❑ O tratamento de dados foi notificado/autorizado pela CNPD?
- ❑ Os dados recolhidos são essenciais para a finalidade do tratamento?
- ❑ Existe um responsável pelas bases de dados pessoais na sua entidade?
- ❑ A sua entidade obteve a autorização da CNPD para a instalação das câmaras de videovigilância e tem afixados avisos que alertem para a existência das mesmas, nos termos previstos na lei?
- ❑ A sua entidade instituiu mecanismos para garantir a segurança e confidencialidade dos dados que tem em seu poder?
- ❑ Antes de comunicar dados pessoais a terceiros, a sua entidade certifica-se que tem autorização/legitimidade para o efeito?
- ❑ A sua entidade celebra contratos escritos com empresas subcontratadas para o tratamento de dados pessoais?

Vieira de Almeida & Associados Sociedade de Advogados, R.L.
apdsi associação para a promoção e desenvolvimento da sociedade da informação

- ❑ Antes de proceder à transferência de dados para países fora da União Europeia/Espaço Económico Europeu a sua entidade confirma que está legalmente autorizada a fazê-lo?
- ❑ Os colaboradores da sua entidade que têm acesso aos dados pessoais estão informados sobre as obrigações que impendem sobre eles e sobre a entidade?
- ❑ Se a sua entidade pretender cruzar dados de uma base de dados com os de outra certifica-se que tal é possível?
- ❑ A sua entidade recolhe dados on-line?
- ❑ Se a sua entidade recolhe dados on-line, disponibiliza no seu site informação sobre o tratamento de dados pessoais que efetua através do mesmo?
- ❑ A sua entidade avalia regularmente o cumprimento da Lei de Proteção de Dados Pessoais?

Patrocinador do GSSI

ANACOM
AUTORIDADE NACIONAL DE COMUNICAÇÕES

Patrocinadores Globais

accenture
High performance. Delivered.

FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

NOS

ORACLE

BancoBIC

everis

Quidgest

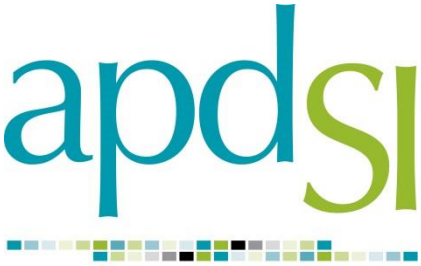
UNISYS

Patrocinadores da APDSI

O Tratamento de Dados Pessoais em Portugal

VIEIRA DE ALMEIDA & Associados Sociedade de Advogados, R.L.

apdsi
associação para a promoção e desenvolvimento da sociedade da informação



APDSI - Associação para a Promoção e Desenvolvimento da Sociedade da Informação

www.apdsi.pt

Rua Alexandre Cabral, n.º 2C - Loja A
1600-803 – Lisboa
Portugal
Tel.: (+351) 21 751 0762
Fax: (+351) 21 757 0516
E-mail: **secretariado@apdsi.pt**

A elaboração deste guia teve a colaboração da

Vieira de Almeida & Associados, Sociedade de Advogados RL

www.vda.pt

LISBOA
Av. Duarte Pacheco, 26
1070-110 – Lisboa
Portugal
Tel.: (+351) 21 311 3400
Fax: (+351) 21 311 3406
E-mail: **lisboa@vda.pt**

PORTO
Av. da Boavista 3433 – 8º piso
4100-138 Porto
Portugal
Tel.: (+351) 22 616 5400
Fax: (+351) 22 610 7951
E-mail: **porto@vda.pt**

TIMOR-LESTE
Timor Plaza
Rua Presidente Nicolau Lobato, Uni. 433
Comoro, Dili –Timor-Leste
Tel: (+670) 3311418
Fax: (+670) 3311317
E-mail: **timorleste@vda.pt**