Lei de Execução Nacional do Regulamento Geral de Protecção de Dados (RGPD) – Lei nº 58/2019 de 8 de Agosto –

— Informação dos Serviços Jurídicos da AGEFE —

Foi publicada no Diário da República nº 151, 1ª Série, de 8 de Agosto, a **Lei nº 58/2019 de 8 de Agosto**, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) nº 2016/679 do Parlamento e do Conselho, de 27 de Abril de 2016 (doravante designado abreviadamente por "*Regulamento Geral de Proteção de Dados" - "RGPD")*, relativo à **proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**.

A lei de execução nacional do RGPD entrou em vigor no dia **9 de Agosto de 2019**.

Este diploma legal vem regular as seguintes matérias:

- As atribuições e competências da Comissão Nacional de Proteção de Dado (doravante referida abreviadamente como *"CNPD")* - a Autoridade de Controlo Nacional;
- O dever de colaboração com a CNPD;
- O encarregado de proteção de dados;
- A acreditação, certificação e códigos de conduta;
- O consentimento de menores;
- A proteção de dados pessoais de pessoas falecidas;
- A portabilidade e interoperabilidade dos dados;
- Videovigilância;
- O dever de segredo;
- O prazo de conservação de dados pessoais;
- A transferência de dados por entidades públicas assim como o tratamento de dados por entidades públicas para finalidades diferentes;
- A liberdade de expressão e informação;
- A publicação de dados pessoais em jornal oficial;
- O acesso a documentos administrativos;
- A publicação de dados no âmbito da contratação pública;
- O tratamento de dados pessoais no âmbito das relações laborais;
- O tratamento de dados de saúde e dados genéticos;
- Os tratamentos para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos;
- A tutela administrativa e jurisdicional dos direitos dos titulares dos dados;

- As contraordenações e coimas por incumprimento do RGPD e da lei de execução nacional do RGPD;
- Os crimes relacionados com os dados pessoais;
- As situações de tratamento de dados pessoais existentes antes da entrada em vigor da lei de execução nacional do RGPD
- Alteração à Lei nº 43/2004 de 18 de Agosto (Lei de Organização e Funcionamento da Comissão Nacional de Proteção de Dados).

No presente documento iremos dar conta das principais novidades assim como as novas obrigações legais que a lei de execução nacional do RGPD veio trazer.

1. A que tratamento de dados é que a nova lei de execução nacional do RGPD é aplicável?

- Aos tratamentos de dados pessoais realizados no território nacional;
- Aos tratamentos de dados pessoais realizados fora do território nacional, quando:
  - Sejam efetuados no âmbito da atividade de um estabelecimento situado no território nacional;
  - Afetem titulares de dados que se encontrem em território nacional, quando as atividades de tratamento estejam relacionadas com a oferta de bens ou serviços a esses titulares de dados em Portugal ou haja o controlo do seu comportamento, desde que esse comportamento tenha lugar em Portugal;
  - Afetem dados que estejam inscritos nos postos consulares de que sejam titulares portugueses residentes no estrangeiro.

2. Comissão Nacional de Proteção de Dados (CNPD)

A **Comissão Nacional de Proteção de Dados** é a **autoridade de controlo nacional** para efeitos do RGPD e da lei de execução nacional do RGPD, que passa a ter **poderes de autoridade** (de polícia)

Cabe à CNPD **controlar e fiscalizar o cumprimento** do **RGPD** e da **lei de execução nacional do RGPD** assim como das demais **disposições legais e regulamentares** em matéria de **proteção de dados pessoais,** assim como **corrigir e sancionar o seu incumprimento**.

A CNPD disponibiliza uma **lista dos tipos de tratamentos de dados** que se encontram sujeitos à **avaliação do impacto sobre a proteção de dados**. Lista essa que já foi publicada e que consta do Regulamento da CNPD nº 1/2018 publicado no Diário da República nº 231, 2ª série, de 30 de Novembro, que se anexa à presente circular.

Cabe, igualmente, à CNPD elaborar e difundir uma **lista de tipos de tratamento de dados cuja avaliação prévia de impacto sobre a proteção de dados não é obrigatória**. Informa-se que até à presente data ainda não foi publicada a referida lista. Mesmo que um tipo de tratamento de dados se encontra nesta lista, as empresas podem efetuar uma **avaliação prévia de impacto** por sua iniciativa.

As listas acima mencionadas são publicitadas no sítio da internet da CNPD.

As empresas encontram-se sujeitas ao **dever de colaboração com a CNPD.** Nesse sentido, as empresas encontram-se obrigadas a prestar colaboração à CNPD, tendo de facultar todas as informações que a CNPD lhe solicitar.

O **dever de colaboração** é assegurado, designadamente, quando a CNPD tenha necessidade para o exercício cabal das suas funções, de examinar o sistema informático e os ficheiros de dados pessoais bem como toda a documentação relativa ao tratamento e transmissão de dados pessoais.

Os membros da CNPD bem como os seus trabalhadores, prestadores de serviços ou pessoas por si mandatadas estão obrigados ao **sigilo profissional,** que se mantém após o termo das respetivas funções**,** nomeadamente quanto aos dados pessoais, segredo profissional, segredo industrial ou comercial ou informações confidenciais a que tenham acesso no exercício das suas funções.

O dever de colaboração bem como os poderes de fiscalização da CNPD não prejudicam o dever de segredo a que as empresas estejam obrigadas nos termos da lei ou de normas internacionais.

3. Encarregado de Proteção de Dados ("Data Protection Officer" – DPO")

O **Encarregado de Proteção de Dados (DPO) não necessita de certificação profissional** e é designado com base nas suas qualidades profissionais e, em especial, pelos seus conhecimentos do direito e das práticas de proteção de dados.

O **Encarregado de Proteção de Dados** pode ser um elemento do pessoal da empresa (com contrato de trabalho) ou pode exercer as suas funções com base num contrato de prestação de serviços ou em regime de avença.

O **Encarregado de Proteção de Dados** deve exercer a sua função com **autonomia técnica** perante a empresa.

De salientar que o **Encarregado de Proteção de Dados** encontra-se sujeito ao **dever de sigilo profissional** em tudo o que diga respeito ao exercício das suas funções, que se mantém após o termo das suas funções.

Encontram-se obrigados ao **dever de confidencialidade,** que acresce aos deveres de sigilo profissional, em relação aos **dados pessoais** a que tenham acesso:

- O Encarregado de Proteção de Dados;
- Os responsáveis pelo tratamento;
- Os subcontratantes; e
- Todas as pessoas que intervenham em qualquer operação de tratamento.

A lei de execução nacional do RGPD vem esclarecer que, para além das **funções do DPO** previstas nos artigos 37º a 39º do RGPD, que tem igualmente as **seguintes funções**:

- Assegurar a realização de auditorias, quer periódicas, quer não programadas;
- Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança;
- Assegurar as relações com os titulares dos dados nas matérias abrangidas pelo RGPD e pela legislação nacional em matéria de proteção de dados.

A lei de execução prevê duas situações em que é **obrigatório** o responsável pelo tratamento e o subcontratante designarem um **Encarregado de Proteção de Dados**, quando a **atividade desenvolvida, a título principal,** implicar:

- 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;**

- Operações de **tratamento em grande escala** das **categorias especiais de dados** (dados sensíveis previstos no artigo 9º do RGPD) ou de **dados pessoais relacionados com condenações penais e contraordenacionais** (nos termos do artigo 10º do RGPD).

4. Acreditação e Certificação em matéria de Proteção de Dados

A autoridade competente para a acreditação dos organismos de certificação em matéria de dados é o **IPAC, I.P.**

5. Consentimento de Menores

Os **dados pessoais de crianças só** podem ser objeto de tratamento com base no **consentimento** e relativo à oferta direta de serviços da sociedade de informação. As crianças que tenham **completado 13 anos de idade** podem elas próprias dar o seu consentimento.

Se a criança tiver **idade inferior a 13 anos**, para que o tratamento seja lícito é necessário que o **consentimento** seja dado pelos **representantes legais** desta, de preferência com recurso a **meios de autenticação segura**.

6. Proteção de Dados Pessoais de Pessoas Falecidas

Os dados sensíveis (nos termos do artigo 9º nº 1 do RGPD) e os dados que se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações de pessoas falecidas são protegidos nos termos do RGPD e da lei nacional de execução do RGPD.

O que significa que os restantes dados pessoais de pessoas falecidas não são protegidos pelo RGPD ou pela lei nacional de execução do RGPD.

Em relação aos dados pessoais de pessoas falecidas protegidos nos termos do RGPD e da lei nacional de execução do RGPD, os **direitos de acesso, retificação e apagamento** são exercidos por quem a pessoa falecida tenha designado para o efeito ou, na sua falta, pelos respetivos herdeiros. A pessoa falecida, titular dos dados, pode deixar determinada a impossibilidade de exercício dos referidos direitos **após a sua morte**.

7. Portabilidade e Interoperabilidade dos Dados

Cumpre realçar que o direito à portabilidade dos dados **apenas abrange os dados fornecidos pelos respetivos titulares dos dados**.

A portabilidade dos dados deve, sempre que possível, ter lugar em **formato aberto**.

8. Videovigilância

As câmaras de videovigilância não podem incidir sobre:

- Vias públicas, propriedades limítrofes ou outros locais que não sejam do domínio exclusivo do responsável pelo tratamento, exceto no que seja estritamente necessário para cobrir os acessos ao imóvel;
- A zona de digitação de códigos de caixas multibanco ou outros terminais de pagamento ATM;
- O interior de áreas reservadas a clientes ou utentes onde deva ser respeitada a privacidade, designadamente instalações sanitárias, zonas de espera e provadores de vestuário;
- O interior de áreas reservadas aos trabalhadores, designadamente zonas de refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetas ao seu descanso.

É proibida a **captação de som**, **exceto** no período em que as instalações vigiadas estejam encerradas ou mediante autorização prévia da CNPD.

De sublinhar que caso se pretenda **captar som** através do sistema de videovigilância quando as **instalações estejam abertas**, é necessário pedir **autorização prévia à CNPD**.

Com o RGPD, já não é necessário pedir autorização à CNPD para utilizar sistemas de videovigilância nas instalações da empresa cuja finalidade seja a proteção de pessoas e bens, exceto quando haja a captação de som quando as instalações estejam abertas.

A empresa terá que cumprir a legislação laboral em vigor (artigos 20º e 21º do Código do Trabalho), o RGPD e a lei de execução nacional do RGPD nesta matéria.

9. Direitos de Informação e de Acesso aos Dados Pessoais pelo Titular dos Dados e o Dever de Segredo

Os direitos de informação e de acesso aos dados pessoais pelo titular dos dados não podem ser exercidos quando por lei a empresa esteja sujeita ao dever de segredo que seja oponível ao próprio titular dos dados.

No entanto, prevê-se que o titular dos dados possa solicitar à **CNPD** a emissão de parecer quanto à oponibilidade do dever de segredo.

10. Prazo de Conservação de Dados Pessoais

O prazo de conservação de dados pessoais é o que estiver **fixado por lei ou regulamento**, ou na falta desta, o que se **revele necessário para a prossecução da finalidade**.

Quando pela natureza e finalidade do tratamento não seja possível determinar antecipadamente o momento em que o tratamento deixa de ser necessário, designadamente, tratamentos para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos, é lícita a conservação dos dados pessoais, desde que sejam adotadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados, designadamente, a **informação da sua conservação**.

Esta norma é importante para as situações em que não é possível de todo prever durante quanto tempo é que a empresa irá necessitar dos dados pessoais e não existe um prazo legal definido de conservação dos dados, abrindo a porta para que se possa utilizar uma cláusula aberta em relação aos prazos legais de conservação dos dados como: *"Os seus dados pessoais serão conservados durante o período de tempo em que necessitamos dos seus dados para a finalidade de ___".*

Quando os dados pessoais sejam necessários para comprovar o **cumprimento de obrigações contratuais** ou de outra natureza, os dados podem ser conservados durante todo o período de tempo enquanto estiver a decorrer o prazo de prescrição dos direitos correspetivos.

Quando a finalidade que motivou o tratamento de dados pessoais cessar, o responsável pelo tratamento deve proceder à destruição ou anonimização dos dados pessoais.

Nos casos em que existe um prazo de conservação de dados imposto por lei, o exercício do direito ao apagamento dos dados pelo titular só pode ser exercido **findo esse prazo**.

Existe uma novidade na lei de execução nacional do RGPD que se prende com os dados relativos às declarações contributivas para efeitos de aposentação ou reforma, que podem ser **conservados sem limite de prazo**, para auxiliar o titular na reconstituição das carreiras contributivas, desde que sejam adotadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados.

11. Relações Laborais

A lei de execução nacional do RGPD vem confirmar que o empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais.

Esclarece-se que é permitido o tratamento de dados efetuado por **subcontratante ou contabilista certificado** em nome do empregador para fins de gestão das relações laborais, desde que ao abrigo de um contrato de prestação de serviços escrito e que sejam asseguradas garantias de sigilo.

Cumpre salientar que não é necessário o consentimento do trabalhador para que a entidade empregadora legitimamente trate os seus dados pessoais nas seguintes situações:

- Se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador; ou
- Se o tratamento for necessário para a execução de um contrato ou para diligências pré-contratuais, a pedido do titular dos dados, de acordo com o artigo 6º nº 1 al. b) do RGPD.

As imagens gravadas e os outros dados pessoais registados através de sistemas de videovigilância ou de outros meios tecnológicos de vigilância à distância (por exemplo, "*car tracking*" ou dispositivos em computador contra roubo), **só** podem ser utilizados no **âmbito do processo penal** bem como para efeitos de **apuramento de responsabilidade disciplinar**, na medida em que o sejam no âmbito do processo penal (ou seja, quando esteja em causa crimes).

De referir que **só** é considerado legitimo o tratamento de dados biométricos de trabalhadores para **controlo de assiduidade** e para **controlo de acessos às instalações do empregador**, não podendo ser utilizados para nenhum outro fim. A entidade empregadora deve assegurar-se que apenas são utilizadas **representações dos dados biométricos** e que o respetivo processo de recolha não permita a reversibilidade dos referidos dados.

12. Tratamento de Dados de Saúde

Cumpre sublinhar que apenas deve ter acesso a dados de saúde e dados genéticos quem necessite de conhecer a informação.

Para efeitos de **medicina no trabalho e/ou a avaliação de capacidade de trabalho do colaborador**, o tratamento dos dados de saúde e genéticos, que são dados sensíveis, deve ser efetuado por um **profissional obrigado a sigilo** ou outra **pessoa sujeita a dever de confidencialidade** e devem ser garantidas as medidas adequadas de segurança da informação.

O acesso aos dados de saúde para efeitos de medicina do trabalho ou para avaliação da capacidade de trabalho do colaborador (i.e., a **ficha de aptidão** do colaborador) é feito **exclusivamente** de forma eletrónica, a menos que seja impossível tecnicamente ou por indicação expressa em contrário do titular dos dados, e é proibida a sua divulgação ou transmissão posterior. O que significa que as fichas de aptidão não podem ser posteriormente divulgadas ou transmitidas pela entidade empregadora a outrem, a menos que o colaborador tenha dado o seu consentimento explícito por escrito para transmitir a sua ficha de aptidão a determinado destinatário.

13. Tratamentos para Fins de Arquivo de Interesse Público, Fins de Investigação Científica ou Histórica ou Fins Estatísticos

O tratamento para **fins de interesse público**, **fins de investigação científica ou histórica** ou **fins estatísticos** deve respeitar o princípio da minimização dos dados (apenas devem ser tratados os dados de que se necessita) e os dados devem ser anonimizados ou deve haver a pseudonimização dos dados, sempre que os fins visados possam ser atingidos por uma destas vias.

Nas situações em que os dados pessoais são tratados para os fins acima mencionados, os direitos de acesso, retificação, limitação do tratamento e de oposição ficam prejudicados, na medida do necessário, se esses direitos forem suscetíveis de tornar impossível ou prejudicar gravemente a realização desses fins.

De salientar que os dados pessoais que são tratados para fins estatísticos devem ser **anonimizados** ou **pseudonimizados,** por forma a acautelar a tutela dos titulares dos dados, no sentido de ser impossível reidentificar o titular após a conclusão da operação estatística. Pelo que, caso uma empresa realize estatísticas deve haver o cuidado para tornar os dados pessoais anonimizados ou pseudonimizados e que os titulares dos dados não possam voltar a ser identificados.

14. Como é que os Titulares dos Dados podem reagir perante uma violação ou incumprimento do RGPD ou da Lei de Execução Nacional do RGPD?

- Apresentar queixa à CNPD;
- Recorrer aos meios de tutela administrativo de cariz de petitório ou impugnatório;
- Se tiver sofrido um dano devido ao tratamento ilícito de dados ou a qualquer outro ato que viole as disposições do RGPD ou da lei nacional de execução do RGPD, tem direito de obter a reparação do dano sofrido (pedir uma indemnização). O responsável pelo tratamento e o subcontratante não incorrem em responsabilidade civil se provarem que o facto que causou o dano não lhes é imputável.
- Propor ações contra as decisões da CNPD, nomeadamente de natureza contraordenacional, e contra as omissões da CNPD bem como ações de responsabilidade civil (pedido de indemnização) pelos **danos** que tais atos ou omissões possam ter causado – estas ações são da competência dos **tribunais administrativos**;
- Propor ações contra o responsável pelo tratamento ou o subcontratante. Estas ações são propostas nos **tribunais nacionais** se o responsável pelo tratamento ou o subcontratante tiver estabelecimento em território nacional ou se o titular dos dados aqui residir habitualmente;
- Mandatar um organismo, uma organização ou uma associação de interesse publico, sem fins lucrativos e cuja a atividade abranja a defesa dos direitos, liberdades e garantias dos titulares dos dados quanto à proteção de dados pessoais, para exercer os direitos acima elencados.

15. CONTRAORDENAÇÕES

A lei de execução nacional do RGPD qualifica as **violações/incumprimento do RGPD** ou **da lei de execução nacional do RGPD** como constituindo contraordenações muito graves ou graves.

As **contraordenações muito graves** são punidas com as seguintes coimas:

- De € 5.000 a € 20.000.000 ou 4% do volume de negócios anual a nível mundial, conforme o que for mais elevado, tratando-se de **grande empresa** (emprega 250 ou mais trabalhadores);
- De € 2.000 a € 2.000.000 ou 4% do volume de negócios anual a nível mundial, conforme o que for mais elevado, tratando-se de **PME** (de 0 a 249 trabalhadores);
- De € 1.000 a € 500.000, no caso de **pessoas singulares**.

As **contraordenações graves** são punidas com as seguintes coimas:

- De € 2.500 a € 10.000.000 ou 2% do volume de negócios anual a nível mundial, conforme o que for mais elevado, tratando-se de **grande empresa** (emprega 250 ou mais trabalhadores);
- De € 1.000 a € 1.000.000 ou 2% do volume de negócios anual a nível mundial, conforme o que for mais elevado, tratando-se de **PME** (de 0 a 249 trabalhadores);
- De € 500 a € 250.000, no caso de **pessoas singulares.**

Na determinação da medida da pena, entre outros previstos no RGPD, a CNPD tem em conta o volume de negócios e o balanço anual, o carácter continuado da infração bem como a dimensão da entidade, tendo em conta o número de trabalhadores e a natureza dos serviços prestados.

Cumpre salientar que as empresas deverão dar especial atenção e ter especiais cuidados em relação ao incumprimento das normas que é considerado como sendo grave ou muito grave, não só pelo elevado valor das coimas em causa mas também pelas consequências que poderão advir para a empresa do incumprimento dessas disposições legais.

É importante referir que, em caso de **negligência ou mera culpa**, antes de ser instaurado um processo de contraordenação, primeiro a CNPD efetua uma **prévia advertência** ao agente para cumprir a obrigação omitida ou para reintegrar a proibição violada, num **prazo razoável designado** para o efeito. Só se a empresa não cumprir a obrigação omitida ou a reintegração da proibição violada é que a CNPD instaura um processo de contraordenação.

No caso de haver dolo, o processo de contraordenação é logo instaurado, sem haver lugar à prévia advertência da empresa por parte da CNPD.

Elencam-se infra alguns **incumprimentos** que constituem **contraordenações muito graves:**

- ✓ O tratamento de dados pessoais que viole os princípios relativos ao tratamento de dados pessoais previstos no artigo 5º do RGPD, a saber,
  - **Princípio da licitude, lealdade e transparência do tratamento dos dados;**
  - **Princípio da limitação das finalidades de tratamento;**
  - **Princípio da exatidão dos dados;**
  - **Princípio da limitação da conservação dos dados;**
  - **Princípio da integridade e confidencialidade dos dados.**
- ✓ Os tratamentos de dados que não tenham por base o consentimento do titular nem tenham por base outro fundamento jurídico previsto no artigo 6º do RGPD ou na norma nacional;
- ✓ O incumprimento das regras relativas à prestação do consentimento (artigo 7º RGPD);
- ✓ O tratamento de dados sensíveis fora das circunstâncias de legitimidade previstas no nº 2 do artigo 9º do RGPD;
- ✓ A exigência do pagamento de uma quantia em dinheiro, fora das circunstâncias em que é admitido, nomeadamente, em relação a pedidos para o exercício dos direitos dos titulares quando estes sejam manifestamente infundados ou excessivos (repetitivos);
- ✓ A exigência do pagamento de uma quantia em dinheiro, quando é admissível (pedidos dos titulares que sejam manifestamente infundados ou excessivos), que exceda os custos necessários para satisfazer o direito do titular dos dados;
- ✓ Quando não se presta a seguinte informação aos titulares dos dados, aquando da recolha dos dados pessoais:
  - Omissão de informação das finalidades a que se destina o tratamento;
  - Omissão de informação acerca dos destinatários ou categorias de destinatários dos dados pessoais;
  - Omissão de informação acerca do direito do titular dos dados de retirar o consentimento em qualquer altura.
- ✓ Não permitir, não assegurar ou dificultar o exercício dos direitos pelo titular dos dados;
- ✓ A transferência internacional de dados pessoais sem respeitar as condições estabelecidas no RGPD para essas transferências;
- ✓ O incumprimento das decisões da CNPD ou a recusa da colaboração que tenha sido exigida pela CNPD.
- ✓ A violação das regras na lei de execução nacional do RGPD relativas ao tratamento de dados pessoais nas relações laborais, ao tratamento de dados de saúde e dados genéticos, tratamentos para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos.

Cumpre referir alguns **incumprimentos** que constituem **contraordenações graves:**

- ✓ A violação das condições aplicáveis ao consentimento de crianças;
- ✓ A não prestação da restante informação que se encontra prevista no artigo 13º do RGPD aos titulares dos dados aquando da recolha dos seus dados pessoais;

- ✓ A violação da proteção de dados desde a conceção e por defeito assim como a não aplicação de medidas técnicas e organizativas que sejam adequadas para assegurar e comprovar que o tratamento é realizado em conformidade com o RGPD;
- ✓ A violação das regras relativamente aos responsáveis conjuntos pelo tratamento;
- ✓ A violação das obrigações relativas ao subcontratante, nomeadamente: apenas recorrer a subcontratantes que apresentem garantias de execução de medidas técnicas e organizativas para que o tratamento satisfaça os requisitos do RGPD; haja autorização geral ou específica para a sub-subcontratação; sejam celebrados contratos ou acordos escritos com todos os subcontratantes e que contenham as cláusulas obrigatórias nos termos do artigo 28º do RGPD;
- ✓ A violação da regra de apenas tratar os dados pessoais por instrução do responsável pelo tratamento;
- ✓ A falta do registo das atividades de tratamento de dados pessoais, quando for obrigatório;
- ✓ A violação das regras de segurança no tratamento dos dados pessoais;
- ✓ O incumprimento do dever de notificar a violação de dados pessoais à CNPD;
- ✓ O incumprimento do dever de informar o titular dos dados de uma violação de dados quando esta for suscetível de implicar um elevado risco para a privacidade do titular dos dados;
- ✓ O incumprimento da realização de avaliações de impacto sobre a proteção de dados nas situações em que é obrigatório;
- ✓ O incumprimento da obrigação de consultar a CNPD previamente à realização de operações de tratamento de dados quando a avaliação de impacto indicar que o tratamento resultaria num elevado risco, na ausência das medidas tomadas para atenuar o risco;
- ✓ O incumprimento do dever de designar um encarregado de proteção de dados, quando for obrigatório;
- ✓ A violação da garantia de independência do encarregado de proteção de dados;
- ✓ A utilização de selos ou marcas de proteção de dados que não tenham sido emitidos por organismos de certificação devidamente acreditados;
- ✓ A violação das regras relativas à videovigilância que constam da lei de execução nacional do RGPD.

16. Crimes relacionados com a Violação de Dados Pessoais:

Cumpre salientar que tanto as pessoas coletivas como as pessoas singulares são responsáveis pelos crimes infra elencados.

- ➢ **Crime de utilização de dados de forma incompatível com a finalidade de recolha:** constitui crime a utilização de dados pessoais de forma incompatível com a finalidade que determinou a recolha dos dados.
- ➢ **Crime de acesso indevido a dados pessoais:** Constitui crime o acesso por qualquer modo, sem a devida autorização ou justificação, a dados pessoais.

- **Crime de desvio de dados:** Constitui crime copiar, subtrair, ceder ou transferir, a título oneroso ou gratuito, dados pessoais sem previsão legal ou consentimento.
- **Crime de viciação ou destruição de dados:** Constitui crime apagar, destruir, danificar, ocultar, suprimir ou modificar dados pessoais sem a devida autorização ou justificação, tornando-os inutilizáveis ou afetando o seu potencial de utilização.
- **Crime de inserção de dados falsos:** Constitui crime inserir ou facilitar a inserção de dados pessoais falsos, com a intenção de obter vantagem indevida para si ou para terceiro, ou para causar prejuízo.
- **Crime de violação do dever de sigilo:** Constitui crime quem, obrigado a sigilo profissional, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou em parte dados pessoais.
- **Crime de desobediência:** Constitui crime o não cumprimento das obrigações previstas no RGPD e na lei de execução nacional do RGPD, depois de ultrapassado o prazo que tiver sido fixado pela CNPD para o respetivo cumprimento.

17. Sanções acessórias

Conjuntamente com as sanções aplicadas pode, acessoriamente, ser ordenada a proibição temporária ou definitiva do tratamento, o bloqueio, o apagamento ou a destruição total ou parcial dos dados.

No caso de **crimes** ou de **coimas de montante superior a € 100.000**, pode ser determinada a publicidade da condenação no Portal do Cidadão por período não inferior a 90 dias, com a identificação do agente, os elementos da infração e as sanções aplicadas.

18. Tratamentos de dados pessoais realizados com base em autorizações emitidas pela CNPD com base na lei anterior de proteção de dados pessoais

Os responsáveis pelo tratamento e os subcontratantes que realizam tratamentos de dados pessoais com base em autorizações emitidas pela CNPD ao abrigo da lei anterior de proteção de dados pessoais (Lei nº 67/98 de 26 de Outubro) encontram-se obrigados a cumprir as obrigações impostas pelo RGPD, no entanto, não é necessário realizar a avaliação de impacto sobre a proteção de dados.

19. Renovação do consentimento

Quando o tratamento dos dados pessoais em curso na data da entrada em vigor da lei de execução nacional do RGPD se basear no consentimento do respetivo titular, não é necessário obter novo consentimento do titular se o anterior tiver cumprido os requisitos previstos no RGPD.

20. **Normas relativas à proteção de dados pessoais**

De salientar que as normas relativas à proteção de dados pessoais previstas em legislação especial (por exemplo no Código do Trabalho) mantêm-se em vigor, quando não contrariem o RGPD e a lei de execução nacional do RGPD.

As normas legais que prevejam autorizações ou notificações de tratamento de dados pessoais à CNPD (por exemplo, no Código do Trabalho para o tratamento de dados biométricos do trabalhador, para a utilização pelo empregador de meios de vigilância à distância no local de trabalho), deixaram de vigorar à data da entrada em vigor do RGPD (em 25 de Maio de 2018).

O que significa que a partir dessa data e para o futuro, as empresas que pretenderem tratar dados biométricos dos seus colaboradores ou utilizar meios de vigilância à distância no local de trabalho (ex: sistema de "car tracking" nos veículos ou videovigilância) **não** têm de notificar ou pedir autorização à CNPD, apenas estão obrigadas a realizar uma **Avaliação do Impacto sobre a Proteção de Dados** dos referidos sistemas que pretendem implementar na empresa**.**

Anexa-se a Lei nº 58/2019 de 8 de Agosto bem como o Regulamento da CNPD nº 1/2018 publicado no Diário da República nº 231, 2ª série, em 2018-11-30, documentos de que se recomenda a leitura.

Com os melhores cumprimentos.

José Valverde

Director Executivo