O Regulamento Geral de Proteção de Dados Pessoais
O que há de novo?

Time to say goodbye…

to the Data Protection Directive!

6

Graça Canto Moniz

NOVA Direito/CEDIS

03/03/2018

Evolução legislativa

Hoje

Diretiva 95/46/EC – **Lei n.º 67/98**

Maio 2018

Regulamento 2016/679 (Legislação portuguesa ?)

Despacho n.º 7456/2017

- Criação de um Grupo de Trabalho com o objetivo de preparar a legislação portuguesa para a aplicação do Regulamento Geral de Proteção de Dados em Portugal.

Compete ao Grupo de Trabalho:

a) Proceder à realização de uma consulta pública, a decorrer até 30 de setembro de 2017;

b) Identificar as regras de segurança no tratamento de dados pessoais, decorrentes do RGPD, e apresentar as diferentes alternativas sobre a arquitetura institucional necessária à operacionalização do Regulamento;

c) Apresentar uma anteproposta de lei até 31 de dezembro de 2017.

Para esse feito, o Grupo de Trabalho trabalhará com as diferentes áreas de governo e níveis de administração pública cuja participação seja relevante para a redação da legislação acima referida.

O Grupo de Trabalho deve ainda, em articulação com as entidades consideradas adequadas, nomeadamente com a Direção-Geral de Qualificação dos Trabalhadores em Função Pública-INA, estudar as melhores formas de garantir a formação dos quadros da Administração Pública sobre o RGPD.

Reforma da Comissão Europeia de 2012

Agenda Digital para a Europa (crescimento da economia digital até 2020): pressupõe um reforço da confiança do consumidor nas novas formas de transações comerciais e digitais – soberano em relação aos seus dados pessoais. Como?

Capacidade de controlo dos dados pessoais

Reforçar os direitos do titular dos dados pessoais

Reforçar a segurança dos dados: resposta ao “ciber” risco

Atitude responsável e pro ativa das organizações que utilizam dados pessoais

Consequências desta reforma da CE?

Regulamento Geral de Proteção de Dados Pessoais

99 artigos e 173 considerandos; diploma difícil de compreender ... E de implementar

O que continua?

- “Dados pessoais”
- “Tratamento”
- “Consentimento”
- “Responsável pelo tratamento e subcontratante”
- “Autoridade de controlo”
- Outros conceitos....

O que há de novo?

- Dados relativos à saúde
- Pseudonimização e anonimização
- Proteção de dados pessoais desde a conceção e por defeito
- Violação da segurança dos dados pessoais
- Consulta prévia
- Avaliação de impacto
- Registos das atividades de tratamento
- Encarregado de proteção de dados pessoais
- Alguns direitos do titular dos dados

<u>Outras definições relevantes: art. 4.º do RGPD</u>

Categorias especiais de dados

Dados pessoais que revelem a origem racial ou étnicas, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical; dados genéticos, dados biométricos, **dados relativos à saúde**, à vida sexual ou orientação sexual: **art. 9.º**

Definição de dados relativos à **saúde: art. 4.º, n.º 15 "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde , que revelem informações sobre o seu estado de saúde**

Conceito de dados relativos à saúde

- **<u>Importância</u>**: regime das **"categorias de dados pessoais"** – art. 9.º (fundamentos do tratamento mais rigorosos)

- **<u>Obrigações</u>**:

a) Designação de um encarregado de proteção de dados pessoais (art. 37.º, n.º 1, al. c));
b) Realização de avaliações de impacto c/ frequência (art. 35.º, n.º 3, al. b))
c) Registo das atividades (art. 30.º)
d) Consulta prévia (art. 36.º)

Pseudonimização

- Considerando 28 e 29 e art. 4.º, n.º 5 – definição:

É *"o tratamento de dados pessoais de forma que* ***deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares****, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável"*

Portanto... é um processo para **camuflar identidades**

Pseudonimização

Exemplo: “*Graça Moniz, nascida a 3 de abril de 1967, tem quatro filhos: dois rapazes e duas raparigas*”. Pseudonimizado:

“*324 tem quatro filhos: dois rapazes e duas raparigas*” ou

“*MOz345 tem quatro filhos: dois rapazes e duas raparigas”*

Quem aceder aos dados não pode identificar “*Graça Moniz, nascida a 3 de abril de 1967*” a partir de “*324*” ou de “*MOz345*”

Anonimização

- Excluídos do âmbito de aplicação do RGPD. Considerando 26:

"(...) informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais ***tornados*** *de tal modo anónimos que o seu titular não seja ou já não possa ser identificado"*

Anonimização

- Principais **técnicas** de anonimização de dados pessoais: a aleatorização, a generalização, a adição de ruído, a permuta, a privacidade diferencial, a agregação, o k-anonimato, a l-diversidade e a t-proximidade.

- Explicação dos seus princípios, pontos fortes e fracos, bem como os erros mais comuns relacionados com a utilização de cada técnica: G29, *"Parecer 05/2014 sobre técnicas de anonimização"*

Proteção de dados desde a conceção e proteção de dados por defeito

- Quanto maior o risco do tratamento tanto mais o responsável pelo tratamento deve aplicar "tanto no momento de **definição** dos meios de tratamento **como no momento do próprio tratamento**, as medidas técnicas e organizativas adequadas, como a **pseudonimização**, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a **minimização,** e a incluir as **garantias necessárias** no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados" (art. 25.º, n.º 1)
- O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, **por defeito, *só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento***. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibi lidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares (art. 25.º, n.º 2)
- Importância dos **procedimentos de certificação**: art. 25.º, n.º 3

Violação de dados pessoais

- "Uma violação da segurança que provoque, de modo acidental ou ilícito, a **destruição**, a **perda**, a **alteração**, a **divulgação** ou o **acesso**, **não autorizados,** a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (art. 4.º, n.º 12).

- Alguns **<u>exemplos</u>**:

1. Acesso por terceiros não autorizados (ex: intrusões);
2. Envio de dados pessoais para um destinatário errado
3. Computadores/*pens* roubados ou perdidos

- **<u>Documentar/registar</u>** todos os incidentes de violação de dados pessoais (art. 33.º, n.º 5). O que fazer quando ocorrem?

Hipótese 1 – notificar a autoridade de controlo

a) Notificar a **autoridade de controlo** a menos que seja **improvável** que a violação ponha em **risco os direitos e liberdades** das pessoas singulares;

b) Prazo: **72 horas** após ter tomado conhecimento. Se não for transmitida dentro do prazo, a notificação deve ser acompanhada dos motivos do atraso;

c) Conteúdo mínimo: a natureza da violação; o nome e os contactos do encarregado de proteção de dados ou de outro ponto de contacto; as consequências prováveis da violação de dados; descrição das medidas adotados ou propostas para repara a violação e atenuar os eventuais efeitos negativos

Hipótese 2 – notificar o titular dos dados

a) Quando a violação dos dados pessoais for suscetível de **implicar um elevado risco para os direitos e liberdades das pessoas singulares**, o RT comunica a violação de dados pessoais ao titular dos dados sem demora injustificada

b) Prazo: ”sem demora injustificada”

c) Conteúdo: o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações; Descrever as consequências prováveis da violação de dados pessoais; Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos;

- **Nota importante:** art. 70.º, n.º 1, al. g) e h) – Comité Europeu vai emitir orientações

G29, on Personal data breach notification under Guidelines Regulation 2016/679

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendations
i. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	

G29, on Personal data breach notification under Guidelines Regulation 2016/679

iii. A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.

G29, Guidelines on Personal data breach notification under Regulation 2016/679

viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
ix. Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	

Conceito de **Avaliação de impacto** (art. 35.º) e de **consulta prévia** (art. 36.º)

- **Avaliação de Impacto:**

"Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais".

- Fator importante: **"A autoridade de controlo elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados por força do n.º1" (art. 35.º, n.º 4).**

- **Conteúdo** mínimo: 34.º, n.º 7

Avaliação de impacto

- CNIL: “Privacy Impact Assessment (PIA)” - https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf e outras ferramentas no site...

- ICO: “Conducting privacy impact assessments. Code of practice” - https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

- G29, “Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679"

Consulta prévia

- Art. 36.º: O RT consulta a autoridade de controlo antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados nos termos do artigo 35.º indicar que **o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo RT para atenuar o risco**

- **Prazo** de resposta da autoridade de **8 semanas**: deve dar orientações por escrito

- **Elementos** a comunicar: art. 36.º, n.º 3.

Registo das atividades de tratamento – art. 30.º

- Conservar um registo de todas as atividades de tratamento, incluindo nesse registo um elenco de informações como:

a) Finalidades do tratamento
b) Descrição das categorias de titulares de dados e das categorias de dados pessoais
c) Prazos previstos para o apagamento
d) Destinatário
e) (...)

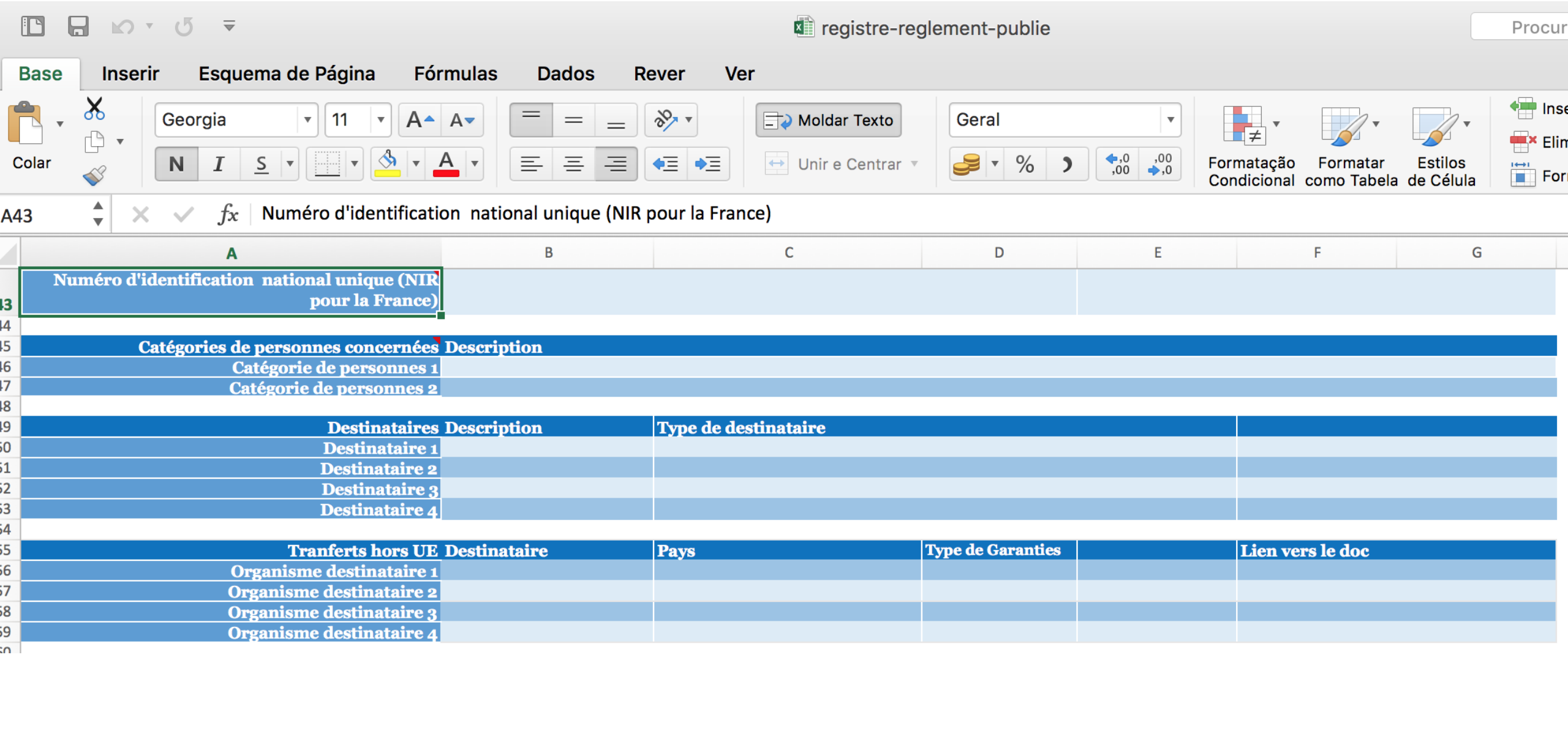
Registo das atividades de tratamento – art. 30.º

- Considerando 82: obrigação de **cooperar** com a autoridade de controlo e **facultar** o registo quando pedido.

- Excluídas organizações com menos de 250 trabalhadores. **Exceto**, "se o tratamento implicar riscos para os direitos fundamentais dos titulares, não seja ocasional e abranja categorias especiais de dados" (art. 30.º, n.º 5)

- É um instrumento que permite ao RT e à autoridade de controlo obter **uma perspetiva geral de todas as atividades de tratamento de dados pessoais levadas a cabo por uma organização.** Trata-se, portanto, de um requisito prévio da conformidade e, como tal, constitui uma medida de responsabilização eficaz.

Modelo de registo da CNIL



	A	B	C	D	E	F	G
43	Numéro d'identification national unique (NIR pour la France)						
44							
45	Catégories de personnes concernées	Description					
46	Catégorie de personnes 1						
47	Catégorie de personnes 2						
48							
49	Destinataires	Description	Type de destinataire				
50	Destinataire 1						
51	Destinataire 2						
52	Destinataire 3						
53	Destinataire 4						
54							
55	Tranferts hors UE	Destinataire	Pays	Type de Garanties		Lien vers le doc	
56	Organisme destinataire 1						
57	Organisme destinataire 2						
58	Organisme destinataire 3						
59	Organisme destinataire 4						

Checklist do ICO

(também tem um modelo para o registo disponível no site)

Documentation of processing activities – best practice

When preparing to document our processing activities we:

□ do information audits to find out what personal data our organisation holds;

□ distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and

□ review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

As part of our record of processing activities we document, or link to documentation, on:

□ information required for privacy notices;

□ records of consent;

□ controller-processor contracts;

□ the location of personal data;

□ Data Protection Impact Assessment reports; and

□ records of personal data breaches.

□ We document our processing activities in electronic form so we can add, remove and amend information easily.

Encarregado de proteção de dados pessoais

- Obrigatório em 4 situações entre elas (37.º, n.º 3):

"As atividades principais do RT ou do subcontratante consistam em operações de tratamento em grande escala de ***categorias especiais de dados*** *nos termos do artigo 9.º (...)".*

Os critérios previstos na versão final do RGPD **não** atendem à **dimensão** da organização (ex. número de colaboradores) mas, antes, ao **risco** que os tratamentos realizados comportam para os DLG do titular dos dados: se a proteção em causa visa acautelar esses esses riscos, as organizações que tratam maior quantidade de dados pessoais ou dados sensíveis, criam mais riscos pelo que devem ser mais responsáveis e, inclusive, designar um EPD.

Perfil do EDP– Art. 37.º, n.º 5 e 6

"O encarregado da proteção de dados é designado com base nas suas **qualidades profissionais** e, em especial, nos seus **conhecimentos especializados no domínio do direito e das práticas de proteção de dados,** bem como na sua **capacidade** para desempenhar as funções (art. 39.º)"

"O encarregado da proteção de dados pode ser um **elemento do pessoal** da entidade responsável pelo tratamento ou do subcontratante, ou **exercer as suas funções com base num contrato de prestação de serviços**"

O considerando 97 prevê que o nível necessário de conhecimentos especializados deverá ser determinado em função das operações de tratamento de dados realizadas e da proteção exigida para os dados pessoais objeto de tratamento.

Posição e funções – art. 38.º e 39.º

- A organização deve garantir que o encarregado de proteção de dados é capaz de desenvolver as suas funções dentro da organização: orçamento próprio e staff (***independência***);

- Não recebe instruções relativamente ao exercício das suas funções (***independência***);

- Pode exercer outras funções dentro da empresa mas atenção aos conflitos de interesse: não pode nunca "*determinar os meios e as finalidades dos tratamentos de dados pessoais*". Exemplos: CEO, Chief Risk Officer, Chief Operations Officer, Diretor de recursos humanos.

Posição e funções – art. 38.º e 39.º

- Tem acesso a outros serviços, como os recursos humanos e os serviços jurídicos, informáticos, de segurança, etc., para que os EPD possam receber apoio, contributos e informações essenciais por parte destes outros serviços;

- Formação contínua: os EPD devem ter a possibilidade de se manter atualizados no que diz respeito aos desenvolvimentos no domínio da proteção de dados. O objetivo deve ser uma melhoria permanente do nível de competência dos EPD, que devem ser incentivados a participar em cursos de formação sobre proteção de dados e noutras iniciativas de desenvolvimento profissional, tais como conferências sobre privacidade, seminários, etc.;

Posição e funções – art. 38.º e 39.º

- **Informa** e **aconselha** o RT ou o subcontratante a respeito das suas obrigações nos termos do RGPD e de outra legislação de proteção de dados. **Boas práticas?**

1. Sessões/workshops de formação sobre proteção de dados pessoais regulares;
2. Participar nas reuniões, de vez em quando (2x/ano), da administração ou direção da empresa para dar nota do estado de conformidade da organização;
3. Criar uma página na intranet para proteção de dados pessoais, incluindo linhas de orientação, posições e decisões da autoridade de controlo e do Comité Europeu de Proteção de Dados, relatórios periódicos do EPD;
4. Publicar artigos e relatórios numa newsletter interna ou outro tipo de publicação;
5. Preparar “booklets” informativos e outro tipo de ficheiros.

Posição e funções – art. 38.º e 39.º

- Controla a conformidade com o RGPD e com outras normas de proteção de dados pessoais substituindo o papel de controlo prévio das autoridades de controlo que é eliminado.

1. garante que os titulares de dados pessoais são informados dos seus direitos;
2. verifica a adequação das políticas de privacidade da organização;
3. conserva e atualiza o registo das atividades de tratamento (este registo, previsto no art. 30.º, é um dos instrumentos que permitem ao EPD desempenhar as suas funções de controlo da conformidade e de prestação de informação e aconselhamento ao RT e ao subcontratante)

Posição e funções – art. 38.º e 39.º

- Papel importante:

1. Nas **avaliações de impacto** nos termos do art. 35.º: dá parecer. O parecer do EDP deve ser sempre devidamente ponderado. Em caso de desacordo, o G29 recomenda, como boa prática, que sejam enunciados os motivos para não seguir o parecer do EDP.

2. Na **consulta prévia** (art. 36.º): nas instituições da EU, o EPD é quem notifica a autoridade de controlo das operações de tratamento que colocam mais risco. No seguimento desta consulta o EPD deve monitorizar a implementação das recomendações da autoridade de controlo

Posição e funções – art. 38.º e 39.º

- **Ponto de contacto** com a autoridade de controlo com quem deve cooperar. Em geral as autoridades de controlo podem pedir ao EPD :

1. Fornecer informação adicional no quadro da consulta prévia (art. 36.º);
2. Prestar esclarecimentos a respeito de uma queixa de um titular dos dados;
3. Monitorizar o progresso da implementação das recomendações da autoridade de controlo;
4. Recolher informação para uma sondagem a realizar pela autoridade de controlo.

- O RGPD não estipula um **prazo** de **resposta** à autoridade de controlo. As boas práticas em termos europeus recomendam um prazo de **duas semanas** a contar da receção do pedido. No caso de necessitar de mais tempo, deverá avisar a autoridade de controlo e determinar quando irá responder.

Posição e funções – art. 38.º e 39.º

- Fazer **recomendações** e dar **pareceres** sempre que for consultado ou por sua iniciativa sobre questões relacionadas com o RGPD:

1. Novos sistemas informáticos;
2. Respostas a pedidos dos titulares de dados;
3. Estratégia de implementação das recomendações da autoridade de controlo;
4. ...

- Obrigação de **sigilo** e **confidencialidade** no exercício das suas funções

Algumas sugestões

1. **Relatório periódico do EPD:** uma ou duas vezes por ano p/ informar o RT ou subcontratante do status da conformidade da organização. Incluir, por exemplo:

- Número de avaliações de impacto e de consultas prévias;
- Ponto de situação do registo das atividades de tratamento;
- Resumo de diligências da autoridade de controlo junto da organização;
- Informação sobre atividades de formação e planeamentos no futuro;
- Relatório sobre os esforços desenvolvidos para implementar eventuais recomendações da autoridade de controlo;
- Número de pedidos dos titulares de dados;
- Resultados de auditorias internas ou externas

Algumas sugestões

2. Programa de trabalho com objetivos anuais:

- Ações de formação e de sensibilização;
- Implementação das exigências e recomendações da autoridade de controlo
- Projetos novos (ex: criação de um registo eletrónico das atividades)
- Identificação das áreas que merecem prioridade dentro da organização
- Ações de consulta prévia a realizar e melhorias no registo
- Realização de auditorias periódicas e verificação das medidas de segurança (*software* antivirus e antispam)

"Princípio geral e assente no bom senso": o encarregado de proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento. Tanto exige que os EPD estabeleçam prioridades nas suas atividades e centrem os seus esforços nas questões que apresentam maiores riscos em matéria de proteção de dados – art. 39.º, n.º 2

Algumas sugestões

3. **Rede de coordenadores:**

- Consoante a dimensão e a estrutura da organização, pode ser necessário criar uma equipa do EPD (o EPD e o seu pessoal). Nestes casos, a estrutura interna da equipa e as funções e responsabilidades de cada um dos seus membros devem estar claramente definidas. De igual modo, se a função do EPD for exercida por um prestador de serviços externo, um conjunto de pessoas que trabalham para essa entidade poderá exercer de modo eficaz as funções de EPD enquanto equipa, sob a responsabilidade de um contacto principal designado para o cliente.

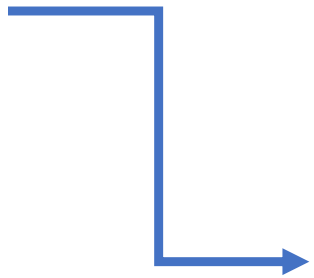
Penalizações e destituições

- As penalizações são proibidas ao abrigo do RGPD **apenas** se forem impostas em resultado do efetivo exercício das funções de EPD. Por exemplo, o EPD pode considerar que determinado tratamento é suscetível de gerar elevado risco e aconselhar o RT ou o subcontratante a realizar uma avaliação de impacto sobre a proteção de dados, mas dar-se o caso de o RT ou o subcontratante discordar da apreciação do EPD. Nesta situação, o EPD não pode ser destituído por ter emitido o seu parecer.

- Como **regra normal de gestão,** e à semelhança de qualquer outro funcionário ou contratante, nos termos e sob reserva da legislação nacional aplicável em matéria contratual ou laboral e penal, um EPD pode, no entanto, ser legitimamente destituído por outras razões que não o exercício das suas funções como EPD (p. ex., em caso de roubo, assédio físico, psicológico ou sexual ou outra falta grave).

Atores principais no RGPD

- O **titular** dos dados pessoais – o doente e os colaboradores
- O **responsável pelo tratamento** (RT) – prestadores de cuidados de saúde/associações de doentes
- **Subcontratantes** – terceiros que tratam os dados pessoais por conta do RT (caso típico do contabilista ou de alguns serviços de *cloud*)
- Autoridade de controlo - **CNPD**



- Mais disponibilidade para “estar no terreno” a realizar investigações ...
- Coimas já existiam em PT!

Artigo 37.º
Omissão ou defeituoso cumprimento de obrigações

1 - As entidades que, por negligência, não cumpram a obrigação de notificação à CNPD do tratamento de dados pessoais a que se referem os n.os 1 e 5 do artigo 27.º, prestem falsas informações ou cumpram a obrigação de notificação com inobservância dos termos previstos no artigo 29.º, ou ainda quando, depois de notificadas pela CNPD, mantiverem o acesso às redes abertas de transmissão de dados a responsáveis por tratamento de dados pessoais que não cumpram as disposições da presente lei, praticam contra-ordenação punível com as seguintes coimas:

a) Tratando-se de pessoa singular, no mínimo de 50 000$ e no máximo de 500 000$;
b) Tratando-se de pessoa colectiva ou de entidade sem personalidade jurídica, no mínimo de 300 000$ e no máximo de 3 000 000$.

2 - A coima é agravada para o dobro dos seus limites quando se trate de dados sujeitos a controlo prévio, nos termos do artigo 28.º.

Artigo 38.º
Contra-ordenações

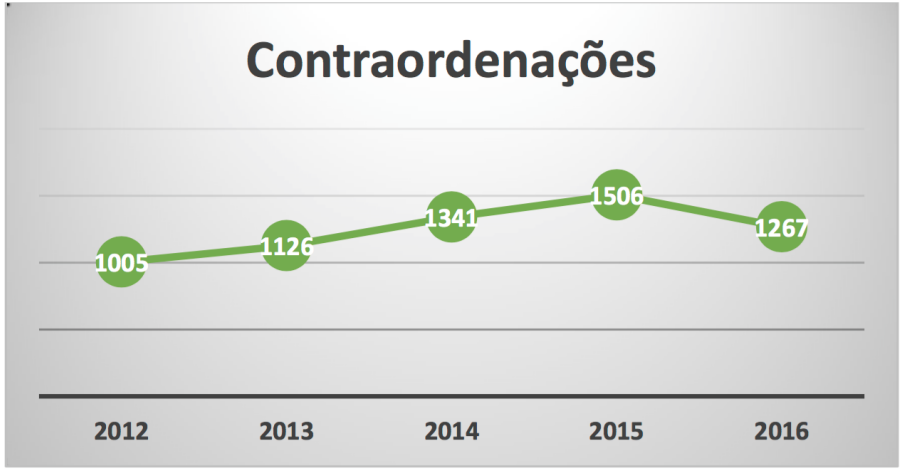
1 - Praticam contra-ordenação punível com a coima mínima de 100 000$ e máxima de 1 000 000$, as entidades que não cumprirem alguma das seguintes disposições da presente lei:

a) Designar representante nos termos previstos no n.º 5 do artigo 4.º;
b) Observar as obrigações estabelecidas nos artigos 5.º, 10.º, 11.º, 12.º, 13.º, 15.º, 16.º e 31.º, n.º 3.

2 - A pena é agravada para o dobro dos seus limites quando não forem cumpridas as obrigações constantes dos artigos 6.º, 7.º, 8.º, 9.º, 19.º e 20.º.

Alguns elementos do relatório de atividades de 2016

Em 2016, foram abertos **1267 processos de contraordenação**, registando-se uma diminuição em relação ao ano anterior para níveis idênticos aos de 2014.

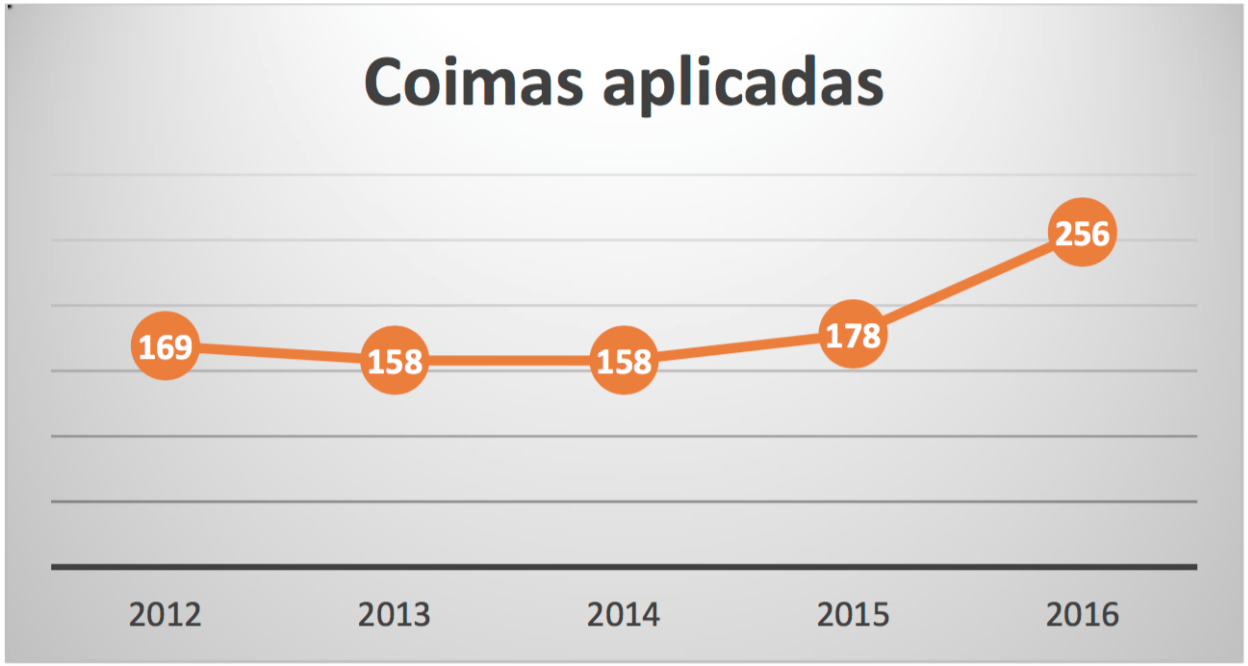


Alguns elementos do relatório de atividades de 2016

Entre estes processos, encontram-se as queixas que deram origem a meio milhar de processos.

Também as participações realizadas pela GNR e pela PSP, essencialmente quanto às condições de funcionamento dos sistemas de videovigilância, motivaram a abertura de 591 processos, enquanto as de outras entidades (tais como Ministério Público, ASAE ou ACT) resultaram em 54 processos. A CNPD decidiu ainda realizar 129 averiguações por iniciativa própria.

Alguns elementos do relatório de atividades de 2016



No quadro desta atividade em 2016, a CNPD aplicou **256 coimas,** num valor que ultrapassou o meio milhão de Euros.

Duas categorias de coimas no RGPD

- 83.º, n.º 4: coimas até **10 milhões** EUR ou, no caso de uma empresa, até 2% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior

- 83.º, n.º 5: coimas até **20 milhões EUR** ou, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior

Condições gerais de aplicação das coimas – art. 83.º e considerando 148

Critérios de proporcionalidade: "em caso de infração menor, ou se o montante da coima suscetível de ser imposta constituir um encargo desproporcionado para uma pessoa singular, pode ser feita uma repreensão em vez de ser aplicada uma coima"

Fatores agravantes ou atenuantes: a natureza, gravidade e duração da infração, o seu caráter doloso, as medidas tomadas para atenuar os danos sofridos, o grau de responsabilidade ou eventuais infrações anteriores, a via pela qual a infração chegou ao conhecimento da autoridade de controlo, etc...

Fator importante de mitigação: adesão a um código de conduta setorial (art. 40.º)

G29, *"Diretrizes de aplicação e fixação de coimas para efeitos do Regulamento 2016/679"*

Princípios relativos ao tratamento dos dados pessoais: o impacto do princípio da **responsabilidade**

- Art 5.º, n.º 2 - o responsável pelo tratamento é responsável pelo cumprimento do RGPD

- O que quer isto dizer? Que tem de respeitar os **princípios relativos ao tratamento dos dados pessoais** (art. 5.º, n.º 1), cumprindo as **obrigações** que sobre ele recaem e respeitando os **direitos do titular** dos dados pessoais e, quando solicitado, **demonstrar** à CNPD a conformidade da sua organização com o RGPD.

Alteração estrutural no esquema regulatório

- Considerando 89:

"A Diretiva 95/56/CE estabelece uma obrigação geral de notificação do tratamento de dados pessoais às autoridades de controlo. Além de esta obrigação origina encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais. ***Tais obrigações gerais e indiscriminadas de notificação deverão, por isso, ser suprimidas e substituídas por regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades****. "*

Princípio da responsabilidade

- Exige dos responsáveis pelo tratamento de dados "a aplicação de medidas **adequadas** e **eficazes** que garantam o respeito dos princípios e obrigações" do RGPD e "quando, solicitado, a sua **demonstração** às autoridades de controlo"" (*G29, "Parecer 3/2010 sobre o princípio da responsabilidade", de 13 de julho de 2010)*

- Não há uma fórmula mágica igual para todas as organizações: as medidas dirigidas a garantir o cumprimento com o RGPD devem ter em conta a **natureza**, o **âmbito**, o **contexto**, os **fins** do tratamento e os **riscos** para os direitos e liberdades dos titulares de dados. O G29 chamou a isto "**adaptabilidade**": a determinação das medidas concretas a aplicar em função do risco do tratamento e do tipo de dados tratados

- De acordo com este enfoque, **algumas das obrigações que o RGPD prevê só se aplicam quando existir um alto risco para os direitos e liberdades, enquanto que outras devem moldar-se em função do nível e do tipo de risco que os tratamentos envolvem**

Que obrigações?

- Art. 24.º - Obrigação geral de adotar "**medidas técnicas e organizativas**" e "**políticas de proteção de dados**" com base num critério de risco e de adaptabilidade/proporcionalidade

Importância do cumprimento de códigos de conduta e de procedimentos de certificação (art. 24.º, n.º 3)

Relevância da “co-regulação” ou “auto-regulação publicamente regulada”

- Não é 100% auto-regulação mas é “publicamente regulada” porque, para produzir efeitos no que respeita à conformidade do RGPD, pressupõe uma intervenção pública no momento de **aprovação** dos códigos de conduta e dos procedimentos de certificação

- **Organismos** competentes para aprovar?

- Códigos de conduta: **CNPD** (art. 40.º, n.º 5)
- Procedimentos de certificação: **CNPD** e “organismos de certificação adequados” (art. 43.º)

Que obrigações?

- Art. 25.º - Proteção de dados desde a conceção e por defeito (ex: importância da pseudonimização e anonimização)

- Art. 30.º Registo das atividades de tratamento: este registo é um instrumento que permite ao RT e à autoridade de controlo obter uma **perspetiva geral de todas as atividades de tratamento de dados pessoais levadas a cabo pela organização**. Trata-se, portanto, de um **requisito prévio da conformidade** e uma **medida de responsabilização eficaz.**

- **Art. 32.º - segurança dos dados:** importância da pseudonimização e da cifragem, dos controlos de acesso, realização de auditorias aos sistemas informáticos, firewalls, etc..

Importância do controlo dos acessos e dos *logs*

https://youtu.be/zasateRDnRA (Fonte: ICO)

Que obrigações?

- Art. 33.º e 34.º - Procedimentos internos e plano de resposta para os casos de violações de dados pessoais, para a notificação de dados pessoais à autoridade de controlo e ao titular dos dados

- Art. 35.º - Metodologia e procedimento para a realização de avaliações de impacto sobre a proteção de dados

- Art. 36.º - Consulta prévia sempre que for o caso

- Art. 37.º Designar um encarregado de proteção de dados

- Art. 40.º a 43.º - Adoção de códigos de conduta e de procedimentos de certificação

Outras medidas

- Programas de educação, formação e sensibilização (organizadas pelo encarregado de proteção de dados por exemplo) para diretores de recursos humanos, gestores de TI, diretores de unidades operacionais, etc..

- Criação de procedimentos internos para gerir pedidos de titulares de dados;

- Controlos internos ou externos (ex: auditorias) para assegurar que as medidas que existem são implementadas e funcionam na prática

Recomendação: *G29, "Parecer 3/2010 sobre o princípio da responsabilidade", de 13 de julho de 2010*

Princípios relativos ao tratamento de dados pessoais

- Licitude, lealdade e transparência (n.º 1, al. a);
- Limitação das finalidades (n.º 1, al. b);
- Minimização dos dados (n.º 1, al. c);
- Exatidão (n.º 1, al. d);
- Limitação da conservação (n.º 1, al. e);
- Integridade e confidencialidade (n.º 1, al. f).

Princípio da licitude do tratamento

- O tratamento só é lícito se ocorrer com base num dos **6 fundamentos** do art. 6.º:

1. **Consentimento** do titular dos dados;

2. 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;

3. Tratamento necessário para o cumprimento de uma **obrigação jurídica** a que o responsável pelo tratamento esteja sujeito.

Princípio da licitude do tratamento

1. Tratamento for necessário para a defesa de **interesses vitais** do titular dos dados ou de outra pessoa singular.

2. Tratamento for necessário ao exercício de funções de **interesse público** ou ao exercício da **autoridade pública**. Exemplos: saúde pública, atividades eleitorais, educação;

3. Tratamento for necessário para efeito dos **interesses legítimos** do responsável pelo tratamento, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais.

Hierarquia?

- **<u>Não</u>**: “A ordem pela qual os fundamentos jurídicos são elencados no artigo 7.º tem sido por vezes interpretada como uma indicação da importância de cada um dos diferentes fundamentos. No entanto, como já foi realçado no parecer do Grupo de Trabalho sobre o conceito de consentimento, **o texto da diretiva não estabelece uma distinção jurídica entre os seis fundamentos nem aponta para a existência de uma hierarquia entre eles.”**

- **Lógica aplicável ao RGPD...**

G29, Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.o da Diretiva 95/46/CE

Consentimento

- N.º 11 do art. 4 (definição) e art. 7.º (condições aplicáveis);

➢ Manifestação de **vontade livre, específica**, **informada** e **explícita**, mediante declaração ou ato positivo inequívoco;

➢ Consentimento será livre se a pessoa em causa puder exercer uma verdadeira escolha e não existir nenhum risco de fraude, intimidação, coação ou consequências negativas importantes se o consentimento for recusado.

➢ Excluído: silêncio, opções pré-validadas ou a omissão

➢ Revogação do consentimento só produz efeitos para o futuro (art. 7.º, n.º 3)

➢ Consentimento de crianças: art. 8.º. Não é válido antes dos 16 anos mas o legislador nacional tem margem de manobra dentro do limite dos 13 anos

G29, "Parecer 1/2011 sobre a definição de consentimento" + "Guidelines on consent under Regulation 2016/679"

Contrato ou diligências pré-contratuais - exemplos

- Se uma pessoa solicitar a uma seguradora uma proposta de seguro automóvel, a seguradora pode tratar os dados necessários, por exemplo, relativos à origem e à idade do automóvel, e outros dados relevantes e proporcionados, de forma a preparar a proposta.

- Compras online para entrega em casa implicam o tratamento de certos dados, como a morada.

- No contexto laboral, este fundamento pode permitir, por exemplo, o tratamento das informações relativas ao salário e dos dados relativos à conta bancária para que os salários possam ser pagos.

Obrigação jurídica

- Acórdão do TJ, *Worten,* C-342/12*:* obrigação de o empregador disponibilizar à Autoridade para as condições de trabalho o acesso imediato ao registo dos tempos de trabalho

- Outros exemplos: legislação que obriga a conservar dados pessoais para demonstrar que não há discriminação de género; processamento de salários deve decorrer nos termos da lei; obrigações fiscais; entre outras...

Interesse legítimo do responsável pelo tratamento

- Determinação unilateral do próprio interessado no tratamento. Se, por um lado, flexibiliza a aplicação do regulamento, por outro cria uma válvula de escape na sua aplicação e cria alguma insegurança jurídica.

- "Cláusula de ponderação de interesses". Importante:

1. Avaliação cuidada: saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade.
2. Os interesses e os direitos fundamentais do titular dos dados podem sobrepor-se ao interesse do responsável pelo tratamento, quando os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional.

Exemplos

1. Os RT que façam parte de um grupo empresarial ou de uma instituição associada a um organismo central poderão ter um interesse legítimo em transmitir dados pessoais no âmbito do grupo de empresas para **fins administrativos internos,** incluindo o tratamento de dados pessoais de clientes ou funcionários (*considerando 48*)

2. O tratamento de dados pessoais, na medida estritamente necessária e proporcionada para assegurar **a segurança da rede e das informações**. Pode ser esse o caso quando o tratamento vise, por exemplo, impedir o acesso não autorizado a redes de comunicações eletrónicas e a distribuição de códigos maliciosos e pôr termo a ataques de «negação de serviço» e a danos causados aos sistemas de comunicações informáticas e eletrónicas (*considerando 49*)

Exemplos

- Quando existir uma relação entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é **cliente** (*considerando 47*)

- Efeitos de **comercialização direta** (considerando 47)

Interesses vitais do titular dos dados

- Considerando 46: O tratamento de dados pessoais também deverá ser considerado lícito quando for necessário à **proteção de um interesse essencial à vida do titular dos dados ou de qualquer outra pessoa singular**. Em princípio, o tratamento de dados pessoais com base no interesse vital de outra pessoa singular só pode ter lugar quando o tratamento **não se puder basear manifestamente noutro fundamento jurídico.** Alguns tipos de tratamento podem servir tanto importantes **interesses públicos** como **interesses vitais** do titular dos dados, por exemplo, **se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catastrofes naturais e de origem humana.**

Regime específico para o tratamento de dados relativos à saúde – art. 9.º

- **Consentimento** explícito;

- Se o tratamento for necessário para **efeitos do cumprimento de obrigações e do exercício de direitos específicos** do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva (...) que preveja garantias adequadas;

- Se o tratamento for necessário para proteger os **interesses vitais do titular dos dados** ou **de outra pessoa singular,** no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento;

Regime específico para o tratamento de dados relativos à saúde – art. 9.º

- Se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma **fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados** a terceiros sem o consentimento dos seus titulares;

- Se o tratamento se referir a dados pessoais que tenham sido **manifestamente** tornados **públicos** pelo seu titular;

Regime específico para o tratamento de dados relativos à saúde

- Se o tratamento for **necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da suas função jurisdicional**;

- Se o tratamento for necessário por motivos de **interesse público** importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, **respeitar** a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;

Regime específico para o tratamento de dados relativos à saúde

- Se o tratamento for necessário para **efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social** com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.o 3;
- Se o tratamento for necessário por **motivos de interesse público no domínio da saúde pública,** tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;

Regime específico para o tratamento de dados relativos à saúde

- Se o tratamento for necessário para **fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos**, em conformidade com o artigo 89.º, n.º 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.

- Nota importante: ***"Os Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde."***

Princípio da transparência

- O RT tem a **obrigação** de informar o titular dos dados sobre o modo como os seus dados estão a ser utilizados (relacionado com os direitos do titular dos dados)

- Este princípio exige que as informações fornecidas aos titulares dos dados (no quadro do direito de informação) sejam de **fácil acesso** e **compreensão** e formuladas numa **linguagem clara e simples**. É essencial que o titular dos dados compreenda o que está a acontecer aos seus dados

G29, "*Guidelines on transparency under Regulation 2016/679" + AEPD, "Guía para el cumplimento del deber de informar"*

Princípio da limitação das finalidades

- Os dados pessoais são recolhidos para finalidades **determinadas** e, em regra, não podem ser tratados posteriormente de uma forma incompatível com essas finalidades.

- Quando partilhamos dados pessoais com outros, temos habitualmente uma **expectativa** acerca das finalidades para as quais esses dados serão utilizados. Há um elemento de valor em honrar essas expectativas e em conservar a confiança e a certeza jurídica, sendo por isto que a limitação da finalidade é uma garantia tão importante, **uma pedra angular da protecção de dados.**

- Exceções: consentimento; legislação da UE e nacional (n.º 4 do art. 6.º) e tratamento para fins de arquivo de interesse público, investigação científica ou histórica ou para fins estatísticos (al. b) do n.º 1 do art. 5.º)

Princípio da limitação das finalidades

- Art. 6.º, n.º 4. Aplicação de um **teste de compatibilidade**: *o tratamento posterior é ou não compatível com a finalidade que determinou a recolha inicial dos dados*? Ter em conta alguns elementos:

a) Ligação entre a finalidade para a qual os dados foram recolhidos e a finalidade do tratamento posterior;

b) O contexto em que os dados pessoais foram recolhidos, em particular as expectativas razoáveis do titular dos dados quanto à posterior utilização;

c) A natureza dos dados;

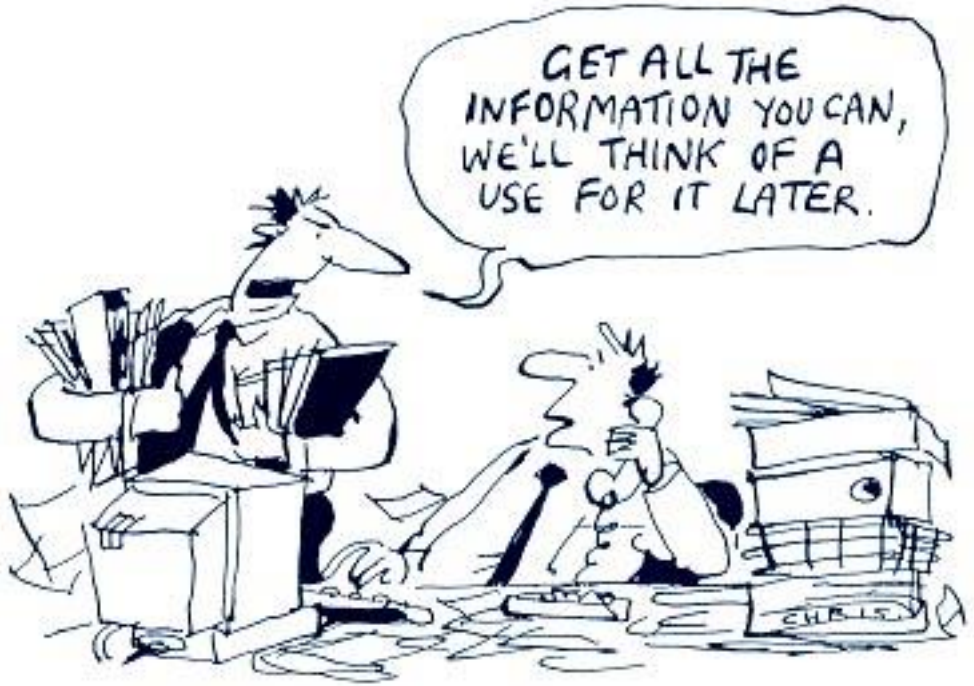
d) As eventuais consequências do tratamento posterior;

e) A existência de salvaguardas adequadas como a pseudonimização.

Princípio da minimização dos dados

- Os dados pessoais tratados têm de ser **adequados**, **pertinentes** e **limitados** ao que é necessário à concretização da finalidade do tratamento. O RT deve restringir a recolha de dados às informações diretamente pertinentes para a finalidade do tratamento;

- O objetivo é reduzir os tratamentos de dados pessoais a um mínimo possível para a das finalidades dos mesmos: dados em excesso e desnecessários devem ser apagados.



Princípio da exatidão

- O responsável pelo tratamento deverá adotar medidas para se certificar, com um grau de certeza razoável, que os dados são **exatos** e estão **atualizados**.

- Especialmente relevante na sequência de pedidos de acesso e de retificação do titular dos dados e em situações nas quais o controlo da exatidão dos dados é uma necessidade absoluta devido aos potenciais danos que o titular poderá sofrer se os seus dados não forem exatos

Princípio da limitação da conservação

- Os dados devem ser conservados de forma a que a identificação dos titulares dos dados possa ser realizada apenas durante o período necessário para as finalidades

- Há certas medidas que garantem o cumprimento deste princípio, como a aplicação de técnicas de anonimização e de pseudonimização; a adoção de uma política de privacidade do RT na qual conste prazos de retenção.

Princípio da segurança, integridade e confidencialidade dos dados pessoais

- O RT e o subcontratante têm a obrigação de colocar em prática medidas técnicas e organizativas para evitar **interferências não autorizadas ou ilícitas nas operações de tratamento, perdas, destruições ou danificações acidentais**

- Estas medidas devem ser implementadas tendo em conta:

1. As técnicas mais avançadas
2. Os custos de aplicação
3. A natureza, o âmbito, o contexto e as finalidades do tratamento
4. Os riscos para os direitos e liberdades das pessoas singulares

ICO, "A practical guide to IT security. Ideal for the small business"

Princípio da segurança, integridade e confidencialidade dos dados pessoais

Que medidas?

1. Pseudonimização e cifragem ou encriptação dos dados

2. *Software* e *hardware* que garanta a confidencialidade, integridade, disponibilidade e resiliência

3. Implementação de sistemas de *backups* para garantir a disponibilidade e o acesso aos dados pessoais no caso de incidentes

4. Processos para testar, apreciar e avaliar a eficácia das medidas para garantir a segurança dos dados (realização de auditorias internas e externas, testes de intrusões)

Princípio da segurança, integridade e confidencialidade dos dados pessoais

1. Certificação de que as autorizações de acesso a dados pessoais foram concedidas pela pessoa competente e exigem documentação adequada;

2. Formações aos funcionários sobre as regras relativas à segurança dos dados e as respetivas obrigações, especialmente em matéria de confidencialidade;

3. Proteção contra o acesso a instalações e a *hardware* e *software* do RT ou do subcontratante, incluindo controlos sobre a autorização de acesso;

- **Nota**: cumprimento de códigos de conduta e de procedimentos de certificação podem ser usados para demonstrar o cumprimento desta medida

Direitos velhos e direitos novos

- Direito à informação (art. 13.º e 14.º)
- Direito de acesso (art. 15.º)
- Direito de retificação (art. 16.º)
- **Direito ao apagamento (art. 17.º)**
- **Direito à limitação do tratamento (art. 18.º)**
- **Direito de portabilidade (art. 20.º)**
- Direito de oposição (art. 21.º)
- **Direito em relação a decisões individuais automatizadas (art. 22.º)**
- **Direito de informação quando ocorra uma violação de dados pessoais (art. 34.º)**

Regras gerais

- **O RT deve facilitar** o exercício destes direitos, criando procedimentos para o efeito, designadamente eletrónicos (art. 12.º) e estabelecendo um mecanismo interno de gestão dos pedidos dos titulares de dados.

- **O exercício é gratuito** (art. 12.º, n.º 5). Exceção: pedidos "manifestamente infundados ou excessivos", "especialmente repetitivos".

- **Recusa** é possível mas deve ser "demonstrado o caráter manifestamente infundado ou excessivo" do pedido do titular (art. 12.º, n.º 5).

- Prazo de resposta **um mês a contar da data da receção do pedido** (poderá estender-se 2 meses para **pedidos especialmente complexos).**

Direitos gerais

- Exercidos em **qualquer** tipo de circunstância e **independentemente** do fundamento do tratamento:

1. Direito à **informação** (art. 13.º e 14.º).

2. Direito à **confirmação** do tratamento e ao **acesso** aos dados pessoais (art. 15.º).

3. Direito de **retificação** (art. 16.º).

Direitos especiais (circunstâncias específicas)

- O exercício destes direitos **não** é **irrestrito** nem **absoluto**:

1. Direito ao apagamento ou "direito a ser esquecido" (art. 17.º)
2. Direito à limitação do tratamento (art. 18.º)
3. Direito de portabilidade (art. 20.º)
4. Direito de oposição (art. 21.º)
5. Direito em relação a decisões individuais automatizadas (art. 22.º)
6. Direito a ser notificado em caso de uma violação de dados pessoais (art. 34.º)

Guia de implementação do Regulamento

a) CNPD, 28.01.2017 – “10 medidas para preparar a aplicação do Regulamento Europeu de Proteção de dados pessoais”

- **Rever a informação** que é fornecida aos titulares dos dados no âmbito da recolha dos mesmos: o regulamento obriga a prestar mais informações do que a diretiva. A organização terá de reformular impressos, políticas de privacidade e todos os textos que prestem informação aos titulares de modo a cumprir com o RGPD;

- **Rever os procedimentos internos** de garantia do exercício dos direitos dos titulares dos dados: o RGPD tem um prazo máximo de resposta e exige a documentação deste procedimento; reconhecem-se mais direitos do que na diretiva.

- Rever os termos do **consentimento** (especial atenção aos menores)

- Avaliar a **natureza dos tratamentos** de dados efetuados, para apurar quais os que se podem enquadrar no conceito de dados sensíveis, e consequentemente se aplicarem condições específicas.

- Analisar o **contexto e a escala** destes tratamentos de dados para verificar se decorrem obrigações particulares, tais como a **designação de um encarregado de proteção de dados.**

- **Documentar** de forma detalhada todas as atividades relacionadas com o tratamento de dados pessoais, tanto as que resultam diretamente da obrigação de manter um registo como as relativas a outros procedimentos internos, de modo a que a organização esteja apta a demonstrar o cumprimento de todas as obrigações decorrentes do RGPD.

- Deve rever os **contratos de subcontratação** de serviços realizados no âmbito de tratamentos de dados pessoais para verificar se contêm todos os elementos exigidos pelo regulamento.

- Necessário designar um **encarregado de proteção de dados pessoais?**

- **Revisão das medidas técnicas e organizativas a adotar** (pseudonimização, controlos de acesso, gestão de privilégios) e das medidas de segurança da informação

- Avaliar rigorosamente o **tipo de tratamentos de dados que tenha projetado realizar num futuro próximo**, de modo a analisar a sua natureza e contexto e os potenciais riscos que possam comportar para os titulares dos dados, de modo a aplicar com eficácia os princípios da proteção de dados desde a conceção e por defeito.

- Adotar **procedimentos internos** e ao nível da subcontratação, se for o caso, para lidar com casos de violações de dados pessoais, designadamente na deteção, identi cação e investigacão das circunstâncias, medidas mitigadoras, circuitos da informação entre RT e subcontratante, envolvimento do EDP e notificação à CNPD, atendendo aos prazos prescritos no regulamento.

b) Outras ferramentas de implementação do RGPD e outros Guias:

- AEPD (Espanha): "FACILITA" - para organizações com pouco risco
- AEPD (Espanha) – "MODELO DE DOCUMENTO DE SEGURIDAD"
- ICO (Reino Unido): "*GDPR consent guidance*" ; "documentation guidance"; "Self-assessment tool", entre outras
- ICO (Reino Unido): "GDPR Myths" (blog no site)

- CNIL (França): “Règlement européen: se préparer em 6 étapes” + um formulário modelo de um registo das atividades de tratamento e outro para as notificações de violação de dados pessoais;

- Agencia Espanola de Proteccion de Datos: “Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento”; “Directrices para La Elaboracion de Contratos entre responsables y encargados del tratamiento”; “Guia para El Cumplimento Del Deber de Informar”;

- Commission de la protection de la vie privée (Bélgica): “Préparez-vous em 13 étapes”;
- Data Protection Commissioner (Irlanda): “The GDPR and you. Preparing for 2018”;

- 24 de janeiro de 2018 a CE publicou orientações sobre o RGPD: http://europa.eu/rapid/press-release_IP-18-386_pt.htm

Obrigada!

Written by Daniel J. Solove www.teachprivacy.com Illustrated by Ryan Beckwith