GRUPO EUROPEU DE ARQUIVOS

ORIENTAÇÕES

SOBRE PROTEÇÃO DE DADOS NOS ARQUIVOS

Orientações do GEA sobre a implementação do Regulamento Geral de Proteção de Dados no setor dos arquivos

Estas orientações pretendem auxiliar os serviços de arquivo da Europa, a aplicar o Regulamento Geral de Proteção de Dados Pessoais. Representam um trabalho contínuo, em desenvolvimento, sujeito a melhorias e enriquecido com a vossa experiência e comentários. Estas orientações poderão ser alteradas com base em jurisprudência futura e nas opiniões e orientações estabelecidas pelo Concelho Europeu de Proteção de Dados.

O Grupo Europeu de Arquivos acolhe vivamente os seus comentários. Os comentários podem ser enviados para o seguinte endereço de e-mail: SG-EAG-GUIDELINES@ec.europa.eu.

AVISO LEGAL

Este documento não se destina a fornecer, e não constitui ou compromete, aconselhamento jurídico sobre qualquer assunto em particular e é disponibilizado apenas para fins de informação geral. Não deverá agir ou abster-se de agir com base nestes conteúdos, sem procurar o devido aconselhamento jurídico legal ou profissional.

Título original: Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector

Autor: © European Archives Group

Data: outubro 2018

Tradução: Rafael António e Sofia Pina

TABELA DE CONTEÚDOS

ACRÓNIMOS E ABREVIATURAS UTILIZADOS NESTAS ORIENTAÇÕES

DIRECTIVA 95/46 / CE: Diretiva 95/46 / CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

DPA: Autoridade de Proteção de Dados (APD)

DPO: Encarregado da pela proteção de dados (EPD)

EAG: Grupo Europeu de Arquivos (GEA)

EDPB: Conselho Europeu de Proteção de Dados (CEPD)

GDPR: Regulamento Geral sobre a Proteção de Dados (RGPD), ou seja, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados)

I. INTRODUÇÃO

1. **A quem se destinam:** estas orientações são dirigidas a instituições públicas e privadas que detêm arquivos, ou seja, documentos que foram selecionados para conservação definitiva. Elas não são apenas dirigidas ao Arquivo Nacional ou Arquivos do Estado, mas também para Arquivos Distritais e Municipais, museus, bibliotecas, fundações e outras entidades públicas e privadas que custodiam arquivos.

2. **Objetivo:** estas orientações pretendem fornecer informação básica e ser um guia prático dos arquivistas no que se refere ao desafio específico da aplicação do Regulamento Geral de Proteção de Dados (RGPD) nos arquivos.

3. **Âmbito:** Assim como qualquer outra entidade pública e privada, os serviços do arquivo procedem ao tratamento de dados pessoais relativos ao seu próprio pessoal. Estas orientações não fornecem diretrizes para tratamento de dados pessoais, por um serviço de arquivo, relativamente aos seus recursos humanos. Estas orientações também não fornecem orientações para o tratamento de dados pessoais dos utilizadores, de doadores, de empreiteiros, de fornecedores bem como de outras entidades singulares ou coletivas com quem estabelecem relações contratuais. As Autoridades de Proteção de Dados nacionais e os Governos Nacionais, a Comissão Europeia, o Conselho Europeu de Proteção de Dados e outros atores já estão a fornecer orientações sobre essas questões (ver o Apêndice: Onde procurar orientação adicional). Estas Orientações concentram-se exclusivamente sobre o tratamento de dados pessoais contidos nos fundos arquivísticos.

4. **O RGPD: as mesmas regras em toda a União Europeia (mas com exceções para o sector dos arquivos).** Um regulamento da UE é um ato legislativo vinculativo que deve ser aplicado, na íntegra, em toda a União. A UE decidiu adotar um regulamento - em vez de uma diretiva - para substituir a anterior legislação de proteção de dados (Diretiva 95/46 / CE 1) a fim de ter normas mais uniformes em todos os Estados Membros. No entanto, o RGPD permite alguma margem aos Estados Membros para introduzirem exceções nalgumas áreas específicas. Uma delas é para "fins de arquivo de interesse público"; outra é para a investigação histórica. Os arquivistas devem verificar se os legisladores nacionais aproveitaram esta oportunidade que o RGPD fornece para incluir tais exceções.

5. **Minimização dos dados versus conservação definitiva**. Um princípio fundamental do RGPD é minimização dos dados. Isto realmente não é novo, a Diretiva 95/46 / CE[1] já foi baseada neste princípio. Os dados pessoais devem ser recolhidos e tratados apenas se for estritamente necessário e serem "conservados de forma a permitir a identificação dos titulares dos dados" (ou seja, a pessoa singular a quem se referem os dados) apenas enquanto forem necessários, para atingir o objetivo para o qual foram recolhidos (art.º

[1] Diretiva 95/46 / CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 sobre a proteção dos indivíduos no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

5 (1) pontos (b) e (e)). Se não houvessem exceções a este princípio então, no futuro, deixariam de existir dados pessoais nos arquivos. Mas o legislador europeu introduziu algumas exceções a esta regra. Foi reconhecido que os arquivos são necessários para respeitar os direitos fundamentais. De fato, o RGPD afirma que "os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos". No entanto, ficam sujeitos à condição de serem tomadas medidas apropriadas "a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»)" (art.º 5 (1) ponto (e)).

6. **O tratamento de dados pessoais apenas quando é realmente necessário não é nada novo para os arquivistas**. Uma das funções principais do arquivo é a seleção de documentos para conservação definitiva. Apenas uma percentagem muito pequena dos documentos criados ou recebidos pelo Estado, administrações públicas ou por entidades privadas, no exercício da sua atividade, é incorporada em instituições arquivísticas. Os arquivistas avaliam e somente selecionam para conservação definitiva, os documentos que são necessários para fazer valer os direitos dos cidadãos e para a pesquisa histórica. As instituições arquivísticas devem publicar os critérios gerais que se aplicam à seleção de documentos para conservação definitiva e deve ser capaz de explicar por que decidiram manter fundos arquivísticos específicos que contenham dados pessoais.

7. **Conservar dados pessoais não é o mesmo que fornecer o acesso:** Em todos os Estado Membros europeus a legislação nacional estabelece regras relativas ao acesso aos documentos mantidos nos arquivos públicos. O prazo estabelecido para restrição de acesso aos documentos que contêm dados pessoais varia de um país para o outro e de acordo com a natureza dos dados pessoais. Em Itália, os dados pessoais que revelam a origem racial ou étnica, as opiniões religiosas e políticas, filiação em partidos, sindicatos, estão inacessíveis por 40 anos, enquanto aqueles que dizem respeito a questões de saúde e à vida sexual estão inacessíveis por 70 anos; e os registos que podem revelar a identidade de uma mãe que pretendeu dar à luz anonimamente estão inacessíveis por 100 anos. O período de restrição de acesso pode ser ainda mais longo; por exemplo, na Roménia os registos médicos e do estado civil estão inacessíveis por 100 anos após a sua criação, enquanto documentos relativos à vida privada de um indivíduo estão inacessíveis por 40 anos após a morte da pessoa em causa. Os cidadãos podem confiar nos arquivos: eles não divulgarão dados pessoais indevidamente.

8. **O RGPD não altera o período de restrição de acesso a documentos com informação pessoal**. O regulamento inclui disposições relativas ao direito dos titulares para aceder aos dados que lhes digam respeito. Mas não inclui regras sobre o acesso aos arquivos, pelo público em geral. O período de restrição de acesso aos documentos que contenham dados pessoais permanecerá o mesmo.

9. **O RGPD não modifica os princípios da liberdade de acesso à informação.** A Carta dos Direitos Fundamentais da União Europeia[2] considera tanto a proteção dos dados pessoais como a liberdade de expressão e de informação (que inclui a liberdade de receber e transmitir informações) como direitos fundamentais. O RGPD não modifica a legislação no que se refere à liberdade de informação. Ele afirma que "Os dados pessoais que constem de documentos na posse dessas autoridades públicas ou organismos públicos deverão poder ser divulgados publicamente por tais autoridades ou organismos, se a divulgação estiver prevista no direito da União ou do Estado Membro que lhes for aplicável." (considerando 154).

10. **O RGPD não modifica a legislação no que se refere à liberdade de expressão.** Os utilizadores dos arquivos incluem, entre outros, jornalistas, académicos e outros investigadores de todos os domínios que irão, em muitos casos, publicar os seus trabalhos. O RGPD não altera as leis de imprensa nem outras regras relativas à liberdade de expressão. Declara que: "Os Estados Membros conciliam por lei o direito à proteção de dados pessoais, nos termos do presente regulamento, com o direito à liberdade de expressão e de informação, incluindo o tratamento para fins jornalísticos e para fins de expressão académica, artística ou literária" (art.º 85). Os Estados Membros estabelecem derrogações ao disposto no RGPD, se forem necessárias para conciliar o direito à proteção de dados pessoais com a liberdade de expressão e de informação. (art.º 85).

11. **Estas orientações não são um código de conduta**. O RGPD encoraja "…a elaboração de códigos de conduta destinados a contribuir para a correta aplicação (art.º 40(1)) do regulamento. Prevê ainda que "As associações e outros organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes podem elaborar códigos de conduta." (art.º 40 (2)) e determina um procedimento específico para a aprovação de códigos de conduta pela Autoridade Nacional de Proteção de Dados (se o código for apenas um âmbito nacional) ou pelo Conselho Europeu de Proteção de Dados e pela Comissão Europeia (se o Código for aplicado em diferentes Estados Membros da UE).

    As presentes orientações foram elaboradas pelo Grupo Europeu de Arquivos (GEA), um grupo de peritos da Comissão Europeia, composto por representantes dos Arquivos Nacionais e Direcções-Gerais de Arquivos dos Estados Membros da UE. Estas Orientações não serão submetidas ao procedimento de aprovação previsto pelo art.º 40 do RGPD para códigos de conduta. Devem ser consideradas um documento orientador dessas políticas.

[2] 2000/C364/01

II. PRINCÍPIOS GERAIS

1. PRINCÍPIOS GERAIS RELATIVOS AO TRATAMENTO DE DADOS PESSOAIS (ART.º 5)

Os arquivistas devem estar cientes de alguns princípios gerais a respeito do tratamento de dados pessoais estabelecidos no art.º 5 do RGPD, que estabelece:

1. Os dados pessoais devem ser:

a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);

b) Recolhidos para finalidades determinadas, explícitas e legítimas não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89º, nº 1 («limitação das finalidades»);

c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);

e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89º, nº 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);

f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»);

2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no nº 1 e tem de poder comprová-lo («responsabilidade»).

Estes princípios têm muitas consequências práticas para serviços de arquivo e devem, portanto, estar sempre presentes. Os arquivistas estão familiarizados com a salvaguarda do princípio da confidencialidade, garantindo este princípio enquanto norma basilar nos arquivos

de forma a proteger informações confidenciais contra o acesso indevido. Algumas implicações destes princípios são, contudo, menos óbvias. Por exemplo:

- o princípio da 'transparência' significa - entre outras coisas - que os arquivos têm a responsabilidade de divulgar informações claras, amigáveis para o utilizador, e sobretudo, em particular, porquê e como tratam os dados pessoais e como os titulares dos dados podem aceder;
- o princípio da 'integridade' significa - entre outras coisas – evitar as más práticas que conduzem à perda de documentos contendo dados pessoais, constituem não só uma violação dos princípios profissionais dos arquivistas e das regras de arquivo, mas também uma violação ao RGPD.

2. LICITUDE DO TRATAMENTO (ARTº 6)

Segundo o RGPD o tratamento de dados pessoais somente fica legitimado se, pelo menos, forem verificadas uma das circunstâncias enunciadas no art.º 6º, incluindo nomeadamente: "o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais"; "o tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte"; "o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito", etc. De especial interesse para os arquivistas é a condição indicada em (1) ponto e) onde o tratamento de dados pessoais é legitimado quando "for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública".

O RGPD deixa à legislação da UE ou nacional o critério para estabelecer o tipo de atividades consideradas como sendo "de interesse público". A legislação nacional pode incluir disposições que definam quando o tratamento dos arquivos por uma determinada instituição, ou o tratamento de certas categorias de arquivos é "de interesse público".

3. O RGPD APENAS PROTEGE OS DADOS PESSOAIS DE PESSOAS VIVAS (MAS A LEGISLAÇÃO NACIONAL TAMBÉM PODE PROTEGER OS DADOS DE PESSOAS FALECIDAS)

O RGPD protege os dados pessoais de pessoas vivas. Não se aplica aos dados pessoais de pessoas falecidas. No entanto, os arquivistas devem verificar se as leis nacionais o permitem. Na verdade, o RGPD estipula que "os Estados Membros podem providenciar regras relativas ao tratamento de dados pessoais de pessoas falecidas" (considerando 27).

Como podem os arquivistas saber se o titular dos dados é falecido? Na maioria dos casos, não conseguem. No entanto, podem razoavelmente assumir que as pessoas nascidas há mais de cem anos atrás não estão vivas. Por exemplo, um arquivista ao tratar dados pessoais de soldados que lutaram na I Grande Guerra, pode assumir que estes titulares já não estão

vivos e que, portanto, o RGPD não se aplica a essas pastas. Muitos outros casos, no entanto, poderão não ser de tão evidente decisão. Os arquivistas terão que fazer, caso a caso, uma avaliação da possibilidade que os fundos à sua guarda possam conter dados pessoais de indivíduos ainda vivos.

III. O QUE É "FINS DE ARQUIVO DE INTERESSE PÚBLICO"?

4. DIFERENTES REGRAS PARA DIFERENTES ARQUIVOS ("FINS DE ARQUIVO DE INTERESSE PÚBLICO" NO CONSIDERANDO 158)

O RGPD permite uma série de exceções relativas a "fins de arquivo de interesse público". O considerando 158 explica o significado desta expressão.

> "As autoridades públicas ou os organismos públicos ou privados que *detenham documentos de interesse público* deverão ser serviços que, nos termos do direito da União ou dos Estados Membros, tenham a obrigação legal de adquirir, conservar, avaliar, organizar, descrever, comunicar, promover, divulgar e facultar o acesso a documentos de valor duradouro no interesse público geral.."(ênfase nossa)

Quais os serviços de arquivo abrangidos por esta definição? Como se pode ver, não é a natureza dos arquivos, mas a missão da instituição que custodia a determinar se a isenção pode ser aplicada. Podemos dizer com segurança que os Arquivos Nacionais e outros Arquivos Históricos dirigidos pelo Estado ou por outros organismos públicos, cumprem a missão de "arquivar com fins de interesse público", conforme o definido no RGPD, tal como faz o Arquivo Histórico da União Europeia.

De acordo com a lei do Estado Membro, outras instituições que custodiam arquivos também se podem enquadrar nesta definição. Por exemplo, a legislação nacional pode indicar que um órgão específico tem a missão de adquirir, preservar e disponibilizar aos investigadores os documentos pessoais de escritores; ou pode criar um museu sobre a história da ciência que inclui, entre as suas tarefas, a aquisição e a preservação de documentos pessoais de cientistas. A lei do Estado Membro pode criar um instituto para a história de um regime autoritário do passado, cuja missão inclui a preservação da herança documental relativa às vítimas da repressão política.

É importante considerar, quando o RGPD se refere à "legislação nacional", isso não significa apenas peças legislativas aprovadas pelos parlamentos nacionais. De facto, o considerando 41, estipula que "Caso o presente regulamento se refira a um fundamento jurídico ou a uma medida legislativa, não se trata necessariamente de um ato legislativo adotado por um

parlamento". O instrumento jurídico que pode atribuir a uma entidade a obrigação legal de adquirir, preservar, organizar e comunicar os arquivos pode mudar de um país para outro, de acordo com os diferentes sistemas constitucionais. Por exemplo, poderia ser uma lei nacional, uma lei regional, um decreto ministerial, e assim por diante. De qualquer forma, os arquivistas devem considerar que um serviço de arquivo ou outra instituição cultural com a missão estatutária de adquirir, preservar e permitir o acesso aos arquivos com fins de interesse público, estão englobados na definição do considerando 158.

Nem todas as entidades que custodiam arquivos têm a obrigação legal de os adquirir e, assim, nem todos estão abrangidos pela definição do considerando 158. No entanto, em muitos casos, estas entidades têm uma missão cultural clara e detêm arquivos para fins de pesquisa histórica. O RGPD admite exceções para tratamento de dados pessoais para investigação histórica, referidos em todo o Regulamento, em particular, no artigo 89.

Por último, os arquivistas devem estar cientes de que as exceções em favor de "fins de arquivo de interesse público" só dizem respeito ao tratamento de dados pessoais incluídos nos fundos mantidos pelos arquivos. Todos os outros tratamentos de dados pessoais realizados pelos serviços dos arquivos submetem-se às mesmas regras de qualquer outra entidade pública ou privada. Noutras palavras, quando os serviços de arquivo tratam dados pessoais dos utilizadores, ou de estudantes que participam de atividades educacionais, ou de participantes em conferências e assim por diante, não beneficiam de qualquer dispensa das regras de proteção de dados.

5. GARANTIAS E DERROGAÇÕES RELATIVAS AO TRATAMENTO PARA FINS DE ARQUIVO DE INTERESSE PÚBLICO OU PARA FINS DE INVESTIGAÇÃO CIENTÍFICA OU HISTÓRICA OU PARA FINS ESTATÍSTICOS (ARTº. 89)

Ao longo do RGPD, encontram-se muitas referências aos arquivos e à investigação histórica. Vários artigos que estabelecem deveres ou proibições ao responsável pelo tratamento de dados permitem, de fato, dispensas quando o tratamento é necessário para fins de arquivo de interesse público ou para fins de investigação científica ou histórica.

Além disso, o RGPD inclui um artigo dedicado especificamente ao "tratamento para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos" (art.º 89). O primeiro parágrafo deste artigo estabelece as regras que são comuns tanto ao tratamento de dados pessoais "para fins de arquivo de interesse público" como ao tratamento para "fins de investigação científica ou histórica e para fins estatísticos".

1. O tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos estará sujeito a garantias apropriadas, de acordo com o presente regulamento, relativamente aos direitos e liberdades dos titulares em causa. Estas garantias devem assegurar que as medidas técnicas e organizacionais estão em vigor, em particular, a fim de garantir o respeito pelo princípio da minimização dos dados. Essas medidas podem incluir pseudonimização desde que esses requisitos possam ser cumpridos dessa forma. Se esses fins puderem ser cumpridos mediante uma transformação posterior que não permita ou que já não permita a identificação dos titulares de dados, esses fins devem ser cumpridos dessa forma.

O artigo 89 declara ainda que

2. Quando os dados pessoais sejam tratados para fins de investigação científica ou histórica ou para fins estatísticos, o direito da União ou dos Estados Membros pode prever derrogações aos direitos a que se referem os artigos 15º, 16º, 18º e 21º, (…)
3. Quando os dados pessoais sejam tratados para fins de arquivo de interesse público, o direito da União ou dos Estados Membros pode prever derrogações aos direitos a que se referem os artigos 15º, 16º, 18º, 19º, 20º e 21º (…)

Em ambos os casos, as derrogações acima mencionadas são possíveis:

> (…) sujeito às condições e às garantias indicadas no parágrafo 1 deste Artigo, na medida em que estes direitos são suscetíveis de tornar impossível ou prejudicar gravemente a realização dos fins específicos, sendo essas derrogações necessárias ao cumprimento desses mesmos fins.

O princípio da minimização dos dados e a obrigação de tomar as devidas medidas de salvaguarda adequadas, a fim de proteger os direitos dos titulares dos dados são, portanto, comuns ao "tratamento para fins de arquivo de interesse público" ou "tratamento para fins de investigação científica ou histórica ou para fins estatísticos ". Mas a aplicação concreta destes princípios será diferente nas diferentes áreas.

Na investigação médica é importante preservar a correlação de diferentes dados médicos sobre um determinado paciente, mas a identidade do paciente é irrelevante. Neste caso, a *pseudonimização* dos registos médicos seria uma medida adequada. No entanto, um serviço de arquivo que contenha documentos de interesse público deve preservar a integridade dos registos médicos selecionados para conservação definitiva no interesse dos titulares dos dados. Por exemplo, recentemente, alguns países conseguiram pagar indemnizações a pessoas que tinham sido submetidas as esterilizações forçadas, décadas atrás, porque a integridade dos registos médicos foi garantida. A história europeia fornece muitos outros casos em que a preservação integral dos documentos que incluíam dados pessoais, tem sido fundamental para restaurar os direitos dos titulares dos dados.

Fazer cumprir o direito à verdade e o direito de reparação e compensação às vítimas de violações graves dos direitos humanos requer a preservação integral dos arquivos

Vítimas de perseguições fascistas e do nazismo ou da utilização nazi do trabalho escravo puderam ser identificados e indemnizados porque os arquivos que continham dados pessoais foram preservados. A preservação integral dos arquivos tem sido igualmente instrumental para devolver propriedades confiscadas depois da queda do comunismo. O RGPD incentiva a preservação integral dos arquivos que documentam violações dos direitos humanos. O considerando 158 estabelece:

> "Os Estados Membros deverão também ser autorizados a determinar o posterior tratamento dos dados pessoais para efeitos de arquivo, por exemplo tendo em vista a prestação de informações específicas relacionadas com o comportamento político no âmbito de antigos regimes totalitários, genocídios, crimes contra a humanidade, em especial o Holocausto, ou crimes de guerra. ".

Quando for tomada uma decisão sobre a retenção ou eliminação de documentos que contenham dados pessoais, os arquivistas devem ter em atenção que a proteção de dados pessoais deve ser balanceada relativamente ao direito à justiça, o direito à verdade e o direito de reparação e compensação para as vítimas de graves violações dos direitos humanos.

Reconhecendo que o tratamento para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, requer diferentes tipos de medidas, de modo a fazer valer o princípio da minimização dos dados, o RGPD nem sempre exige a pseudonimização, mas apenas quando "esses propósitos só podem ser cumpridos dessa maneira".

Os arquivistas reforçam o princípio da minimização dos dados de forma diferente do que fazem os cientistas e os estatísticos. Em primeiro lugar, selecionam os documentos que contêm dados pessoais para conservação definitiva somente quando for realmente

necessário fazê-lo, em conformidade com a missão que a lei atribui ao arquivo. Além disso cumprem as leis relativas ao acesso aos arquivos, restringindo o acesso a documentos que contenham dados pessoais, por tanto tempo quanto a legislação nacional o exige. As restrições legais sobre o acesso aos arquivos diferem de um país para outro e para certos tipos de dados pessoais o período de restrição pode ser tão longo que chega aos 120 anos.

Quando os documentos que contêm dados pessoais se tornam comunicáveis, mas exista ainda a possibilidade de que o titular dos dados esteja vivo, os arquivistas devem abster-se de qualquer tratamento que possa resultar em danos à dignidade do titular dos dados. Estes devem ter em mente o expresso no art.º 1º da Carta dos Direitos Fundamentais da União Europeia: “A dignidade humana é inviolável. Deve ser respeitada e protegida.” A realização concreta deste princípio implica abster-se de publicar documentos de arquivo em linha ou instrumentos de descrição cuja difusão possa atentar contra a dignidade dos titulares dos dados.

Os serviços de arquivo também podem fazer uso de pseudonimização, mas se for praticada pelos serviços de arquivo, esta deve ser totalmente reversível e feita de tal forma que não ponha em risco o valor probatório dos documentos. No caso de dados pessoais conservados para fins de arquivo de interesse público, os dados originais inalterados devem ser armazenados numa instalação protegida e ser feita cópia dos dados pessoais sob pseudónimo para o acesso dos investigadores, se desta maneira poderem ser satisfeitos os propósitos referidos.

Permitirá o RGPD conservar arquivos empresariais contendo dados pessoais?

Algumas empresas privadas conservam arquivos centenários, incluindo dados pessoais, que são verdadeiros tesouros para os historiadores. Será que os historiadores do futuro poderão aceder a fontes de arquivo semelhantes? Por outras palavras, será possível a conservação de arquivos empresariais que contenham dados pessoais ser aceite pelo RGPD? Não há uma resposta simples para essa questão.

Os documentos criados por organismos privados podem ser tratados para fins de arquivo de interesse público tal como os criados por organismos públicos. Tal tratamento, no entanto, apenas é qualificado como "fins de arquivo de interesse público" se for realizado por um organismo público ou privado que tenha "a obrigação legal de adquirir, preservar, avaliar, organizar, descrever, comunicar, promover, divulgar e fornecer acesso aos documentos de valor duradouro para o interesse público em geral." (considerando 158). Como é entendida a "obrigação legal", difere em países de direito românico-germânico e em países de direito anglo-saxónico.

Entidades que têm uma missão de investigação histórica, mas não têm a obrigação legal de adquirir e tratar arquivos, pode tratar arquivos empresariais que contenham dados pessoais para fins de investigação histórica. Tanto o princípio da "limitação da finalidade" e o de "limitação de conservação" (art.º 5 (1), alíneas b) e e)) permitem de fato derrogações não só para fins de arquivo de interesse público, mas também para propósitos de investigação histórica. Essas derrogações estão sujeitas à implementação de medidas adequadas a fim de salvaguardar os direitos e liberdades dos titulares dos dados. A interpretação de tais disposições tornar-se-á progressivamente mais clara, com as futuras decisões e orientações das Autoridades de Controle e do Conselho Europeu para a Proteção de Dados.

IV. DIREITOS DOS TITULARES DOS DADOS

6. O CERNE DA QUESTÃO: GARANTIR ÀS PESSOAS SINGULARES O CONTROLO SOBRE OS SEUS DADOS PESSOAIS

Um dos principais objetivos do RGPD é conceder às pessoas singulares o controle sobre seus dados pessoais. Por esta razão fornece um abrangente conjunto de direitos aos titulares tendo em vista os seus dados pessoais (o direito de saber que dados são tratados, e porquê, o direito ao acesso, ao apagamento, à transferência, etc.), que apenas permitem derrogações limitadas. Arquivar para fins de interesse público é motivo de derrogação à maioria dos direitos dos titulares de dados. Em duas situações "direito à informação" (art.º 14) e "direito ao esquecimento" (art.º 17), o RGPD introduz derrogações diretas ao arquivo para fins de interesse público. Noutros casos, permite aos Estados Membros fazê-lo. Como já foi referido, de facto, o art.º 89 permite os Estados Membros derrogar os direitos referidos nos artigos 15º, 16º, 18º, 19º, 20º e 21º. O que significa que os arquivistas em diferentes países europeus têm que obedecer a leis diferentes, considerando alguns direitos dos titulares de dados

Em qualquer destes casos, as derrogações não são absolutas mas sujeitas a garantias enunciadas no art.º 89(1), isto é, medidas técnicas e organizativas destinadas a reforçar o princípio da minimização de dados e a proteção dos direitos e garantias dos titulares dos dados. Além disso, os serviços de arquivo devem permitir aos titulares dos dados o maior controlo possível dos seus dados. Este princípio tem a maior relevância quando os arquivos conservam documentos pessoais de indivíduos vivos, que os doaram, venderam ou depositaram nos serviços de arquivo; ou quando os serviços de arquivo preservam entrevistas orais recolhidas durante os projetos da história oral. Os arquivos, contudo, não podem aceitar os pedidos dos indivíduos se isso implicar a violação da missão estatutária da preservação da integridade dos fundos, relacionados com a organização, descrição e comunicação ao público.

7. INFORMAÇÕES A FACULTAR QUANDO OS DADOS PESSOAIS NÃO SÃO RECOLHIDOS JUNTO DO TITULAR (ARTº. 14)

O RGPD declara que o responsável pelo tratamento de dados deve fornecer aos titulares dos dados certas informações sobre o tratamento que realiza. Isto aplica-se mesmo quando o responsável pelo tratamento não tenha obtido os dados pessoais diretamente do seu titular, como define o artigo 14. Essa é, regra geral, a situação dos arquivos que tratam documentos contendo informações pessoais que não recolheram, mas foram obtidos pela entidade que originou a sua retenção.

Contudo, o RGPD permite algumas derrogações, e uma refere-se aos arquivos. O artigo 14 declara que a obrigação de fornecer informação aos titulares quando os dados pessoais não são obtidos junto do seu titular, não se aplica quando "se comprove a impossibilidade de disponibilizar a informação, ou que o esforço envolvido seja desproporcionado, nomeadamente para o tratamento para fins de arquivo de interesse público, para fins de investigação científica ou histórica…". Nestes casos, o art.º 14, encoraja explicitamente os responsáveis pelo tratamento de dados a disponibilizar ao publico as informações sobre o tratamento de dados.

Quando os arquivos adquirem, organizam, descrevem, conservam e disponibilizam aos investigadores os fundos arquivísticos que contenham dados pessoais sobre um número indefinido de pessoas, na medida em que informar os titulares dos dados sobre este tratamento seria "impossível ou implicaria um esforço desproporcionado", a melhor linha de ação parece ser tornar disponível no sitio web as informações sobre o tratamento realizado pelo arquivo, para que o público, em geral, possa ter conhecimento.

Nalguns casos, pode ser realizado um esforço maior para informar os titulares dos dados em causa. Por exemplo, se for adquirido o arquivo de uma associação, de um partido político ou de um sindicato, que tratou apenas os dados pessoais dos seus associados, podemos aceitar que usem os seus canais de informação (boletins, sítios, listas de discussão, etc. .), a fim de informar os seus associados sobre o tratamento que o serviço de arquivo irá executar.

O art.º 14 inclui uma lista detalhada de elementos de informação que o responsável pelo tratamento deve fornecer aos titulares dos dados quando os dados pessoais não tenham sido obtidos através deles. Resumindo, os serviços de arquivo devem explicar em termos facilmente compreensíveis por alguém que nada saiba sobre arquivos, que tipo de tratamento de dados executam, porquê e qual é a base legal. Além disso, devem informar os titulares sobre a forma como podem aceder aos seus dados e explicar que os fundos arquivísticos acessíveis aos utilizadores, estão sujeitos às limitações legais sobre o acesso aos documentos contendo informações pessoais. Finalmente, se os titulares dos dados

contactarem os serviços de arquivo para solicitar informações sobre o tipo de tratamento realizado, os arquivistas devem estar preparados para esclarecer os titulares de dados disponibilizando todas as informações possíveis.

8. DIREITO DE ACESSO DO TITULAR DOS DADOS (ART.º 15)

Por regra, os titulares de dados têm o direito de obter a confirmação do responsável pelo tratamento, independentemente dos seus dados pessoais estarem a ser tratados ou não. Além disso, os titulares de dados têm também o direito de conhecer as finalidades do tratamento, as categorias de dados pessoais em causa e outras informações relativas ao tratamento dos seus dados pessoais.

Os arquivos processam grandes volumes de dados pessoais que foram recolhidos por outras entidades. Quando estas entidades transferem os seus documentos para um serviço de arquivo, devem também transferir os instrumentos de descrição de forma a permitir aos serviços de arquivo saber, entre outras coisas, os dados pessoais existentes nos documentos transferidos. No entanto, acontece frequentemente os serviços de arquivo receberem transferências sem instrumentos de descrição detalhados, mas apenas uma lista genérica de transferência. Como consequência, os arquivistas não podem saber quais os dados pessoais incluídos nos documentos transferidos. Além disso, os serviços de arquivo, recebem muitas vezes arquivos que perderam a ordem original e necessitam de um cuidadoso trabalho de organização para os recuperar.

Estas condições geram dificuldades objetivas na aplicação de alguns dos direitos dos titulares dos dados, expressos no RGPD. O RGPD reconhece isso e, como já mencionado, o artigo 89 prevê que a lei da União ou a legislação dos Estados membros possam introduzir derrogações aos direitos dos titulares dos dados.

Os arquivistas devem, portanto, verificar se a legislação nacional introduziu derrogações ao direito de acesso dos titulares dos dados fornecidos pelo artigo 15 do RGPD. Tais derrogações protegem os arquivistas de serem responsabilizados se não puderem cumprir integralmente os pedidos dos titulares de dados, para obter informações sobre o tratamento dos seus dados pessoais por um serviço de arquivo. No entanto, estas derrogações não isentam os arquivistas de fazerem o seu melhor para cumprir com estes pedidos dos titulares de dados.

Se um titular de dados contactar um serviço de arquivo para aceder aos seus dados pessoais, os arquivistas devem fornecer toda a assistência possível, explicando como pesquisar nos arquivos e quais os fundos de arquivo com maior probabilidade de conter dados pessoais, esclarecendo a forma de consultar os instrumentos de descrição e como fazer os pedidos para requisição dos documentos. Se o titular dos dados tiver dificuldades específicas em realizar pesquisas devido à idade avançada, ao nível de literacia ou a um impedimento físico, os serviços

de arquivo fornecerão assistência especial, na medida do possível, levando em conta as restrições com o número de funcionários disponíveis.

9. DIREITO DE RECTIFICAÇÃO (ART. 16)

O art.º 16 do RGPD estipula que os titulares dos dados têm o direito à retificação dos seus dados pessoais, se forem inexatos, e completar os que estejam incompletos. O responsável pelo tratamento tem que cumprir as solicitações do titular de dados "sem demora injustificada".

Os serviços de arquivo devem garantir a integridade dos arquivos, a fim de manter o valor probatório dos documentos. Isto é necessário para proteger os direitos dos titulares dos dados. Por exemplo, os arquivos da polícia de regimes repressivos geralmente incluem informações depreciativas sobre os adversários políticos. Manter a integridade de tais arquivos é necessário para permitir que titulares dos dados possam solicitar indemnização pela discriminação que sofreram às mãos do regime repressivo.

O RGPD permite conciliar a responsabilidade dos serviços de arquivo na manutenção da integridade de documentos, com o direito de os titulares dos dados completarem os seus dados pessoais incompletos. A retificação pode ser obtida "fornecendo uma declaração suplementar". Além disso, como já mencionado, o artigo 89.º prevê que a legislação da União ou do Estado Membro possa introduzir derrogações aos direitos dos titulares de dados previstos no artigo 16º.

Os serviços de arquivo devem facilitar ao titular dos dados o exercício do direito de atualizar, retificar ou complementar os seus dados “disponibilizando uma declaração suplementar” e garantir que os dados sejam mantidos de uma forma que permita que o material original permaneça separado e seja distinto de qualquer outra informação suplementar.

10. DIREITO DE APAGAMENTO DOS DADOS («DIREITO A SER ESQUECIDO») (ART.º 17)

O “direito a ser esquecido” dentro da UE foi declarado pela primeira vez na decisão histórica de 2014, do Tribunal de Justiça da União Europeia, no caso do Google Espanha. O Tribunal ordenou à Google Espanha para remover dos resultados de pesquisa dois relatórios sobre

insolvências relativamente ao um cidadão espanhol, Mario Costeja González. Os relatórios haviam sido legitimamente publicados por um jornal, em 1998, e continuavam a aparecer com destaque ao procurar o nome de Costeja. A decisão do Tribunal deixou intactos os arquivos analógicos e digitais do jornal. Somente se aplica ao resultado da pesquisa no Google do nome Costeja (as descrições permanecem recuperáveis ao usar outros termos de pesquisa). Segundo a decisão do Tribunal, os titulares dos dados podem solicitar que os dados pessoais que lhes digam respeito, (se forem inadequados, irrelevantes ou deixarem de ser relevantes) sejam ignorados pelos mecanismos de pesquisa, de modo a que esses dados não voltem a aparecer se for realizada uma pesquisa pelo nome.

A decisão do Tribunal de Justiça da UE no caso Google Espanha foi fundamentada na Diretiva 95/46 / CE a qual não incluem explicitamente o "direito a ser esquecido". Por contraste, o RGPD utiliza esta expressão no título do artigo 17º Direito de apagamento dos dados («direito a ser esquecido»)

Segundo o RGPD o direito de ser esquecido não se refere à desvinculação, mas ao real apagamento dos dados pessoais. O artigo 17º concede, de facto, o direito de os titulares dos dados obterem do responsável pelo tratamento de dados o apagamento de dados pessoais que lhe digam respeito, sem demora injustificada. Este direito pode ser aplicado quando "os dados pessoais não são mais necessários em relação aos fins para os quais foram recolhidos," ou "o titular dos dados retira o consentimento" ao seu tratamento, bem como noutras circunstâncias. Ao mesmo tempo, o direito a ser esquecido está sujeito a diferentes restrições, e não se aplica quando o tratamento for necessário para fins de arquivo de interesse público, caso o apagamento "seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento" (art.º 17 (3)).

O considerando 158 explica que as autoridades públicas e outros organismos que mantêm documentos de interesse público são serviços que têm "a obrigação legal" para tratar arquivos selecionados para conservação definitiva. O apagamento de dados pessoais existentes nos documentos de arquivo impossibilitaria, assim, que os arquivos cumprissem a missão que a lei lhes atribui. O direito de apagamento no artigo 17 da RGPD, portanto, não se aplica a documentos selecionados para conservação definitiva por serviços de arquivo que se enquadrem na definição de considerando 158. O direito de apagamento do artigo 17.º do RGPD não se aplica, portanto, a documentos selecionados para conservação permanente pelos serviços de arquivo que sejam abrangidos pela definição do considerando 158.

Ao mesmo tempo, os arquivistas devem lembrar-se que o direito a ser esquecido, como declarado pelo Tribunal de Justiça da UE (isto é, não o apagamento, mas a exclusão dos dados pessoais), pode ser imposto pelos serviços de arquivo sem prejuízo de sua missão.

Desligar, remover de um índice ou de qualquer outra forma impedir o uso de motores de busca para procurar nomes em documentos, de fato, não afeta a integridade dos documentos de arquivo, nem põe em risco a sua conservação permanente. Além disso, os serviços de arquivo podem prevenir as pesquisas por um nome num documento, mantendo–o recuperável através de chaves de pesquisa diferentes dos nomes de pessoas.

Em primeiro lugar, os serviços de arquivo devem abster-se de publicar documentos de arquivo em sistemas em linha ou disponibilizar instrumentos que contenham dados pessoais que possam comprometer a dignidade dos titulares dos dados. Além disso, sempre que publicarem documentos de arquivo ou instrumentos de descrição que contêm dados de pessoas vivas, têm que considerar - de acordo com a natureza dos dados pessoais - se não seria mais apropriado publicá-los em áreas de acesso restrito dos seus sítios, fora do alcance dos motores de busca.

Numa base casuística, os arquivistas avaliarão a melhor forma de equilibrar a sua obrigação legal de "descrever, comunicar, promover, divulgar e fornecer acesso a documentos de valor duradouro para o interesse público geral" (considerando 158) com o princípio da minimização dos dados (art.º 5), que exige sejam imitados ao que é necessário, relativamente às finalidades para as quais são tratados.

11. DIREITO À LIMITAÇÃO DO TRATAMENTO (ARTº. 18) E DIREITO DE OPOSIÇÃO (ARTº. 21)

O RGPD concede aos titulares de dados tanto o direito de obter a restrição de tratamento pelo responsável pelo tratamento, como o direito de se opor ao tratamento de dados pessoais relativos a cada um. Quais são as diferenças entre estes direitos e quais são as implicações práticas relevantes para os serviços de arquivo?

Estes direitos partilham o mesmo objetivo final de conceder aos indivíduos o controlo sobre o tratamento dos seus dados pessoais, mas aplicam-se em diferentes circunstâncias e têm diferentes consequências. O que mais importa aos arquivistas, é que o direito nacional pode introduzir derrogações de ambos os direitos, no caso do tratamento de dados pessoais para fins de arquivo de interesse público (art.º 89 (3)).

Nas circunstâncias específicas descritas no art.º 18 (1), os titulares dos dados têm o direito de obter a limitação do tratamento dos seus dados pessoais. De relevância chave para os serviços de arquivo é que esta limitação ao tratamento não obste à recolha de dados pessoais (art.º 18 (2)). Portanto, a conservação de documentos de arquivo, não pode ser prejudicada por estas limitações.

Além disso, os titulares de dados têm o direito de se opor ao tratamento de dados pessoais que lhes digam respeito, mesmo que o tratamento "seja necessário para o desempenho de uma tarefa realizada no interesse público". Nestes casos, "O responsável pelo tratamento cessa o tratamento dos dados pessoais, ((art.º 21 (1)). No entanto, o responsável pelo tratamento de dados pode continuar o tratamento de dados pessoais, se puder demonstrar "razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados" ((art.º 21 (1)). Esta disposição pode aplicar-se ao tratamento de arquivos de interesse público, mas os arquivistas não a podem dar como adquirido. É aconselhável que se mantenham informados sobre a forma como os tribunais interpretam esta disposição.

Em primeiro lugar, os arquivistas devem verificar se os legisladores nacionais fizeram uso da possibilidade de introduzir derrogações aos direitos de limitação do tratamento (art.º 18) e de oposição (art.º 21) e, neste caso, quais as salvaguardas que a lei estabeleceu quanto aos direitos e liberdades dos titulares de dados que os serviços de arquivo deverão considerar.
Se a legislação nacional não sugerir salvaguardas apropriadas, os serviços de arquivo terão de apreciar, caso a caso, a melhor forma de aplicar os princípios relativos ao tratamento de dados pessoais enumerados no art.º 5 do regulamento.

Finalmente, os arquivistas devem considerar que:

> Onde os dados pessoais sejam tratados para fins de investigação científica ou histórica ou para fins estatísticos nos termos do n.º 1 do artigo 89.º, o titular dos dados, por motivos relacionados com a sua situação particular, terá o direito de se opor ao tratamento de dados pessoais que lhe digam respeito, a menos que o tratamento seja necessário para o desempenho de uma tarefa realizada por razões de interesse público. (art.º 21 (6)).

Esta disposição pode ser relevante para os arquivistas que trabalham em museus ou outras entidades culturais ou organizações que conservam arquivos por razões de interesse público, mas não estão abrangidos pelos "fins de arquivo de interesse público", de acordo com a definição do considerando 158.

12. OBRIGAÇÃO DE NOTIFICAÇÃO DA RETIFICAÇÃO OU APAGAMENTO DOS DADOS PESSOAIS OU LIMITAÇÃO DO TRATAMENTO (ART. 19)

O RGPD determina que " O responsável pelo tratamento comunica a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados

pessoais ou limitação do tratamento a que se tenha procedido em conformidade (…) salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado.“ (Art.º 19)
Como já foi mencionado, o direito nacional pode introduzir derrogações aos direitos de retificação, apagamento ou restrição de tratamento, no caso do tratamento de dados pessoais para efeitos de arquivos de interesse público. Portanto, é improvável que os dados pessoais incluídos nos documentos de arquivo conservados pelos serviços de arquivo sejam objeto de retificação, eliminação ou restrição de processamento.

Além disso, o direito nacional também pode introduzir uma derrogação à obrigação de notificação, se os dados pessoais forem tratados para fins de arquivo de interesse público (artigo 89.º, n.º 3). Finalmente, os arquivistas devem considerar que um responsável pelo tratamento de dados deve cumprir a obrigação expressa pelo art.º 19, “a menos que isso seja impossível ou envolva um esforço desproporcional”, o que pode muito bem ser o caso dos serviços de arquivo.

13. DIREITO DE PORTABILIDADE DOS DADOS (ARTº 20)

O RGPD concede aos titulares dos dados “o direito de receber os dados pessoais que lhe digam respeito, e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática,” (art.º 20 (1)). Além disso, “o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre responsáveis pelo tratamento, sempre que tal seja tecnicamente possível. Os serviços de arquivo não recebem os dados pessoais incluídos nos fundos de arquivo que custodiam, diretamente do titular dos dados, exceto no caso de documentos pessoais. A maioria dos fundos arquivísticos tratados atualmente pelos serviços de arquivo estão num formato analógico, de modo que transmitir os dados pessoais dos titulares de dados num “formato legível por máquina” não é, em geral, “tecnicamente viável”.

Finalmente, os arquivistas devem estar cientes que a legislação nacional pode introduzir derrogações ao direito de portabilidade de dados se os dados pessoais forem tratados para fins de arquivo de interesse público (art.º 89 (3)).

V. TRATAMENTO DE CATEGORIAS DE DADOS QUE EXIGEM SALVAGUARDAS ESPECIAIS

14. TRATAMENTO DE CATEGORIAS ESPECIAIS DE DADOS PESSOAIS

O RGPD proporciona uma proteção especial a determinadas categorias de dados pessoais, cujo tratamento poderia criar riscos significativos aos direitos e liberdades fundamentais dos titulares de dados. Ele proíbe o

> tratamento de dados pessoais revelando origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, ou filiação sindical, e o tratamento de dados genéticos, dados biométricos com a finalidade de identificar unicamente uma pessoa singular, dados relativos a saúde ou dados relativos à vida sexual ou orientação sexual da pessoa singular (art.º 9 (1))

No entanto, o RGPD permite algumas derrogações a esta disposição. A proibição de tratamento desses dados sensíveis não se aplica nos casos em que "o tratamento for necessário para fins de arquivo de interesse público" e para a pesquisa histórica. Tal tratamento deve ser baseado na lei e deve ser "proporcional ao objetivo perseguido". Além disso, deve "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. (art.º 9(2) ponto (j))

Para a maior parte, as disposições do artigo 9º não são novas. A Diretiva 95/46 / CE já proibiu o tratamento de categorias especiais de dados pessoais, com algumas derrogações. O RGPD alargou as categorias de dados pessoais que merecem proteção especial, adicionando à lista que aparece no artigo 9º os "dados genéticos, dados biométricos com o objetivo de identificar uma pessoa de forma inequívoca"

De acordo com a legislação nacional dos Estados Membros da UE, os documentos que contêm categorias especiais de dados pessoais são excluídos do acesso por longos períodos, que vão desde algumas décadas a um século ou mais. Os arquivistas, portanto, já têm uma longa e bem-sucedida experiência na aplicação de leis que restringem o acesso a categorias especiais de dados pessoais.

15. TRATAMENTO DE DADOS PESSOAIS RELACIONADOS COM CONDENAÇÕES PENAIS E INFRAÇÕES (ARTº. 10)

O RGPD define regras muito rígidas em relação ao tratamento de dados pessoais respeitantes a condenações penais e crimes e não permite quaisquer exceções. O tratamento deste tipo de dados pessoais é possível "sob o controlo de uma autoridade pública ou se o tratamento for autorizado por disposições do direito da União ou de um Estado Membro. A lei deve prever "garantias adequadas para os direitos e liberdades dos titulares dos dados" (art.º 10).

Nos Estados Membros da UE, as leis nacionais determinam que após um determinado número de anos - geralmente 20 ou 30 anos - decisões judiciais, ficheiros judiciais e registos penais selecionados para conservação permanente sejam transferidos para o Arquivo Nacional ou para outras instituições arquivísticas. Estes serviços de arquivo tratam, portanto, grandes volumes de dados relacionados com condenações criminais: selecionam, transferem para os seus repositórios, organizam, descrevem e disponibilizam aos investigadores. Este tipo de tratamento é totalmente compatível com o RGPD porque é ditado pela lei e realizado por autoridades oficiais com garantias adequadas aos direitos e liberdades dos titulares de dados. Por exemplo, se a lei nacional restringir o acesso aos arquivos judiciais por determinado número de anos, os arquivistas aplicam cuidadosamente tais restrições. Se disponibilizarem em linha documentos de acesso livre, relacionados com condenações penais, e houver a possibilidade de os titulares dos dados ainda estarem vivos, os serviços de arquivo podem tomar medidas como sejam publicar esses documentos numa área de acesso restrito dos seus sítios ou editar nomes, em conformidade com o princípio fundamental de respeito e proteção da dignidade das pessoas.

Se um organismo público ou privado (por exemplo, uma universidade, fundação ou organização da sociedade civil) custodiar arquivos legais ou cópias de processos judiciais e decisões judiciais ou de outra forma recolher, preservar e disponibilizar aos investigadores documentos contendo dados pessoais, relativos a condenações e infrações penais (por exemplo: um centro académico especializado no estudo do terrorismo ou um arquivo comunitário criado por ativistas anti máfia), deve contactar a respetiva Autoridade de Proteção de Dados para obter instruções sobre as salvaguardas apropriadas para os direitos e liberdades dos titulares dos dados em questão.

VI. PROTECÇÃO DE DADOS

16. PROTECÇÃO DE DADOS DESDE A CONCEPÇÃO E POR DEFEITO (ARTIGO 25): O QUE SIGNIFICA NOS ARQUIVOS?

O Artigo 25 determina que quando se planeiam os meios para tratar dados pessoais, o responsável pelo tratamento de dados "aplica, 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". Isto é o que o RGPD refere como "proteção de dados *desde a conceção*".

Um dos princípios fundamentais da proteção de dados é a minimização dos dados. Na verdade, o Artigo 25 exige ainda que o responsável de tratamento de dados "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". (ênfase nosso).

O artigo 25 aplica-se especialmente ao desenvolvimento de novos sistemas de informação. Nos arquivos, isso pode envolver, por exemplo:

- Criação de um repositório digital;
- Criação de uma base de dados sobre registos de nascimento ou outros fundos contendo informação pessoal;
- Criação de um sistema de informação para gerir os serviços da sala de leitura;
- Criação de ferramentas para acesso em linha.

Os serviços de arquivo devem ter o artigo 25 em mente quando planeiam os diferentes tipos de atividades que normalmente executam, ou seja, avaliação, organização e descrição, fornecendo acesso e a comunicação dos arquivos.

Avaliação: Os serviços de arquivo adotam uma política de avaliação que limita a conservação permanente dos documentos que contêm dados pessoais, para além do que é realmente necessário, de acordo com sua missão. Colocam em prática o Artigo 25, elaborando cuidadosamente tabelas com prazos de conservação que definem o tipo de documentos que contêm dados pessoais e devem ser selecionados para conservação permanente. Para serviços de arquivo, as tabelas com prazos de conservação são o meio de demonstrar a conformidade com o Artigo 25.

Organização e descrição: Os serviços de arquivo reforçam o princípio da minimização de dados pessoais quando criam instrumentos de descrição. Quando organizam e descrevem um fundo de arquivo que inclui dados pessoais de indivíduos vivos, sobre saúde, vida sexual, opiniões políticas e outras categorias especiais de dados, ou dados relacionados com condenações criminais, os serviços de arquivo devem criar instrumentos de descrição que forneçam os nomes reais, para poder responder a possíveis pedidos dos titulares de dados e cumprir outros direitos dos titulares. Ao mesmo tempo, para as pesquisas em linha (caso a legislação nacional permita o acesso a tais registos), os serviços de arquivo podem criar uma outra versão dos instrumentos de descrição em que os nomes reais são substituídos por pseudónimos, se desta maneira puder cumprir a sua missão de fornecer acesso aos arquivos. Um programa para descrição arquivística que permita a criação de duas versões diferentes de um instrumento de descrição (um com os nomes reais e um com pseudónimos) é uma ferramenta para a conformidade com o art.º 25.

Disponibilizar acesso aos arquivos. Os serviços de arquivo são obrigados a garantir que o acesso aos documentos seja gerido de forma apropriada e que estejam em vigor proteções organizacionais e técnicas. Os serviços de arquivo têm uma longa história de gestão e comunicação dos seus documentos, por meio de procedimentos de controlo, como o pedido de registo do leitor, verificando se os arquivos solicitados estão disponíveis para consulta pública e limitando o número de documentos presentes na sala de leitura.
No ambiente eletrónico, as questões de acesso serão agravadas devido à escala, variedade e complexidade dos registos eletrónicos. Em muitos casos, grandes volumes de dados não podem ser verificados e confirmados manualmente antes do acesso e por isso as proteções e os controlos devem ser cada vez mais automatizados.

Atividades de supervisão e colaboração com produtores de arquivos. No espaço da UE, a natureza das relações entre as entidades produtoras e os serviços de arquivo mudam de um país para outro, de acordo com o setor público e o setor privado. Nalguns casos, os Arquivos do Estado têm a autoridade de supervisão, monitorização ou aconselhamento, mas noutros países isso não acontece.

Relevante para serviços de arquivo é a conceção de novos sistemas pelos órgãos públicos cujos documentos podem ser transferidos no futuro para os serviços de arquivo. O desafio pode estar na conceção de novos sistemas de informação que se esforçam para cumprir com o RGPD, onde o arquivo de interesse público não está incluído na fase inicial de planeamento. É importante, portanto, garantir que os serviços de arquivo estejam envolvidos na conceção e planeamento dos sistemas para garantir que, no momento apropriado, os registos podem ser exportados ou replicados para ingestão e transferência para um serviço de arquivo. Idealmente, o sistema de informação deveria automaticamente ter em consideração o destino final dos documentos.

17. SEGURANÇA DOS DADOS PESSOAIS (ARTIGO 32-34)

SEGURANÇA DO TRATAMENTO

Um princípio fundamental do RGPD é que o " responsável pelo tratamento e o subcontratante apliquem as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, " (Artigo 32). Este é o 'princípio da segurança'.

Isso exige que o responsável pelo tratamento e o subcontratante considerem a análise de risco, as políticas organizacionais e as medidas físicas e técnicas. Também devem ter em consideração os requisitos adicionais sobre a segurança do tratamento.

O responsável pelo tratamento e o subcontratante podem considerar o estado da arte e os custos de implementação, ao decidir as medidas a tomar, mas essas medidas devem ser apropriadas tanto às circunstâncias quanto ao risco apresentado pelo tratamento.

Estas medidas devem garantir a "confidencialidade, integridade e disponibilidade" dos sistemas e serviços e os dados pessoais que tratam. As medidas também devem permitir que o responsável pelo tratamento e o subcontratante consigam restabelecer o acesso e a disponibilidade dos dados pessoais em tempo útil, no caso de um incidente físico ou técnico.

O responsável pelo tratamento e o subcontratante também precisam de garantir que têm os meios apropriados implementados para testar a eficácia das suas medidas e realizar quaisquer melhorias necessárias.

TÉCNICAS DE GESTÃO DE RISCO

O RGPD não define as medidas de segurança que o responsável pelo tratamento e o subcontratante devem implementar. Exige que tenham um nível de segurança "adequado" aos riscos apresentados pelo tratamento. Antes de decidir quais as medidas apropriadas, precisam de avaliar o risco da sua informação, através uma metodologia formal de gestão de riscos.

VIOLAÇÃO DE DADOS PESSOAIS

O RGPD estabelece um procedimento de notificação de uma violação de dados pessoais à autoridade de controlo (artigo 33). Esta noção de violação significa “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” (Artigo 4(12)). Inclui violações resultantes de causas acidentais e deliberadas. Isto também significa que uma violação é mais do que uma simples perda de dados.

Quando a violação de dados pessoais for suscetível de resultar num risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento notificará o mais rapidamente possível a autoridade de supervisão competente da violação de dados pessoais e, se possível, no prazo máximo de 72 horas.

O subcontratante deve notificar sem demora o responsável pelo tratamento, após tomar conhecimento de uma violação de dados pessoais (Artigo 33 (2)).

O conteúdo da notificação é estabelecido pelo Artigo 33 (3) do RGPD.

ASSEGURAR O TRATAMENTO DE DADOS PESSOAIS NOS ARQUIVOS E ASSEGURAR O ACESSO NÃO AUTORIZADO AOS DADOS PESSOAIS GUARDADOS NOS ARQUIVOS

Os arquivistas são responsáveis pela segurança dos dados pessoais sob o seu cuidado e, de acordo com as práticas profissionais existentes, salvaguardam a integridade e autenticidade e protegem contra acesso não autorizado, alteração, perda, dano ou destruição.

Os documentos devem ser armazenados de forma segura para que a confidencialidade seja garantida em todos os momentos. O acesso só deve ser permitido aos que têm uma necessidade de conhecimento que possa ser satisfeita conforme a lei. A organização do arquivo e o princípio da proveniência não devem ser comprometidos pela separação entre documentos pessoais e não pessoais.

O nível de segurança deve ser adequado e proporcional à natureza dos dados e aos danos que possam resultar de uma violação da segurança. Isto deve refletir as normas dos profissionais e a utilização de técnicas de gestão de risco para avaliar a natureza, nível e impacto dos riscos e a tomada de medidas apropriadas para proteger os dados.

As medidas práticas de segurança a serem consideradas incluem a instalação de dispositivos de segurança física tais como alarmes de intrusão, restrições de acesso a áreas seguras, manutenção de um registo de visitantes e supervisão das suas atividades, na medida do possível. Os dados eletrónicos devem ser protegidos, por exemplo, através de programas contra vírus e cavalos de troia, e o acesso controlado por palavra passe apenas para utilizadores autorizados. Os dados pessoais devem ser transmitidos de forma segura: as ferramentas de encriptação devem ser usadas na transmissão segura de dados pessoais eletrónicos.

Embora os serviços de arquivo existam para conservar e fornecer acesso a documentos, não devem divulgar documentos que contenham dados pessoais, a menos que possam conciliar

os requisitos de investigação, histórica ou sobre evidências, com os direitos e liberdades fundamentais dos titulares de dados.

O QUE PODEM / DEVEM FAZER OS ARQUIVISTAS EM CASO DE VIOLAÇÃO DE DADOS?

No caso de uma violação grave decorrente do tratamento - seja de armazenamento, acesso, comunicação ... - de documentos, os serviços de arquivo devem considerar se a violação é suscetível de causar danos significativos aos interesses dos titulares vivos de dados. Em caso afirmativo, a notificação da violação deve ser considerada nos termos do artigo 34.º, n.º 3, alínea c), do Regulamento e entregue à autoridade de supervisão.

O artigo 34(1) declara: "Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada". No entanto, caso isso envolva um "esforço desproporcional" - o que, claro, pode existir quando ocorrer uma violação em relação a uma grande série arquivística contendo milhares de dados pessoais - art.º 34 (3) ponto (c) "é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz". Pode, por exemplo, ser um aviso no sítio Web ou uma comunicação por meio de uma lista de correio eletrónico.

As violações de segurança devem ser registadas e investigadas e a equipa deve ser incentivada a informar e responder a incidentes de segurança.

18. AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS E CONSULTA PRÉVIA (ARTIGOS 35-36)

O RGPD exige que os responsáveis pelo tratamento realizem uma avaliação de impacto da proteção de dados (AIPD) antes do tratamento, quando o tratamento "for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (Artigo 35 (1)). Os AIPD's são ferramentas importantes para a responsabilização, pois ajudam o responsável pelo tratamento não apenas cumprir os requisitos do RGPD, mas também demonstrar a "conformidade com o Regulamento"[3]

[3] Grupo de trabalho do artigo 29. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248 rev.01, 13 Oct. 2017.*

O QUE É UMA AVALIAÇÃO DE IMPACTO DA PROTEÇÃO DE DADOS (AIPD)?

O objetivo de uma AIPD é identificar e avaliar o risco que poderia surgir para o indivíduo (como cidadão, cliente, paciente, etc.) de um novo tipo de tratamento. O Grupo de Trabalho do Artigo 29 definiu AIPD como: "um processo concebido para descrever o tratamento, avaliar a sua necessidade e proporcionalidade e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares resultantes do tratamento de dados pessoais, avaliando-os e determinando as medidas para os resolver."[4]

QUANDO É (OU NÃO É) EXIGIDA UMA AVALIAÇÃO DE IMPACTO DE PROTEÇÃO DE DADOS?

Quando as novas tecnologias para o tratamento de dados pessoais ou um novo tipo de operação de tratamento são introduzidas, como primeiro passo, deve ser realizada uma avaliação de risco. Se a natureza dos dados ou o modo de tratamento for suscetível de criar um alto risco para os titulares de dados, é necessário uma AIPD.

Uma AIPD é dispensada quando o tratamento *não é* suscetível de criar riscos aos titulares de dados e quando é semelhante às atividades de tratamento anteriores para as quais já foi executada uma AIPD. O RGPD deixa claro, de fato, que "Se um conjunto de operações de tratamento apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação" (Artigo 35 (1)).

Aguarda-se que as Autoridades de Proteção de Dados publiquem uma lista do tipo de operações de tratamento que estão sujeitas à exigência de uma avaliação de impacto de proteção de dados e também as que estão dispensadas.

O QUE SIGNIFICA "ALTO RISCO?"

O RGPD não define exatamente o tipo de tratamento que acarreta um alto risco. No entanto, fornece alguns exemplos, incluindo um que pode muito bem dizer respeito a serviços de arquivo, nomeadamente o tratamento de dados pessoais relativos a condenações penais ou a dados pessoais sensíveis (ou seja, dados reveladores de origem racial ou étnica, opiniões políticas, religiosas ou crenças filosóficas ou filiação sindical, dados genéticos, dados biométricos e dados relativos à saúde ou à vida sexual ou orientação sexual de uma pessoa) (artigo 35.º, n.º 3, alínea b)). Além disso, ao avaliar se o tratamento pode resultar num risco elevado para os direitos e liberdades dos titulares de dados, os serviços de arquivo devem

[4] Ibidem

considerar se os dados pessoais se referem a titulares de dados vulneráveis, como por exemplo pessoas com doenças mentais (considerando 75).

QUANDO TÊM OS SERVIÇOS DE ARQUIVO REALIZAR AIPD'S?

Quando os serviços de arquivo decidirem digitalizar materiais ou criar instrumentos de descrição digitais para dados pessoais, destinados a disponibilizar localmente ou colocar em linha pode ser necessária uma AIPD. Este poderá certamente ser o caso ao tratarem documentos de arquivo contendo dados pessoais confidenciais, como processos médicos, processos de tribunais criminais ou processos individuais de reclusos.

A AIPD garantirá que o serviço de arquivo considerou os aspetos de proteção e privacidade de dados do projeto ou trabalho proposto e pode satisfazer ou demonstrar a uma Autoridade de Proteção de Dados que essas preocupações foram abordadas ou incorporadas na conceção ou na implementação.

O QUE TEM QUE SER FEITO?

No decorrer da avaliação de impacto de proteção de dados, a operação de planeamento do tratamento e o interesse legítimo da operação devem ser descritos de forma sistemática. Como passo seguinte, a proporcionalidade e a necessidade da operação prevista devem ser avaliadas. Em seguida, os riscos para os direitos e liberdades da pessoa em causa têm de ser avaliados, seguindo-se um plano detalhado das medidas que serão tomadas para gerir os riscos. Quando a operação de tratamento está em execução, deve ser monitorizada regularmente e a AIPD deve ser adaptada quando ocorram mudanças.

Algumas Autoridades de Proteção de Dados publicaram ferramentas para ajudar os responsáveis pelo tratamento realizar uma AIPD. Veja-se, por exemplo, o programa de acesso livre produzido pela APD francesa: https://www.cnil.fr/en/cnil-releases-free-software-pia-tool-help-data-controllers-carryout-data-protection-impact

QUANDO DEVE SER INFORMADA A AUTORIDADE DE SUPERVISÃO?

A autoridade de supervisão (ou seja, a Autoridade de Proteção de Dados) deve ser consultada se a avaliação de impacto da proteção de dados indicar que "o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco. (Art.º 36). Se a autoridade de supervisão considerar que o tratamento planeado não está em conformidade com o Regulamento ou se as medidas previstas para mitigar o risco não forem suficientes, deve fornecer aconselhamento escrito ao responsável pelo tratamento.

VIII. MEDIDAS DE TRANSPARÊNCIA E PROMOÇÃO DE CONFORMIDADE

19. REGISTOS DAS ATIVIDADES DE TRATAMENTO (ARTIGO 30)

O artigo 30 estabelece: “Cada responsável pelo tratamento e, sendo caso disso, o seu representante conserva um registo de todas as atividades de tratamento sob a sua responsabilidade”.
O registo de atividades de tratamento - também muitas vezes chamado de "registo de tratamento (de dados)" - é um instrumento muito útil para apoiar uma análise das implicações de qualquer tratamento existente ou planeado. O registo facilita a avaliação factual do risco das atividades de tratamento executadas por um responsável pelo tratamento ou pelo subcontratante, sobre os direitos dos indivíduos, e a identificação e implementação de medidas de segurança apropriadas para proteger dados pessoais - ambos componentes-chave do princípio de responsabilidade contido no RGPD.

Este registo deve ser feito por escrito (incluindo em formato eletrónico), de forma clara e inteligível. Uma vez que as "atividades de tratamento" no contexto do RGPD dizem respeito a operações realizadas com dados pessoais relativos a uma pessoa singular identificada ou identificável, apenas estão em causa atividades relacionadas com dados pessoais.

A obrigação de manter um registo das atividades de tratamento não se aplica a organizações dotadas com menos de 250 trabalhadores, a menos que se encontrem na posição de executar um tratamento que possa resultar num risco (não apenas alto risco) para os direitos da empresa, titulares de dados, ou se estiverem a tratar dados pessoais numa base não ocasional ou se tenderem a tratar categorias especiais de dados ao abrigo do n.º 1 do artigo 9.º (ou seja, dados relativos à saúde, à vida sexual, às origens étnicas, opiniões políticas e outro tipo de informações sensíveis) ou dados relativos a condenações penais nos termos do artigo 10º. Se uma dessas circunstâncias se aplicar - o que, na verdade, é o caso da maioria, para não dizer todas as instituições arquivísticas – a organização é obrigada a manter o registo de atividades de tratamento.

As organizações e os seus representantes devem fornecer esse registo à Autoridade de Proteção de Dados (APD), mediante solicitação.

QUE INFORMAÇÕES DEVE TER O REGISTO DE TRATAMENTO DE ATIVIDADES?

O registo deve conter informações específicas sobre cada atividade de tratamento realizada

- **nome e dados de contacto** do:
  - serviço de arquivo, ou seu representante;
  - se necessário, outras organizações com as quais o serviço de arquivo estabeleceu objetivos e formas de tratamento comuns;
  - o encarregado pela proteção de dados (EPD), se tiver sido nomeado pelo serviço de arquivo;

- Os **fins** pelos quais o serviço de arquivo trata dados pessoais

  Da mesma forma que a "pesquisa histórica", já foi reconhecida como uma "finalidade" no passado, "arquivar (propósitos) no interesse público" deveria ser suficiente como objetivo. Não é claro se a associação "de interesse público" deve ou não ser adicionada para fundamentar a informação.

- Uma descrição das **categorias de pessoas** das quais os serviços de arquivo tratam dados
  Por exemplo: estudantes, recrutas, réus, pacientes,

- Uma descrição das **categorias de dados pessoais**. Identificar também os dados "sensíveis" tais como informações sobre saúde e informações judiciais
  Por exemplo: atividades profissionais, transações financeiras, informações judiciais sobre condenações criminais e sentenças, dados a partir dos quais as opiniões políticas possam ser induzidas, …

- A **data em que os dados devem ser eliminados** (se conhecida).
  Atenção: Do ponto de vista dos serviços de arquivo, é de particular importância ressalvar aos produtores que o 'período de retenção' não deve ser confundido com 'eliminação' de informação, e que devem agir em conformidade com a Lei dos Arquivos e estipulado pelos prazos de conservação. De fato os dados arquivados no interesse público nunca devem ser destruídos.

- As **categorias de destinatários** para quem o serviço de arquivo fornece dados pessoais.
  Note-se que referimos "categorias de destinatários": isto é, por exemplo, «universidades e instituições de pesquisa», «investigadores individuais»…

- O serviço de arquivo partilha dados com um **país estrangeiro ou uma organização internacional fora da UE**? Então deve indicar isso no registo.

- A descrição geral das **medidas técnicas e organizacionais** tomadas para proteger os dados pessoais que o serviço de arquivo está a tratar: descrição da tecnologia, aplicações e programas utilizados para o tratamento de dados, ou seja, que tipo de 'proteção de dados por conceção ou por defeito' foi usado.

> As organizações devem considerar este registo como uma ferramenta interna para ajudar a implementar o RGPD. O registo pode conter qualquer informação adicional que seja considerada importante pelo encarregado de proteção de dados (EPD) em função das atividades realizadas, por exemplo, indicação de base legal para o tratamento de dados ou uma visão geral de todas as violações referentes a dados pessoais.

O tratamento por subcontratante

Observação: se um serviço de arquivo subcontratar noutras entidades o tratamento de dados pessoais em seu nome, deve ser assinado um "contrato de tratamento de dados" com essas organizações. Para estabelecer este contrato, o serviço de arquivo garante que terceiros não usam ou tratam dados pessoais para os seus próprios fins.

Apenas agentes que garantam plenamente o cumprimento dos requisitos legais devem ser selecionados. Os serviços de arquivo que decidam externalizar as atividades de tratamento a um subcontratante, permanecem totalmente responsáveis por cumprir os requisitos do RGPD.

ALGUNS MODELOS DE REGISTO DE ATIVIDADES DE TRATAMENTO DISPONÍVEIS EM LINHA, POR EXEMPLO:

Modelo oferecido pela APD belga, disponível em francês e holandês: https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement

A APD francesa publicou dois modelos de registos, um mais complexo e um mais simples : https://www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique

A Autoridade Europeia para a Proteção de Dados (ou seja, a Autoridade de Proteção de Dados independente da UE) publicou um modelo de registo: https://edps.europa.eu/data-protection/ourwork/publications/other-documents/register-template-0_en

Os estados membros podem criar um registo de aplicação das atividades de tratamento, cujo uso é obrigatório para os serviços públicos. A Bélgica é um caso em questão. A Bélgica é disso, um exemplo.

20. ENCARREGADO DE PROTEÇÃO DE DADOS (ARTIGO 37): PRECISAM OS ARQUIVOS DE DESIGNAR ALGUÉM?

O encarregado pela proteção de dados (EPD) auxilia o responsável pelo tratamento ou o subcontratante em todas as questões relacionadas com a proteção de dados pessoais. As suas principais tarefas são:

- informar e aconselhar o responsável pelo tratamento e os empregados que realizam o tratamento, das suas obrigações ao abrigo do RGPD e das normas nacionais de proteção de dados.
- monitorizar a conformidade com o RGPD
- Prestar aconselhamento sobre a avaliação do impacto da proteção de dados (AIPD)
- cooperar com a autoridade de supervisão;

O RGPD introduziu a obrigação de designar um EPD para autoridades públicas e entidades privadas que realizam certos tipos de atividades de tratamento. Todas as autoridades públicas devem ter um EPD, mas isso não significa que cada serviço de arquivo no setor público nomeie um. Na maioria dos casos, a entidade hierarquicamente superior pode indicar um EPD, cujas responsabilidades se estendem ao serviço de arquivo. Por exemplo, um município pode ter um EPD responsável por monitorizar a conformidade do RGPD e aconselhar todos as unidades do município, incluindo os Arquivos Municipais.

As entidades do setor privado devem nomear um EPD se:

- A sua atividade principal requer uma monitorização regular e sistemática em grande escala dos titulares de dados.
- A sua atividade principal consiste no tratamento de dados pessoais revelando origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, ou filiação a sindicatos, e o tratamento de dados genéticos, dados biométricos com a finalidade de identificar unicamente uma pessoa física, dados relativos a saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa singular, ou dados pessoais relacionados com condenações penais e infrações.

É pouco provável que fundações, museus, bibliotecas, associações culturais e outros órgãos do setor privado que possuem arquivos realizem a "monitorização regular e sistemática de dados em larga escala". Por outro lado, é inteiramente possível que a sua atividade principal consista no tratamento de dados pessoais sensíveis.

De fato existem fundações, arquivos comunitários e outras entidades do setor privado especializadas no tratamento de arquivos produzidos por ONG's e organizações de direitos humanos no curso de suas atividades, que podem incluir, por exemplo, dados pessoais que revelam a origem racial ou étnica, de pessoas vítimas de atos de intolerância. Como já foi mencionado, existem centros de investigação especializados no estudo do terrorismo ou arquivos comunitários criados por ativistas anti máfia que tratam dados pessoais relacionados com condenações penais e ofensas. Podem existir arquivos comunitários que contenham arquivos produzidos por organizações feministas que ajudaram mulheres vítimas de violência e que incluem todos os tipos de dados pessoais altamente sensíveis.

Em todos estes casos deste tipo, os organismos privados que tratam arquivos devem nomear um EPD. "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. "(Artigo 37.6) As pequenas entidades podem partilhar o mesmo EPD com outras entidades semelhantes. É muito aconselhável que pequenas entidades que tratem arquivos para "fins de arquivo de interesse público" ou para fins de investigação, partilhem o mesmo EPD com outras entidades semelhantes para que o EPD possa desenvolver uma especialização especifica no tipo de tratamento de dados pessoais que realizam.

ANEXOS

GLOSSÁRIO

Arquivo: O RGPD não define o termo "arquivo". Nas presentes orientações, "arquivo" é usado para referir ao conjunto dos documentos criados e recebidos por uma pessoa, família ou organização, pública ou privada, no exercício da sua atividade, e selecionado para conservação definitiva. Em algumas línguas europeias, o mesmo termo é usado para se referir tanto aos documentos ativos como os selecionados para conservação definitiva. Neste texto, o termo arquivo é usado apenas para referir a documentos selecionados para conservação definitiva.

Grupo de Trabalho do Artigo 29.º: Grupo de trabalho criado nos termos do art.º 29 da Diretiva 95/46 da EU. O grupo de trabalho foi composto por representantes das autoridades responsáveis pela proteção de dados nos Estados Membros, a Autoridade Europeia para a Proteção de Dados e um representante da Comissão Europeia. O grupo de trabalho deixou de existir em 25 maio de 2018, quando foi substituído pelo Conselho Europeu de Proteção de Dados (CEPD).

Responsável pelo tratamento: a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais (RGPD, art.º 4).

Pessoa singular: a pessoa cujos dados pessoais estão sujeitos a tratamento.

Autoridade de Proteção de Dados (APD): Ver Autoridade de Supervisão

Encarregado pela proteção de dados (EPD) : Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações relacionadas com a proteção de dados pessoais.. O RGPD introduziu a obrigação de designar um EPD para as autoridades públicas e as entidades privadas que realizam certos tipos de atividades de tratamento.

Conselho Europeu de Proteção de Dados (CEPD): o RGPD substituiu o grupo de trabalho do artigo 29 pelo CEPD. Ao contrário de seu antecessor, o CEPD tem o estatuto de um organismo da UE com personalidade jurídica dotado de um secretariado independente. Tem amplos poderes para decidir os litígios entre as autoridades nacionais de supervisão

e dar conselhos e orientações sobre conceitos-chave do RGPD. É composto pela APD dos Estados Membros e da Autoridade Europeia para a Proteção de Dados. A Comissão tem o direito de participar nas suas reuniões.

Autoridade Europeia para a Proteção de Dados (AEPD): A AEPD é um órgão independente da UE responsável pelo acompanhamento da aplicação das regras de proteção de dados entre as instituições europeias e para investigação de reclamações.

Dados pessoais: "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular" (RGPD art.º4).

Os arquivistas devem ter em mente que o RGPD protege apenas os dados pessoais de pessoas vivas. No entanto, a legislação nacional também pode prever a proteção de dados pessoais de pessoas falecidas.

Tratamento : "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (RGPD, art.º 4).

Os arquivistas devem ter em conta que atividades como a seleção para conservação definitiva de documentos que contenham dados pessoais, transferência para uma instituição de arquivo, organização, descrição e disponibilização para os investigadores são todas consideradas pelo RGPD como "tratamento de dados pessoais".

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" (RGPD, art.º 4).

Esta definição é de relevância fundamental para arquivistas. Isso implica que, se os dados pessoais foram selecionados para conservação definitiva e forem custodiados de uma instituição de arquivo, os arquivistas têm de proteger sua integridade. Entre os princípios relativos ao tratamento de dados pessoais, o regulamento inclui de fato "integridade e confidencialidade" (art.º 5). A perda ou alteração acidental de tais registos violaria não só

a ética arquivística, mas também a RGPD. O mesmo é verdadeiro se arquivistas permitirem a divulgação não autorizada ou o acesso a dados pessoais.

Subcontratante: "uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes" (RGPD, art.º 4).

Pseudonimização: "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;" (RGPD, art.º 4).

É importante notar que o RGPD sugere a possibilidade de pseudonimização de dados pessoais conservados para fins de arquivo de interesse público ou para fins de pesquisa histórica e não menciona "anonimização". Ao contrário da anonimização, a pseudonimização preserva a correlação de diferentes dados relativos a uma pessoa, assim como a relação entre os diferentes registos de dados. Os dados pessoais pseudonimizados mantêm a sua natureza de dados pessoais e, portanto, estão sujeitos às disposições do Regulamento.

Categorias especiais de dados pessoais: dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa (RGPD, art.º 9). Este tipo de dados são muitas vezes referidos como "dados pessoais sensíveis".

Autoridade de supervisão: O Art.º 51 do RGPD estipula que cada Estado Membro deve prever uma ou mais autoridades públicas independentes, que serão responsáveis pelo acompanhamento da aplicação do regulamento. Estas autoridades têm nomes diferentes em países diferentes (por exemplo, na Finlândia "Gabinete do Provedor de Proteção de Dados", na França "Comissão Nacional da Informática e das Liberdades", na Irlanda "Comissário para a Proteção de Dados", na Itália "Garante para a proteção de dados pessoais"), e são comumente conhecidos como autoridades de proteção de dados (APD).

ONDE PROCURAR MAIS ORIENTAÇÃO

- A Comissão Europeia tem uma seção em seu sítio "Proteção de dados. Regras para a proteção de dados pessoais dentro e fora da UE" https://ec.europa.eu/info/law/law-topic/data-protection_en onde publicou algumas perguntas frequentes sobre o RGPD, por exemplo, que são dados pessoais? O que constitui o tratamento de dados? O que são Autoridades de Proteção de Dados (APD), etc. A informação é destinada a leitores que não têm nenhum conhecimento prévio sobre o RGPD. Atualmente, só está disponível em língua inglesa.

- Manual sobre a lei Europeia de proteção de dados, edição 2018 - http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law.
  O manual foi elaborado pela Agência Europeia dos Direitos Fundamentais (FRA), com o Conselho da Europa (em conjunto com a Secretaria do Tribunal Europeu dos Direitos Humanos) e da Autoridade Europeia para a Proteção de Dados. Descreve tanto a lei de proteção de dados da União Europeia (UE) como do Conselho da Europa (CoE) e inclui jurisprudência selecionada do Tribunal Europeu dos Direitos do Homem (TEDH) e do Tribunal de Justiça da União Europeia (TJUE).

- O Conselho Europeu de Proteção de Dados (EDPB) vai publicar diretrizes, recomendações e boas práticas. Assim, será útil ter em atenção este sítio https://edpb.europa.eu/edpb_en website, que está em todas as línguas da UE (embora, no momento, vários documentos apenas estejam disponíveis em língua inglesa). No seu primeiro dia de existência, o EDPB aprovou as diretrizes produzidas por seu antecessor, o Grupo de Trabalho do artigo 29.

- O Grupo de Trabalho do artigo 29 (que deixou de existir em 25 de Maio, 2018) publicou nove diretrizes e outros documentos sobre a implementação do RGPD, visando contribuir para uma interpretação uniforme e aplicação pelos diferentes APD e os governos em toda a UE. O Conselho Europeu de Proteção de Dados (EDPB) aprovou todos esses documentos disponibilizados em seu sitio https://edpb.europa.eu/edpb_en
  - *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (wp251rev.01), 13-02-2018
  - *Guidelines on Consent under Regulation 2016/679* (wp259), 24-01-2018, [adopted, but still to be finalized]

- *Guidelines on Data Protection Impact Assessment (DPIA) on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (wp248rev.01) 13-10-2017
- *Guidelines on Data Protection Officers ('DPOs')* (wp243rev.01), 30-10-2017
- *Guidelines on Personal data breach notification under Regulation 2016/679* (wp250rev.01), 13-02-2018
- *Guidelines on the application and setting of administrative fines* (wp253). Now including available language versions, 13-02-2018
- *Guidelines on the Lead Supervisory Authority* (wp244rev.01), 31-10-2017
- *Guidelines on the right to "data portability"* (wp242rev.01), 27-10-2017
- *Guidelines on Transparency under Regulation 2016/679* (wp260), 24-01-2018 [adopted, but still to be finalized]
- *Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*, 19–04-2018.

- As Autoridades de Proteção de Dados dos Estados Membros da UE publicam material informativo, como folhetos, folhas de informação, infográficos, traduções do artigo Diretrizes 29.º, para explicar os novos direitos dos cidadãos e para ajudar as administrações públicas e as pequenas e médias empresas a cumprir com o RGPD. Confirme o sítio da sua Autoridade de Proteção de Dados! As suas coordenadas podem ser encontradas em https://ec.europa.eu/justice/article-29/structure/data-protectionauthorities/index_en.htm

- O Supervisor Europeu de Proteção de Dados (SEPD) tem uma *Glossário* (em língua Inglesa, Francesa e Alemã) com mais de 70 entradas no seu sítio: https://edps.europa.eu/dataprotection/data-protection/glossary_en.
  Além disso disponibilizou em acesso livre a uma Biblioteca de Referência (https://edps.europa.eu/data-protection/data-protection/referencelibrary_en) e outros materiais informativos, principalmente destinados a orientar as instituições da UE na execução do RGPD, mas que pode ser útil para entidades públicas e privadas nacionais.

- Os Arquivos Nacionais do Reino Unido, em conjunto com as orientações de política governamental sobre arquivo e a Associação de Arquivos e Documentação, preparou uma *Guia para o arquivo de dados pessoais*, e disponibilizou gratuitamente no seu sítio. Pode ser uma leitura útil também para arquivistas de outros Estados membros, desde que tenham em consideração que este Guia é específico para o sistema legal britânico.
  http://www.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf