ESCOLA SUPERIOR DE ENFERMAGEM DO PORTO

MANUAL DE BOAS PRÁTICAS DE PROTEÇÃO DE DADOS

2024

Edição: 1

Índice

Introdução

Considerando o Plano de implementação do RGPD que a ESEP tem vindo a desenvolver, e no âmbito da colaboração da equipa que atualmente integra o Encarregado de Proteção de Dados, foi elaborado um manual de boas práticas que condensa um conjunto de entendimentos práticos, de formulação simples e acessível, que concernem à aplicação do Regulamento Geral de Proteção de Dados aos principais e específicos processos e âmbitos de atuação da ESEP, nomeadamente nas áreas de ensino e investigação.

Este manual vem, assim, dar resposta a uma necessidade sentida na comunidade académica da ESEP de um enquadramento concetual que torne mais fácil a interpretação e a aplicação prática deste normativo. A ESEP tem centrado a sua preocupação com a matéria de proteção de dados, não só na forma como a aplica aos seus discentes, docentes e pessoal técnico-administrativo, como também, na sua aplicação aos contextos de ensino clínico e de investigação.

A organização deste manual obedece a uma estrutura simples que permite, num primeiro âmbito, o engajamento com os conceitos básicos do RGPD, onde é feita uma abordagem aos tipos de dados pessoais e às suas categorias, após o que se define o âmbito de intervenção e responsabilidade dos diferentes sujeitos do RGPD e, por conseguinte, são apresentados os fundamentos de licitude, regras de tratamento e as medidas técnicas que podemos implementar para elevar os níveis de proteção.

1. Conceitos de Proteção de Dados

Por forma a dotarmos o nosso público-alvo sobre a proteção de dados e a sua essência, assim sendo, é importante iniciarmos pelo elemento basilar:

Dado pessoal, são informações relativas a uma pessoa singular, viva, identificada ou identificável. Olhando à definição estabelecida no RGPD *"«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»);*

- Explicando detalhadamente:

A definição à luz do parecer 4/2007[1] do GT do artigo 29.º tem 3 blocos centrais, devidamente sublinhados em cima, tal como a diretiva 95/46/CE o RGPD apresenta-nos uma definição ampla com vista a conseguir preencher o maior número de situações;

O que, por conseguinte, originou que várias situações possam ser enquadráveis com o seu conceito basilar, ajudando desta forma o aplicador a esclarecer se estamos ou não no âmbito de um dado pessoal.

A forma mais simples que temos de proceder à interpretação do conceito é olhar efetivamente para o seu desiderato, como tal, e como supramencionado, trata-se de **uma informação** e aqui referimo-nos a qualquer informação, repare-se que a própria definição estabelece os exemplos adequados para demonstrar a diversidade de informação que vai desde o **nome** do titular dos dados (aqui pessoa singular) até ao mais elementar elemento de especificidade de identidade física ou fisiológica do sujeito. Tudo posto, um dado pessoal (nada mais) é do que alguma "pista" que possa ajudar a proceder a identificação do seu "proprietário".

É importante esclarecer que esta informação poderá ser tida em qualquer formato, não importa se é manuscrito ou digital, e aqui não podemos esquecer os formatos áudio, fotográficos ou até gráficos, independentemente se se encontra em dispositivos de armazenamentos atuais ou

[1] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf, definição dada à luz da diretiva 95/46/CE, mas que no seu objeto se aplica ao conceito explorado pelo RGPD e que aqui aproveitamos;

rudimentares, tudo o que sirva para estabelecer uma relação com o individuo é sem dúvida um ponto de partida para o (re)conhecimento do seu proprietário[2];

Além destes marcadores mais genéricos, temos alguns bem mais específicos que deverão ser tidos em conta por parte do nosso público-alvo que são os dados pessoais resultantes de marcadores genéricos mencionados na própria definição.

Sendo o primeiro elemento a "**informação**", será o segundo elemento da definição a "**relativa a**" em termos latos, podemos dizer que este é o elemento conector entre a informação e a quem é que a mesma diz respeito, já o GT29 se manifestou e esclareceu esta parte da definição[3], quando nos indica "*que os dados se referem a uma pessoa se se referirem à identidade, características ou comportamentos de uma pessoa ou se tal informação for utilizada para determinar ou influenciar a forma como essa pessoa é tratada e avaliada*",

O terceiro elemento da definição, é o facto de com essa **informação a pessoa singular (titular dos dados) possa ser identificada ou identificável**, ora por outras palavras, quando a informação diretamente ou indiretamente possa levar à descoberta da pessoa singular que lhe diz respeito, *"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".*

De forma resumida, podemos dizer que, não só, mas também, são dados pessoais, de acordo com a própria definição, 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, e aqui enquadramos obviamente o e-mail, o endereço postal, por exemplo: a matrícula do veículo, o IP de um computador, etc...

[2] Se virmos a jurisprudência do TJUE, no Acórdão do Tribunal de Justiça Europeu C-101/2001de 6.11.2003 (Lindqvist), §24: O conceito abrange claramente o nome de uma pessoa em conjunto com o seu número de telefone ou informação sobre as suas condições de trabalho ou tempos livres"

[3] Documento do Grupo de Trabalho, nº WP 105: "Documento de trabalho sobre questões relativas à proteção de dados no âmbito da tecnologia RFID", adotado em 19.1.2005, p. 8

Posto isto, e regressando ao ponto de partida**, dados pessoais** são informação relativa a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa.

Quanto aos **dados de saúde**, por inerência do público-alvo este será essencialmente a grande matéria-prima de trabalho para a prossecução da sua finalidade, a de concluir com sucesso o trabalho para o qual se propõem a cumprir.

O RGPD, estipula uma definição para **Dados relativos à saúde**, *dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde*[4]. No entanto e por forma a explicitar melhor a situação e olhando ao considerando 53 são uma categoria de dados que necessita de uma salvaguarda maior uma vez que são dados de categorias especiais. Explicando, dados de categoria especial são dados que devido à sua natureza carecem de cuidados acrescidos para que os mesmos possam ser sujeitos a tratamento por parte do operador. Olhando à enumeração legal que se consagra no artigo 9.º n.º 1 "*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".*

Por último mas não menos importante, trata-se da definição de **tratamento**, prevista e esclarecida no artigo 4.º n.º 2 do RGPD, estabelecendo que por **tratamento**, devemos entender como, *" 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;"*. Assim sendo e da leitura da definição devido à sua amplitude, qualquer operação que seja feita com um dado pessoal, é considerada uma situação de tratamento.

[4] Artigo 4.º n.º 15 RGPD;

Ora, para os Estudantes/Investigadores é importante que entendam, que "*qualquer coisa*" que é feita com um dado ou um conjunto de dados, cai numa operação de tratamento e como tal, devem estar habilitados à prática dessa operação.

Após procedermos à abordagem de alguns conceitos basilares para a compreensão da temática, torna-se necessário realizar uma apresentação aos papeis que podem ser desempenhados à luz do RGPD, e aqui iremos abordar como podem ser os Estudantes, a própria ESEP e os utentes/clientes, classificados enquanto sujeitos deste regulamento;

Aqui destacamos os papeis de **Responsável pelo Tratamento (RT)**, trata-se de uma 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. O Responsável pelo tratamento é por isso, alguém que define as finalidades e os meios de tratamento de dados pessoais, isto é, o Responsável pelo tratamento, pode ser o Estudante, que tem de trabalhar um certo tema que se propôs a trabalhar para obter o grau ao qual se candidata, poderá ser também o estudante, que para obter aprovação nas unidades curriculares com ensino clínico, tenha que proceder à recolha e ao tratamento de dados com vista à prestação dos melhores cuidados. Também é por exemplo a ESEP que procede à aprovação dos projetos que lhe são submetidos para validação de requisitos.

Posto isto, tanto o Estudante/Investigador, como a ESEP, são **Responsáveis pelo Tratamento**, já que ambos determinam as finalidades e os meios de tratamento de dados pessoais, isto é, conjuntamente entre ambos delimitam o âmbito e o sentido do estudo e isso é feito para os primeiros quando submetem os seus projetos, e para o segundo quando avalia a sua viabilidade de execução.

Ora, é importante explicitar uma pequena distinção entre os estudantes da Licenciatura em relação aos estudos considerados já pós-graduados, isto porque, somos do entendimento que os estudantes que estão no CLE, assumem per si o papel de **subcontratante**[5], uma vez que estes apenas executam os trabalhos de acordo com as orientações tanto do seu tutor de ensino clínico como do Responsável

[5] «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.

pela unidade curricular. Isto porque, poderá existir algum livre-arbítrio do estudante quando elabora o trabalho, mas tudo o resto é da responsabilidade do Coordenador da unidade curricular.

2. Regras de tratamento

Após a abordagem dos conceitos, é agora importante dotar o leitor com algumas regras que o habilitem a tratar dados, na aceção do conceito.

Isto é, não é pelo facto de ser estudante/investigador/professor, que automaticamente estão habilitados para realizar operações sobre os dados pessoais de um titular. Terão de existir fundamentos que nos permitam a tal prática e devemos ter algumas cautelas na sua laboração.

Desta forma, o RGPD[6], estabelece como essenciais para o tratamento de dados pessoais o cumprimento de sete princípios que são:

a) Os dados devem ser tratados de forma lícita, leal e transparente face ao titular dos dados;

b) Os dados recolhidos devem ter uma finalidade determinada, explícita, legítima e só poderão ser tratados no futuro caso não haja incompatibilidade com o pré-estabelecido;

c) Os dados a serem recolhidos devem ser no mínimo para o cumprimento da sua finalidade, ou seja, não devem ser recolhidos mais dados dos que os necessários;

d) Os dados utilizados e necessários para os estudos, deverão ser exatos e atualizados, devendo o Responsável pelo Tratamento criar medidas para descartar os dados que não sejam exatos ou que não estejam atualizados, evitando assim que, haja uma contaminação do estudo;

e) É necessário em traços gerais que a utilização dos dados tenha um prazo de duração, ou seja, não podemos (salvo raras exceções) conservar os dados eternamente. Devemos por isso estipular um prazo de conservação para os mesmos;

[6] Artigo 5.º RGPD

f) Ao aplicar as operações de tratamento que tencionamos efetuar nos dados pessoais, é necessário que o façamos com alguns cuidados, nomeadamente contra o tratamento não autorizado ou contra a perda ou destruição desta matéria-prima, sendo certo que, deverá o Responsável pelo tratamento de implementar medidas técnicas e organizativas que visam esta preocupação de integridade e confidencialidade;

g) Por último, mas não menos importante, é alias uma das grandes novidades que o RGPD nos trouxe, é o facto de o Responsável de Tratamento ou Subcontratante são responsáveis pelo cumprimento dos princípios supramencionados (a-f), e deverão ser capazes de demonstrar essa conformidade. São por isso responsabilizados, tratando-se aqui do princípio da responsabilidade.

Resumidamente, para procedermos a um correto tratamento de dados, temos de cumprir meticulosamente os princípios supramencionados, que são a licitude, lealdade e transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade, confidencialidade e a responsabilidade.

Apontando já os princípios norteadores que devem conduzir qualquer operação de tratamento, torna-se necessário que entendamos, que para proceder às operações de tratamento e para cumprir com o que é pedido logo com o primeiro princípio de que, os dados pessoais são tratados de forma lícita leal e transparente em relação ao seu "proprietário" é necessário, desde logo, analisarmos o ponto seguinte, que passa pela forma como verificamos ou não se estamos habilitados à realização das operações de tratamento necessários.

Assim sendo, torna-se necessário proceder ao enquadramento legal do artigo 6.º do RGPD, cuja epígrafe é "Licitude do tratamento".

É aqui, que vamos analisar se estamos ou não habilitados à prática de operações de tratamento sobre os dados, de outra forma, vamos saber se podemos ou não tratar os dados por forma a cumprir a finalidade a que nos propomos.

Porquanto torna-se necessário à luz do artigo 6.º enumerar quais são as "autorizações" que existem para proceder ao tratamento de dados pessoais, esclarecendo assim qualquer dúvida que exista:

a) O Consentimento do titular dos dados;
b) Execução de um contrato em que o titular dos dados é parte, ou para diligências pré contratuais a pedido do titular dos dados;
c) Cumprimento de uma obrigação jurídica a que o RT está obrigado;
d) Defesa de interesses vitais do Titular dos dados ou de outra pessoa singular;
e) Exercício de funções de interesse público ou exercício da autoridade pública;
f) Interesses legítimos do Responsável de tratamento, exceto quando prevalecerem os interesses ou direito dos respetivos titulares.

Exceto o primeiro fundamento de licitude, todos os outros fundamentos devem ser demonstrados pelo próprio responsável de tratamento à luz do princípio de responsabilidade, que se encontra vertido no artigo 5.º n. º 2 do RGPD.

O Consentimento, é aquele que obedece a regras próprias que se encontram mencionadas no artigo 7.º, e para que o mesmo possa ter validade prática (sendo legalmente aceite), este consentimento, para que o titular dos dados não tenha dúvidas no seu alcance, deve ser apresentado de um modo inteligível e de fácil acesso e numa linguagem clara e simples.

<u>De uma forma categórica e exemplificativa o Consentimento deve ser:</u>

- Manifestação de vontade livre;
- Específico[7];
- Explícito;
- Informado;
- Inequívoco;
- Acão positiva demonstrável;
- Retirável a qualquer momento;

Por motivos subjacentes e práticos, para os Estudantes/Investigadores[8], entendemos que ao existir outro fundamento de licitude, dos acima elencados, que permitam a estes (enquanto) Responsáveis de tratamento e/ou subcontratantes, executar operações de tratamento sem recurso ao

[7] O silêncio ou inatividade não permite o consentimento.
[8] Tudo em sentido lato e amplo.

Consentimento será uma mais-valia devido às implicações futuras que a retirada do consentimento pode acarretar no âmbito do referido estudo.

Ora até aqui estivemos a verificar as condições de licitude para o tratamento de dados, referentes a dados de categoria geral, ou por outras palavras a dados de tipo "normal", partimos agora, de igual forma para a verificação de qual a forma de habilitar os Estudantes/investigadores a procederem ao tratamento de dados de categoria especial, que por inerência dos estudos e da Escola onde estão envolvidos, pois é natural que se deparem com grande frequência com este tipo de dados conforme definição já supra abordada.

Desta forma, verificamos que existe uma regra, face ao artigo 9.º é que é proibido o tratamento de dados pessoais de categoria especial, contudo para toda a regra existe a respetiva exceção e no âmbito dos dados de categoria especial, não distinta.

Temos de certa forma autorizações que nos habilitam ao tratamento de dados, à semelhança do mencionado no artigo 6.º, por forma a resumir:

- Consentimento explícito;
- Cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social;
- Proteção dos interesses vitais do titular dos dados ou de outra pessoa singular;
- Atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares;
- Dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;
- Exercício ou defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional;

- Interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;
- Efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social;
- Interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos;
- Fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos;

Como abordado no documento denominado por: Conformidade com o Regulamento Geral de Proteção de Dados. Projetos de Investigação Científica, entendemos que, devido às finalidades que a ESEP legalmente adquiriu, que tem esta um papel a desempenhar a nível de investigação tanto científica como histórica. Sendo enquadrável a autorização para o tratamento de dados na alínea j) do n. º 2 do artigo 9.º do RGPD, a qual define:

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

Ao utilizar este fundamento de licitude, estamos habilitados à prática do tratamento de dados, mas sempre com observância em dois fatores, o primeiro os que se encontram vertidos ao abrigo do artigo 5.º e segundo, os que decorrem do artigo 89.º do RGPD;

Estabelece assim o artigo 89.º RGPD: "*O tratamento para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, está sujeito a garantias adequadas, nos termos do presente regulamento, para os direitos e liberdades do titular dos dados.*

Essas garantias asseguram a adoção de medidas técnicas e organizativas a fim de assegurar, nomeadamente, o respeito do princípio da minimização dos dados. Essas medidas podem incluir a pseudonimização, desde que os fins visados possam ser atingidos desse modo. Sempre que esses fins possam ser atingidos por novos tratamentos que não permitam, ou já não permitam, a identificação dos titulares dos dados, os referidos fins são atingidos desse modo."

A imposição do artigo é clara, já que nos esclarece que para este tipo de finalidade obriga os Responsáveis pelo Tratamento a um conjunto de medidas técnicas e organizativas que devem colocar em prática nas suas operações de tratamento.

Destacamos por isso, as seguintes medidas:

i. Minimização de dados;
ii. *Pseudonimização*;
iii. Cifra do equipamento onde se encontram armazenados os dados;
iv. Tratamento de dados em ambiente propício (com todas as medidas de segurança);
v. Os equipamentos/terminais, devidamente atualizados e com as respetivas ferramentas de segurança;
vi. Cuidado no uso de *clouds*, que não sejam devidamente "contratualizadas" pela ESEP, devido à possibilidade de transferências internacionais ou devido às condições de segurança mínimas que possam ser exigidas;
vii. Não copiar os dados para dispositivos de armazenamento pessoais;
viii. Atenção ao envio de dados pessoais por via de correio eletrónico pessoal ou não certificado pela ESEP;
ix. Garantir a confidencialidade, integridade e disponibilidade dos dados a todos os membros da equipa, devidamente segregados caso o estudo o exigia;
x. Vincular os investigadores com as políticas de confidencialidade inerentes à investigação;
xi. Entre outras.

Aqui chegados e de forma resumida, a título de boas práticas, os responsáveis pelo tratamento ou subcontratantes, devem, todavia, cumprir os princípios enumerados ao abrigo do artigo 5.º que não nos cansamos de reiterar.

Sendo estes uns dos principais cuidados no cumprimento do RGPD, aliados a estes princípios, estão sem dúvida, com igual importância, os direitos que devem ser garantidos aos titulares dos dados.

De forma resumida, abordaremos os Direitos destes.

3. Direitos dos titulares dos dados

A figura do titular dos dados, é proeminente no RGPD, aliás, o mesmo foi construído assente nessa figura, já que o próprio artigo 1.º lhe estabelece o direito à proteção dos dados pessoais, devido à importância desta para com a economia comum da união, como tal, foi-lhe atribuído um conjunto de direitos que lhe permite intrometer-se nas operações de tratamento que o Responsável pelo Tratamento ou Subcontratante pretendem executar, sendo-lhe atribuído um único capítulo III do RGPD, que vai do artigo 12.º ao 25.º.

Ora, por forma a cumprir com o regulamento existe um conjunto de direitos (à semelhança dos princípios), que têm de ser cumpridos. Decidimos por isso, de forma breve apontar e descrever em traços largos o que se entende por cada um dos direitos atribuídos.

1. **Direito à Proteção dos dados pessoais:**

Este direito é o corolário do vertido nos artigos 35.º da Constituição da república portuguesa e no 8.º da Carta dos Direitos Fundamentais da União Europeia. Trata-se do primeiro direito e a razão de ser da existência do RGPD, isto é, vem dotar os titulares dos dados de um conjunto de proteções relativamente ao tratamento que os seus dados são sujeitos.

2. **Direito à Informação:**

Assim que o Responsável pelo tratamento, de uma forma direta ou indireta inicia a recolha de dados do seu titular, torna-se, efetivo, necessário e obrigatório este prestar direito à informação ao proprietário dos dados. A equipa de EPD, já preparou uma comunicação em que se colige todas as obrigações para cumprir este direito, no documento: Comunicação ao participante para tratamento de dados pessoais.

Fazemos a ressalva que à luz da interpretação do artigo 12.º do RGPD em conformidade com as opiniões do Comité Europeu de Proteção de Dados, a informação mencionada tanto no artigo 13.º (quando existe uma recolha diretamente com o Titular dos dados), como no artigo 14.º (quando a recolha é indireta), pode ser prestada oralmente com recurso a testemunha que ateste que ao Titular lhe foi comunicada toda a informação.

Esta solução é apenas uma forma de cumprimento, já que atendendo ao meio onde os responsáveis pelo tratamento se vão inserir, é difícil criar mais procedimentos ou mecanismos que entravem, quer com a avaliação destes, quer com os procedimentos e normas internas em vigor naquele local de acolhimento.

3. Direito de acesso:

Este direito é um direito peculiar, pois permite (em regra geral), o acesso aos dados por parte dos seus titulares, permite-lhes saber o que anda o Responsável de tratamento a "fazer" com os seus dados. Este direito encontra-se tipificado no artigo 15.º, cujo escopo legislativo não foge em traços largos ao que aqui escrevemos, ou seja, o responsável pelo tratamento a pedido do titular dos dados, deve fornecer um conjunto de informações que permitam ao titular dos dados, validar a forma como os seus dados estão a ser trabalhados.

4. Direito de retificação:

Ora o artigo 16.º estipula que todos os titulares têm direito à retificação dos dados pessoais que não estejam corretos ou atualizados que digam respeito a esse titular.

Isto é o responsável pelo tratamento, deverá facultar ao Titular dos dados, a possibilidade de aportarem dados novos ou atualizados, sempre que para tal seja necessário.

5. Direito ao apagamento dos dados ou direito a ser esquecido:

É um dos direitos mais conhecidos atribuídos à panóplia da proteção de dados, que se materializa no pedido de apagamento de certos dados dos titulares de dados pelo Responsável pelo tratamento.

Todavia, não se trata de um direito absoluto, há algumas exceções que terão em caso de dúvida, ser analisado casuisticamente.

Contudo, como veremos adiante há situações em que este direito é restringido face às finalidades inerentes às próprias operações de tratamento bem como ao próprio fundamento de licitude que permitiu essas operações.

6. **Direito à limitação do tratamento:**

Como a epígrafe do artigo bem afirma, trata-se do direito de o Titular dos dados, mediante as situações específicas elencadas no artigo 18º n. º1, pode exigir ao Responsável pelo tratamento de uma limitação ao tratamento efetuado.

7. **Direito à Notificação:**

Qualquer alteração que é efetuada aos dados seja a pedido dos Titulares dos dados, seja por operação dos Responsáveis pelo tratamento, deve ser sempre comunicada/notificado ao titular dos dados.

Ora, o Titular dos dados, tem o direito de acompanhar o que é feito com os seus dados.

8. **Direito à Portabilidade dos dados:**

Trata-se de um direito que viu o seu nascimento com o RGPD, cujo principal enfoco é dotar o Titular de Dados com mais poderes e ferramentas que lhe permita fazer uma tutela efetiva da forma como o Responsável pelo tratamento procede ao tratamento dos seus dados;

De uma forma simples, trata-se da faculdade de exigir ao Responsável pelo Tratamento que possibilite a portabilidade dos seus dados, num formato legível e acessível ao Titular de Dados.

9. **Direito de Oposição:**

O Titular de Dados tem por isso o direito de se opor a qualquer momento às operações de tratamento sobre os dados que lhe digam respeito.

Contudo, é importante informar, que não é um direito absoluto, ou seja, esta faculdade atribuída ao Titular de dados, não é uma "carta branca" que lhe permita opor-se ou obstaculizar-se todas as operações de tratamento efetuadas por parte do Responsável de tratamento. É por isso uma situação de análise casuística, conforme pede o artigo 21.º que se faça.

10. Direito a não ficar sujeito a decisões automatizadas e aqui inclui-se as definições de perfis:

Ora, devido à evolução proporcionada pelos novos sistemas e plataformas, a automatização de tarefas é cada vez mais realizada, o que estabelece o artigo 22.º é que o Titular de Dados, não tem de ficar sujeito a nenhuma decisão (do Responsável de tratamento), que assente única e simplesmente em decisões automatizadas (nas quais não intervenha o Ser-Humano), isto estende-se à definição de perfil.

11. Direito a ter conhecimento em caso de violação de dados:

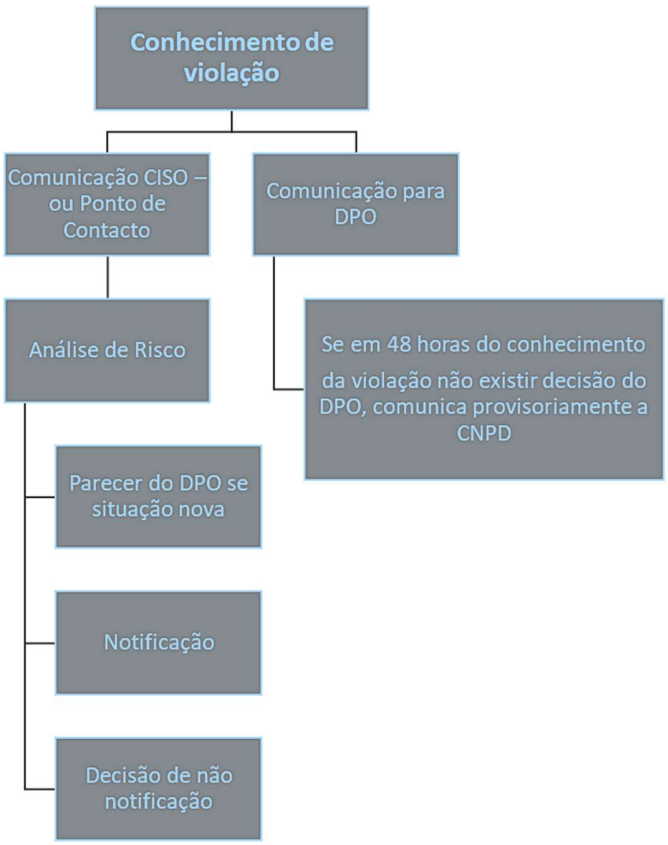
Este direito está implícito da leitura do artigo 34.º do RGPD, que estabelece que os titulares de dados têm o direito de serem informados da existência de qualquer violação de dados pessoais, desde que, essa violação seja considerada de alto risco, para os direitos liberdades e garantias.

12. Limitações aos direitos:

Deixamos para o último a exceção aos direitos, única e simplesmente para informar que, segundo o que acrescenta o artigo 89.º, existe face ao fundamento de licitude do tratamento uma derrogação em relação a alguns dos direitos supramencionados. Contudo e por um critério de simplicidade e rigor, iremos deixar apenas as ressalvas já feitas a cada um dos direitos. Por forma ao Responsável pelo tratamento, tenha o cuidado de o seguir de uma forma clara e concisa.

4. Violação de dados pessoais

WORKFLOW



Nos dizeres do número 12 do artigo 4.º do RGPD *«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"*, à primeira vista, podemos verificar que, se trata de uma definição extremamente abrangente e ampla, ou seja, qualquer situação que ocorra com os dados que não estava devidamente "planeada", poderá ser considerada uma violação de dados pessoais.

No entanto, a grande novidade que o RGPD importou é o que se encontra mencionado no artigo 33.º n. º 1 é a obrigatoriedade de o Responsável de Tratamento, tem de sem demora injustificada ou até 72 h, após o Responsável ter o seu conhecimento. Contudo, tal situação não é necessário

comunicar, caso seja verificável que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.

Ora, à **Autoridade de Controlo** (CNPD), o Responsável de Tratamento deverá comunicar a violação de dados com a informação que se encontra vertida no n.º 3, do mencionado 33.º:

- Descrever a natureza da violação dos dados pessoais incluindo:
    - As categorias e o número aproximado de titulares de dados afetados;
    - As categorias e o número aproximado de registos de dados pessoais em causa;
- Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;
- Descrever as consequências prováveis da violação de dados pessoais;
- Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos;

A obrigação de comunicação da violação de dados, não se esgota na comunicação à Autoridade de Controlo, como vimos nos direitos dos titulares de dados, estes também têm o direito de ser informados se tal acontecer.

Estabelece, assim, o artigo 34.º n. º 1 do RGPD que, se da Violação de Dados, resultar um elevado risco dos direitos liberdades e garantias da pessoa singular (aqui **Titular dos Dados**), o Responsável de tratamento sem demora injustificada, deverá comunicar a este a Violação de Dados.

<u>Comunicação que é feita, com a seguinte informação dispensada:</u>

- De forma clara e simples explica o que aconteceu;
- Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;
- Descrever as consequências prováveis da violação de dados pessoais;
- Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos;

Contudo, para o Titular dos Dados, existem três condições justificativas que podem operar para que a comunicação ao Titular dos Dados não seja feita, apenas e só se:

- O responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem;
- O responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados não é suscetível de se concretizar; ou
- Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.

Tudo posto e por um critério de organização, toda e qualquer situação que possa configurar uma violação de dados pessoais, deve ser imediatamente comunicada ao Encarregado de Proteção de Dados, para que se possa analisar e avaliar a situação de forma concreta.

Resumidamente, face à informação produzida e apresentada, o investigador/estudante, deverá comunicar sempre que tenha conhecimento de uma violação de dados, ao Encarregado de Proteção de Dados, mas também ao Departamento informática da ESEP. Podendo assim, estes dois responsáveis auxiliarem na resolução/acompanhamento de toda a situação.

5. Avaliação de Impacto sobre a Proteção de Dados (AIPD) e a sua Responsabilidade

Uma **Avaliação de Impacto sobre Proteção de Dados** (AIPD) é um documento que descreve múltiplas operações de tratamento, avalia a necessidade do tratamento e auxilia a gestão dos riscos para determinar medidas necessárias no tratamento dos dados pessoais.

Quando **implica um elevado risco** do tratamento nas atividades de processamento de dados pessoais, é obrigatório a realização de uma AIPD às operações de tratamento existentes de forma a mitigar os riscos identificados.

Sempre que não se conseguir encontrar medidas suficientes para reduzir os riscos elevados identificados para um nível aceitável, é obrigatório consultar a autoridade de controlo.

O documento deve ser preparado com vista de uma situação atual de acordo com os critérios e elementos no artigo 35º, nº 7, nomeadamente:

- Âmbito do AIPD;
- Objetivos da avaliação de impacto;
- Equipa e contactos dos responsáveis;
- Operações de Tratamento de dados pessoais:
- Avaliação das necessidades nas operações de processamento:
- Avaliar e mitigar riscos inerentes do direito dos titulares dos dados:
- Prever medidas de segurança e procedimentos para assegurar a proteção de dados:
- Recomendações de melhoria;

Por uma questão de boas práticas, uma AIPD deve ser continuamente revista e regularmente reavaliada.

O Responsável pelo Tratamento será a figura que administrará todos os procedimentos a serem realizados com os dados pessoais de um titular, ou seja, é o *dominus* da relação e sobre este, impendem não só, mas também, as obrigações que já foram verificadas.

A acrescer à lista obrigações a ter, está a necessidade ou não de proceder a avaliações de impacto sobre as operações de tratamento.

As Avaliações de Impacto, deverão ocorrer sempre que o Responsável de Tratamento, tenha a especial noção que essa operação de tratamento for suscetível de implicar um elevado risco para os direitos liberdade e garantias dos titulares dos dados.

Assim que haja esta noção, em momento anterior ao início do tratamento, o Responsável pelo tratamento deve iniciar esta avaliação de impacto.

Estabelece precisamente isso o artigo 35.º do RGPD, que a obrigação não é geral, apenas nasce "*Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares*".

Desta forma, e por um critério preventivo, dever-se-á realizar para a sua grande maioria de operações de tratamento, uma avaliação de impacto, ou uma pré-avaliação sobre as operações de tratamento.

Este cuidado/obrigação advém do próprio artigo 35.º, quando dá a possibilidade pelo n. º 4 às Autoridades de Controlo (aqui em Portugal CNPD), de elaborar e publicar uma lista das atividades de tratamento que são sujeitas a avaliação preventiva. Essa lista, nasceu com o Regulamento n.º 798/2018[9], quando menciona no n.º 6 "*Tratamento dos dados previstos no n.º 1 do artigo 9.º ou no artigo 10.º do RGPD ou ainda dos dados de natureza altamente pessoal para finalidade de arquivo de interesse público, investigação científica e histórica ou fins estatísticos, com exceção dos tratamentos previstos e regulados por lei que apresente garantias adequadas dos direitos dos titulares;*" a CNPD, suportou esta tomada de posição da *guideline* do grupo de trabalho do artigo 29[10], no ponto 4, "*Dados sensíveis ou dados de natureza altamente pessoal: inclui categorias especiais de dados pessoais, tal como definido no artigo 9.º (por exemplo, informações acerca das opiniões políticas dos indivíduos), bem como dados pessoais relacionados com condenações penais e infrações, tal como definido no artigo 10.º. Um exemplo seria um hospital geral que mantenha registos médicos dos doentes ou um investigador privado que mantenha informações acerca dos*

[9] Disponível em https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121818
[10] Disponível em https://www.cnpd.pt/media/f0ide5i0/aipd_wp248rev-01_pt.pdf

autores das infrações. Para além destas disposições do RGPD, algumas categorias de dados podem ser consideradas como categorias que aumentam os possíveis riscos para os direitos e as liberdades dos indivíduos. Estes dados pessoais são considerados sensíveis (na aceção comum deste termo) porque estão associados a atividades privadas e familiares (tais como comunicações eletrónicas cuja confidencialidade deve ser protegida) ou porque afetam o exercício de um direito fundamental (tais como dados de localização cuja recolha põe em causa a liberdade de circulação) ou porque a sua violação implica claramente que a vida quotidiana do titular dos dados será gravemente afetada (tais como dados financeiros que possam ser utilizados numa fraude de pagamentos). A este respeito, pode ser relevante saber se os dados já foram tornados públicos pelo titular dos dados ou por terceiros. O facto de os dados pessoais já terem sido tornados públicos pode ser considerado um fator pertinente para avaliar se, possivelmente, os dados seriam ou não utilizados para determinados fins. Este critério pode também incluir dados como documentos pessoais, mensagens de correio eletrónico, diários, notas de dispositivos eletrónicos de leitura equipados com funções de introdução de notas, bem como informações muito pessoais incluídas em aplicações onde ficam registados eventos da vida dos indivíduos."

Por isso é que somos do entendimento que, o Responsável pelo Tratamento, deve pelo menos nas circunstâncias supra expostas proceder à realização deste instrumento.

Uma AIPD tem como objetivo a recolha de informação que permita a construção da avaliação de impacto de proteção de dados e simultaneamente perceber que ações devem ser tomadas por parte das entidades envolvidas, de forma a apoiar a sua avaliação no que diz respeito aos requisitos do Regulamento Geral de Proteção de Dados (RGPD).

De forma a apoiar a construção da Avaliação de Impacto sobre a Proteção de Dados (AIPD), a enviar à autoridade nacional de controlo (CNPD), em conjunto com a minuta de protocolo a estabelecer, entre a ESEP e outras entidades cujos dados sejam necessários para a gestão de processos, é necessário a obtenção de um conjunto de elementos, que permita avaliar o nível de risco residual de privacidade.

Adicionalmente e caso as entidades envolvidas não possam disponibilizar as medidas de mitigação, tanto técnicas como organizativas de imediato, na referida AIPD, uma data previsível de implementação, com pelo menos a indicação do mês e ano que deverá ser anterior à transferência de dados em produção.

As medidas técnicas passam neste caso entre outras por: encriptação dos dados nos logs e nas Bases de dados da aplicação a usar; registo dos acessos tanto a nível aplicacional como de base de dados (auditoria); assim como medidas de controle de acessos e medidas organizativas: formação dos intervenientes; cláusulas contratuais específicas com empresas subcontratantes caso existam; política de privacidade e código de conduta. Como outras boas práticas não devem ser usadas réplicas totais ou parciais de Bases de Dados, dado que o mesmo aumenta o risco de privacidade.

O Encarregado de Proteção de Dados (EPD/DPO), terá aqui um papel consultivo e de auxílio na realização deste instrumento. Como tal, deverão os interessados/responsável pelo tratamento questionar o EPD que procederá à monotorização desta tarefa.

Se encararmos o que refere o artigo 35.º como elementos mínimos para a realização da **Avaliação de Impacto**, o n. º 7 estipula que:

a) "*Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;*

b) *Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;*

c) *Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o n.º 1; e,*

d) *As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa*", por forma a auxiliar nesta questão, é importante que seja vista a *guideline wp248*[11], já devidamente mencionada a partir da página 16, uma vez que esquematiza como realizar e estabelece exemplos de uma avaliação aceitável.

[11] https://ec.europa.eu/newsroom/article29/items/611236

Conclusão

O que se pretende com o Manual de Boas Práticas ora endereçado é dar a conhecer aos interessados os principais pontos a atender, nos diferentes âmbitos de atuação da ESEP, com especial enfoque na atividade de investigação científica, para a salvaguarda do cumprimento do RGPD.

Neste desiderato, este documento resume, sob uma perspetiva mais prática, os mais importantes princípios a adotar, num conhecimento basilar sobre estas matérias.

Na sequência do plano de trabalhos em curso, onde se integra já o presente manual, o EPD da ESEP está a desenvolver um conjunto de formulários e auxílios ao nível da proteção por defeito e da proteção por conceção, que auxiliem os interessados a praticar uma atividade de investigação alinhada com os mais exigentes princípios e procedimentos de proteção de dados, contribuindo para a qualidade e rigor da produção académica na ESEP.

Verificado assim, o enquadramento legal para o referido tratamento de dados pessoais, recomenda-se, através deste Manual, que os respetivos procedimentos devam ser cumpridos pelos diferentes interlocutores, por se encontrarem enquadrados nas orientações emitidas pelas autoridades responsáveis e que legitimam a ESEP perante a legislação nacional.

Titular do Documento e Aprovação

Ana Paula França e Ricardo Marques, a atuar como Vice-Presidente e como Encarregado de Proteção de Dados, respetivamente, são os titulares deste documento e são os responsáveis por garantir que esta política é revista e aprovada periodicamente, de acordo com os requisitos de revisão suprarreferidos.

Uma versão atualizada deste documento está disponível para toda a comunidade académica no site da ESEP, em área específica dedicada à Proteção de Dados.

Registo de Alterações:

Edição	Descrição da Alteração	Aprovação	Data da Edição
1	Edição inicial	Ana Paula França e Ricardo Marques	20/09/2023

Porto, 20 de setembro de 2023

Encarregado de Proteção de Dados - ESEP

E-mail: *epd@esenf.pt*

Equipa de Projeto RGPD

EPD / DPO da ESEP