POLITÉCNICO DE LEIRIA
ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Projeto

Mestrado em Administração Pública

A PROTEÇÃO DE DADOS

numa Instituição de Ensino Superior

Carla de Jesus Martins da Costa

Leiria, setembro de 2019.

Esta página foi intencionalmente deixada em branco

Projeto

Mestrado em Administração Pública

A PROTEÇÃO DE DADOS

numa Instituição de Ensino Superior

Carla de Jesus Martins da Costa

Projeto de Mestrado realizado sob a orientação do Professor Jorge Barros Mendes, Professor Adjunto da Escola Superior de Tecnologia e Gestão do Politécnico de Leiria.

Leiria, setembro de 2019.

Esta página foi intencionalmente deixada em branco

Originalidade e Direitos de Autor

O presente projeto de Mestrado é original, elaborado unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para o elaborar.

Reproduções parciais deste documento serão autorizadas na condição de que seja mencionada a Autora e feita referência ao ciclo de estudos no âmbito do qual o mesmo foi realizado, a saber, Curso de Mestrado em Administração Pública, no ano letivo 2018/2019, da Escola Superior de Tecnologia e Gestão do Politécnico de Leiria, Portugal, e, bem assim, à data das provas públicas que visaram a avaliação destes trabalhos.

Esta página foi intencionalmente deixada em branco

Dedicatória

Gostaria de dedicar este trabalho, bem como de expressar a minha gratidão à minha família, em especial ao meu marido e filho, pela motivação que me deram ao longo deste Mestrado, nomeadamente, pelo tempo que privamos de estar juntos, em virtude de o retirar para a realização deste Projeto.

Esta página foi intencionalmente deixada em branco

Agradecimentos

Este trabalho só foi possível com a ajuda de diversas pessoas, que direta ou indiretamente, com os seus contributos permitiram que o mesmo se tornasse realidade.

Aos professores do Mestrado em Administração Pública, o meu agradecimento pelos conhecimentos que me transmitiram durante este percurso académico.

Ao Professor Jorge Barros Mendes, orientador deste Projeto, que desde o início deste trabalho, sempre me ajudou com as suas orientações e conhecimentos especializados nesta matéria, e me motivou continuamente para a realização do mesmo.

Ao Coordenador do Curso de Mestrado em Administração Pública, Professor Eugénio Lucas, que quando nos cruzávamos na ESTG, tinha sempre uma palavra amiga, motivando-me à realização deste trabalho.

À Professora Gorete Marques, que me transmitiu conhecimentos e orientações para a realização deste Projeto. A sua disponibilidade foi imprescindível para que este trabalho chegasse a bom porto.

Por fim, à minha família e amigos, o meu profundo agradecimento pelo carinho e paciência que tiveram durante este caminho.

Esta página foi intencionalmente deixada em branco

Resumo

Com este projeto, pretende-se explorar o tema da proteção de dados no ensino superior português. Considerando a existência de uma lacuna nas Instituições de Ensino Superior: não possuíam Códigos de Conduta e Política de Privacidade dos seus dados, o objetivo deste trabalho foi implementar e propor essa ferramenta para uma IES.

Este trabalho parte da revisão de literatura na área da privacidade dos dados, com principal enfoque para o RGPD, e destacando-se por último uma proposta de uma Política de Privacidade para as IES em Portugal. Começando pelo historial da proteção de dados em Portugal, e passando pela Europa, o projeto abarca a temática da proteção de dados segundo o RGPD, e propõe a implementação e criação de um regulamento de privacidade de dados para uma IES.

Como consequências da criação desta Política de Privacidade, vemos como resultados principais, o facto de os estudantes poderem ter disponível um recurso, que os ajudará na manutenção dos seus direitos em termos de privacidade dos seus dados. Este documento salvaguardará todos as liberdades e direitos que estão eminentes para os estudantes de ensino superior.

Palavras-chave: *proteção de dados, RGPD, estudantes, dados pessoais.*

Esta página foi intencionalmente deixada em branco

Abstract

This project intends to explore the data protection theme in the Portuguese High Education. This theme allowed to discover a gap in high schools in Portugal: they didn´t have a Privacy Policy and Data Protection, so the goal of this work was implementing and proposing that resource for a high school.

In order to prepare this work, I consulted all information about data protection, mainly the GDPR, to propose a Privacy Policy to a high school in Portugal. Starting by the data protection history in Portugal, as well as in Europe, the project intends to explore the data privacy according to GDPR and proposes the implementation and the creation of a regulation to a high school.

As a consequence of the creation of this Privacy Policy, students will have available one resource that will help them to support their data privacy rights. This document will preserve their rights and the privacy freedom of all students.

Keywords: data protection, GDPR, students, personal data.

Esta página foi intencionalmente deixada em branco

Lista de figuras

Esta página foi intencionalmente deixada em branco

Lista de tabelas

Esta página foi intencionalmente deixada em branco

Lista de siglas

AP – Administração Pública

CNPD – Comissão Nacional de Proteção de Dados

CPA – Código do Procedimento Administrativo

CRP – Constituição da República Portuguesa

DPO – *Data Protection Officer*

EPD – Encarregado de Proteção de Dados

ESTG – Escola Superior de Tecnologia e Gestão

GDPR – *General Data Protection Regulation*

IES – Instituição de Ensino Superior

ISO – *International Organization for Standardization*

RGPD – Regulamento Geral da Proteção de Dados

UE – União Europeia

Esta página foi intencionalmente deixada em branco

Índice

Esta página foi intencionalmente deixada em branco

1. Introdução

Atualmente a relação de proximidade entre os jovens (estudantes) e a internet torna-os verdadeiros aliados. Um jovem que atualmente não tenha um telemóvel com acesso à internet ou que não aceda a sítios on-line (websites) é considerado uma exceção ou diferente da generalidade da sua geração. Assim sucede também com os estudantes do ensino superior porque são verdadeiros *amigos* das novas tecnologias, e estas últimas correm a ritmos alucinantes. Por vezes, elas avançam sem perguntar se podem entrar, ficar ou sair aos seus próprios "proprietários" - os estudantes.

Este projeto debruça-se sobre a proteção de dados dos estudantes de ensino superior, adultos e maiores de idade, que, portanto, têm o direito e a liberdade de exercer os seus direitos. No entanto há, por outro lado, deveres iminentes que estão subjacentes aos direitos, e que fazem destes jovens, pessoas mais responsáveis e conscientes da sua vida privada: nomeadamente quanto à privacidade dos seus dados (sendo também os seus resultados académicos do seu foro pessoal e intransmissível a outrem).

O projeto engloba uma finalidade que é uma proposta de uma Política de Proteção de dados para os estudantes de uma IES. Tem como ponto de partida o historial português e europeu na matéria de proteção de dados, passando ainda pela avaliação da implementação e criação de um regulamento para uma IES. A terminar o trabalho, optou-se por introduzir um glossário dos termos mais importantes da proteção de dados pessoais.

2. A Proteção de Dados

2.1 A(in)Segurança da Informação

A proteção de dados é uma temática muito discutida atualmente, no entanto, já em 1890, Samuel Warren tinha publicado um artigo "*The right to privacy*", em que defendia já nesta época o direito à privacidade e a proteção da privacidade das pessoas.

A informação digital hoje em dia flui de tal maneira, tanto através das vias de comunicação cada vez mais modernas e rápidas - os e-mails, como através dos *mass-media*, não se podendo esquecer as redes de comunicação digitais como as redes sociais, muito em voga atualmente.

Assim desta forma, podemos assumir de que existe segurança da informação quando temos a noção de que o que falamos no preciso momento, não vai destruir a reputação de uma pessoa ao serem divulgados os dados da sua vida privada num qualquer meio de comunicação social ou digital, ou seja, que há a privacidade da informação no que concerne à liberdade de comunicação e expressão.

A importância da privacidade e a segurança da informação começaram a ter mais relevância com a criação das grandes cidades, em que é possível esconder ou não revelar quem se é na realidade, e ter uma reserva da sua vida íntima e/ou privada garantida.

Já no que respeita à insegurança da informação, pudemos assistir recentemente em 2018, a uma falha de segurança de uma rede social mundial (Facebook) em que os seus

utilizadores (50 milhões) perderam o controlo das suas contas,e tornaram-se públicas informações que eram privadas ou do foro pessoal do seu utilizador.

A informação sendo um forte e potencial fator de desenvolvimento das sociedades livres e democráticas, torna-se assim vulnerável e frágil, e se a segurança estiver comprometida com fatores digitais alheios (exposição pública indevida) à vontade expressa do titular dos dados pessoais, enfrentamos um problema grave de insegurança da informação. Assim, quando não há garantias de segurança de informação, todo um manancial de direitos e liberdades fica afetado, isto é, a confidencialidade, a privacidade, a integridade e proteção da liberdade de informação.

2.2 Em Portugal

Em 1976, Portugal foi um dos primeiros países a englobar na sua Constituição (CRP – Constituição da República Portuguesa), doravante CRP, nomeadamente no seu artigo 35.º - Utilização da Informática, os dados pessoais informatizados e foi também a primeira Constituição do mundo a proteger expressamente os dados pessoais. Diz-nos o art. 35.º da CRP (versão original de 1976) o seguinte:

ARTIGO 35.º
(Utilização da informática)

1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização.
2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos.
3. É proibida a atribuição de um número nacional único aos cidadãos.

Entretanto, a CRP já sofreu várias alterações, e foi atualizada ao longo dos tempos, através de revisões constitucionais. Assim, e após várias revisões, atualmente o art. 35.º está redigido da seguinte forma:

Artigo 35.º
(Utilização da informática)

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.
3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.
5. É proibida a atribuição de um número nacional único aos cidadãos.
6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei.

Neste artigo, podemos antever alguns direitos primários das pessoas, como seja a proteção dos seus dados pessoais, bem como o tratamento dos dados pessoais que lhe digam respeito.

Os dados pessoais dizem respeito à própria pessoa e esta tem todo o direito e garantia em reservá-los para si mesma e proteger os mesmos do conhecimento de outrem. Advém do direito constitucional que protege este direito, liberdade e garantia como principal defesa de uma liberdade adquirida.

Cada um de nós tem o direito à reserva da sua informação para si mesmo, contando com uma proteção fundamental: a liberdade de ter informação de si mesma e para si mesma, a reserva de informação do próprio e para o próprio, ou seja, aquilo que me pertence (informação) é meu e a mim me diz respeito, devendo para isso ser protegido o acesso e o tratamento dessa informação.

Acerca deste artigo 35.º da CRP, dizem-nos Canotilho e Moreira (2007) que a proteção e defesa contra o tratamento informático de dados pessoais, se analisa principalmente em três direitos:

> "a) direito de acesso das pessoas aos registos informáticos para conhecimento dos seus dados pessoais dele contantes (n.º 1), bem como a rectificação e complementação dos mesmos;
> b) direito ao sigilo em relação aos responsáveis de ficheiros automatizados e a terceiros dos dados pessoais informatizados e direito à sua não interconexão (n.º 4);
> c) direito ao não tratamento informático de certos tipos de dados pessoais (n.º 3). A proibição do número nacional único (n.º 5) funciona como garantia daqueles direitos, dificultando o tratamento informático de dados pessoais e a sua interconexão, que seria facilitada com um identificador numérico comum."

Desta forma, com estes três princípios acima reconhecidos podemos deduzir que a interconexão e a assunção de um número nacional único (cuja atribuição é expressamente proibida pela CRP), facilitaria uma rápida identificação e não garantiria a proteção dos direitos inerentes ao titular dos dados.

E com funções de proteção dos dados pessoais, atribuições e competências ao nível fiscalizador e penalizador, temos no nosso país, a entidade competente nesta matéria que é a CNPD – Comissão Nacional de Proteção de Dados, criada através da Lei nº 43/2004 de 18 de agosto. Trata-se de uma entidade administrativa e independente que funciona junto da Assembleia da República. Esta Autoridade Nacional de Controlo de Dados Pessoais tem entre outras competências as de controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais,assim como de cooperar com as autoridades de controlo de proteção de dados de outros Estados, nomeadamente na defesa e no exercício dos direitos de pessoas residentes em território nacional e/ou no estrangeiro.

As recentes alterações ao Código de Procedimento Administrativo, levaram o legislador a consagrar no seu art. 18.º o princípio da proteção dos dados pessoais, definindo que os particulares têm direito à proteção dos seus dados pessoais e à segurança dos mesmos, como podemos ler abaixo:

"Artigo 18.º

Princípio da proteção dos dados pessoais

"Os particulares têm direito à proteção dos seus dados pessoais e à segurança e integridade dos suportes, sistemas e aplicações utilizados para o efeito, nos termos da lei."

Portugal não tem um grande historial registado na aplicação de multas pesadas neste âmbito.

No primeiro ano seguinte à entrada em vigor do RGPD, a CNPD aplicou coimas a quatro entidades diferentes, num valor total de 424 mil euros, e registou 864 processos de averiguação, que podem resultar em contraordenações ou repreensões (medidas corretivas).

Entre os registos de coimas aplicadas, há a destacar o facto recente (em 2018) no nosso país, de um processo de uma multa de 400 mil euros, ao Centro Hospitalar do Barreiro-Montijo pela inobservância na proteção dos seus dados pessoais. O caso deveu-se à infração de três áreas fulcrais do RGPD: violação dos artigos 5.º - princípio da minimização, artigo 83.º - princípio do tratamento e artigo 32.º - segurança do tratamento dos dados pessoais.Verificou-se que, neste Centro Hospitalar, estavam registados "perfis" de utilização informática que deveriam ter acesso restrito, no entanto, os perfis existentes não limitavam a consulta dos seus utilizadores aos processos médicos. Exemplificando, o perfil de "Técnico" deveria ter permissões específicas, mas tinha as mesmas permissões que o perfil de "Médico".

Verificou-se também em Portugal o caso de um Call Center que não deixou o/a possuidor/a de dados pessoais aceder aos seus dados (gravações telefónicas), arquivados pelo Call Center, em virtude de alegar que só deveria fazê-lo sob ordem judicial. Por ter violado o art. 83.º n.º 3 – violação do direito de acesso aos seus dados pessoais, esta entidade foi multada em € 20.000,00 (vinte mil euros) pela CNPD – Comissão Nacional de Proteção de Dados.

Temos ainda registado no seu website (por parte da CNPD) dois processos de contra-ordenação, com multas de € 2.000,00 (dois mil euros) por violação do direito de

informação aos titulares sobre o tratamento dos seus dados pessoais, protegidos no art. 13.º n.º 1 e 2, uma vez que devem ser facultadas informações sobre os seus dados e o seu tratamento ao titular dos mesmos.

Portugal era um dos únicos países (juntamente com a Grécia) que ainda não tinha validado qualquer legislação nacional no âmbito do novo RGPD. Esta situação já não se verifica uma vez que já saiu recentemente a Lei de Execução Nacional, em agosto deste ano.

2.3 Na Europa

Em 1950, umas décadas antes da adesão de Portugal à UE, a Convenção Europeia dos Direitos do Homem, referia no seu artigo 8.º, o direito ao respeito pela vida privada e familiar, ressalvando que: "Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência."

Aquando da adesão de Portugal à União Europeia (em 1986), o nosso país assumiu compromissos com a Europa e com os seus Estados-Membros. No que diz respeito à proteção de dados, viria no ano 2000 a ser consagrado no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, o direito à proteção dos dados pessoais, o qual se transcreve a seguir:

Artigo 8.º

Protecção de dados pessoais

1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.

2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

Mais recentemente em 1995, a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, vem aplicar matéria jurídica no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados.

Em 2009 (em 1 de dezembro), entrou em vigor o Tratado de Lisboa, que reproduz e junta dois tratados: da União Europeia e da Comunidade Europeia. Com o Tratado de Lisboa, assinado na cidade portuguesa de Lisboa, em 13 de dezembro de 2007, os seus Estados-Membros reformaram o funcionamento da União Europeia, prevendo já neste ano como possível a saída efetiva de um Estado-Membro da União Europeia, facto que não constava no Tratado da União Europeia (TUE, Maastricht; 1992) bem como no Tratado que estabelece a Comunidade Europeia (TCE, Roma; 1957), mais tarde renomeado para Tratado sobre o Funcionamento da União Europeia (TFUE). No Art. 16.º deste Tratado, que se cita infra, pode-se ver o princípio base que estabelece o direito à privacidade dos dados pessoais:

"ARTIGO 16.º
1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito."

Vinte anos depois, através do Jornal Oficial da União Europeia, é publicado o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 - *General Data Protection Regulation*, ou seja, o novo RGPD - Regulamento Geral da Proteção de Dados. Com este novo regulamento que revoga a Diretiva de 1995, e que começou a produzir efeitos em 2018, a matéria da proteção de dados e o tratamento de dados, bem como a circulação dos mesmos, ficou melhor protegida e melhor salvaguardada em termos legais. Note-se que este Regulamento foi publicado em 2016, no entanto, seguiram-se dois anos para ajuste pelos setores privado e público às novas regras da proteção de dados.

2.4 O RGPD

O RGPD (Regulamento Geral da Proteção de Dados) ou GDPR (*General Data Protection Regulation*) é um documento oficial europeu (legislação) constituído por um conjunto de considerandos (173 considerandos), bem como ainda por uma série de artigos legislativos (99 artigos), que regulamentam a privacidade dos dados pessoais com vista à proteção dos mesmos dentro da União Europeia, e não só (uma vez que o direito à privacidade não existe só dentro da UE, mas também fora dela, na medida da relação existente com todos os países – ou seja, ao nível mundial).

Este regulamento começou a ser delineado em 2012, mas só quatro anos depois é que viria a ser publicado no Jornal Oficial da União Europeia, em 4 de maio de 2016, com data oficial de entrada em vigor, em 25 de maio de 2018 (com dois anos de interregno).Desde 25 de maio de 2016,e até à mesma data em 2018, serviu este intervalo de dois anos para uma existisse uma completa e total transição bem como uma adaptação pelas organizações públicas e privadas da União Europeia.

No âmbito de atuação do RGPD, este segue um conjunto de princípios reguladores relativos à proteção e tratamento de dados pessoais, nomeadamente entre outros, que é muito importante que os dados devam ser tratados de forma lícita, leal e transparente, sempre para cumprimento de determinadas finalidades, explícitas e legítimas. Já no que concerne à "minimização dos dados", estes devem ser adequados e limitados, essenciais e necessários, ao que é estritamente indispensável tratar e para as finalidades a que se destinam.

Uma das formas lícitas, bem como o principal princípio de proteção dos dados pessoais é o princípio da minimização, ou seja, só recolher ou receber os dados estritamente necessários para a finalidade a que se destinam. Também os dados recolhidos devem ser exatos e atualizados, e ainda conservados de forma a que garanta a segurança da

informação de quem os transmitiu, incluindo a proteção contra o tratamento não autorizado e ilícito.

Neste regulamento, estão descritas uma lista de definições (no seu artigo 4.º) e também os princípios sobre a proteção de dados, nomeadamente o que são: dados pessoais, tratamento, limitação do tratamento, definição de perfis, pseudonimização, ficheiro, responsável pelo tratamento, subcontratante, consentimento, violação de dados pessoais, destinatário, entre muitos outros significados, estes que referi anteriormente considero como os mais pertinentes neste estudo.

Entre algumas das definições mais importantes do RGPD, é de destacar primeiramente o que é entendido por 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". A informação pessoal de um indivíduo que se consiga identificar é um dado pessoal, que é passível de ser tratado, no entanto, para esse tratamento, há que se obter um consentimento ou seja, trata-se de pedir uma autorização para ser efetuado um tratamento desses dados pessoais. Os dados pessoais de uma pessoa são identificáveis desde logo quando ocorre uma ligação entre a informação e o seu titular, e quando conseguimos relacionar os dados ao seu titular, aqui podemos dizer que os dados pessoais são nominativos, ou seja relativos ao titular X ou Y.

De seguida, apontámos abaixo o significado de 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".

A operação acima é tão importante quanto o consentimento, porque permite registar, alterar, e analisar a informação dos estudantes e tratar os dados pessoais com o objetivo de os classificar para determinadas finalidades. No tratamento, poderemos anonimizar ou não os dados dos estudantes, uma vez que é permitido a separação entre o titular e os dados, de forma a não haver ligação entre uns e outros. Consoante o objetivo do tratamento dos dados, há a forma de os apresentar: ou nomináveis ou anonimizados, tendo assim o tratamento um caráter muito importante na sua transformação da informação apresentada.

Uma outra definição que aparece no RGPD, e que é não menos importante, é a de 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".Como referi anteriormente a pseudonimização ou anonimização revestem o caráter de dados não identificáveis de alguém. Podemos através das listagens e da sua forma organizativa, transformar os dados em informação estatística anónima e não identificável relativamente ao seu titular.

Entende-se ainda por Consentimento (do titular dos dados), uma das definições mais importantes do RGPD como: "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento". O consentimento é um ato muito importante que aprova ou não, e autoriza que a informação seja recolhida, tratada e arquivada pela entidade/organização promotora desse pedido.Quando necessário e nas IES, o consentimento deve ser realizado por escrito, gravado ou transmitido de forma inequívoca para que não haja dúvidas de licitude no tratamento dos dados.

Nas IES quando um estudante realiza a sua matrícula, normalmente é solicitada uma série de dados pessoais que são de caráter identificativo e/ou académico, dados que são necessários para a efetivação da matrícula. Assim, as IES para poderem tratar os dados

pessoais anteriormente referidos, necessitam do consentimento escrito desse estudante, uma vez que para o tratamento, bem como para a transferência de dados é necessário que o estudante tenha expressado através de uma autorização escrita, com esse sentido de autorização para aqueles efeitos.

2.5 Privacidade desde a conceção (*Privacy by design)*

No RGPD, o art. 25º fala-nos de proteção de dados desde a conceção, que significa prever, calcular, tratar o conceito de privacidade desde o início, ou seja, desde a conceção de um produto, bem ou informação, até à prossecução da sua finalidade. Ora, neste caso a privacidade é um processo previamente elaborado, analisado e aplicado desde o momento em que se conjetura a conceção de um novo produto, bem ou serviço. Nesta linha de seguimento, este conceito de privacidade pressupõe que desde o início de um bem/serviço é logo pensada a proteção dos seus dados e a privacidade surge logo aquando a criação desse novo produto/bem ou serviço. Permanece a privacidade ao longo da construção e desenvolvimento do bem e/ou serviço, em continuidade desde o início até atingir a sua meta ou finalidade.

É um conceito completo e abrangente e compreende sete princípios fundamentais de privacidade que estimulam como objetivo principal uma privacidade incorporada e mais capacitada, capaz de abranger desde a conceção até à prossecução da finalidade.

Em 2010, em Jerusalém, reuniram-se especialistas de todo o mundo para falar sobre esta matéria específica (abordar a temática da privacidade desde a conceção) e daí resultou uma resolução, que reconheceu que a privacidade desde a conceção, é um elemento fundamental para a privacidade e proteção dos dados pessoais.

2.6 Privacidade por defeito

(*Privacy by default)*

O conceito de privacidade por defeito, segundo o RGPD, consiste na aplicação de "medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento". Este conceito aplica-se só à quantidade necessária ou aos dados recolhidos, à extensão do seu tratamento e ao prazo normal de conservação, tendo por base a intervenção humana neste processo.

Embora a expressão em português soe diferente, o que se passa é que este conceito de privacidade abrange que desde o início que há dados a proteger e a expressão "Default", ou seja, defeito indica-nos que a privacidade deveria acontecer espontaneamente e por defeito, ou seja de forma automática.

2.7 A Lei de Execução Nacional

Foi publicada muito recentemente, em 8 de agosto de 2019, a Lei n.º 58/2019 que assegura a execução, a nível nacional, do RGPD que foi publicado em 2016. Esta lei configura ao nível interno do nosso país, a regulação da proteção de dados pessoais, para cumprimento de normas específicas de privacidade, bem como estabelece em concreto as regras, que em sintonia com o RGPD, devem ser cumpridas, a fim de que exista uma segurança efetiva na informação e na proteção de dados pessoais.

Através desta lei, que segue as linhas de orientação do RGPD, podemos constatar que as atribuições da CNPD (entidade nacional de controlo e proteção de dados) estão em consonância com o RGPD, bem como as funções do EPD, estão bem definidas e delimitadas, com um elenco de responsabilidades específicas. Verifica-se também que a função de EPD ou DPO gera o aparecimento de uma nova profissão no mercado profissional. A responsabilidade acrescida do(a) Encarregado da Proteção de Dados é segundo o art. 9.º, de autonomia técnica e este está obrigado ao dever de sigilo e confidencialidade, mesmo após o término das suas funções, e muito para além do sigilo profissional previsto na lei.

No artigo 15.º desta lei, está claramente exposto que compete à CNPD estimular a elaboração de códigos de conduta, para que ao nível privado e/ou público estejam reguladas todas as vertentes da privacidade dos dados pessoais nas diversas áreas da sociedade. Os códigos de conduta referidos na administração direta e indireta do Estado, poderão de acordo com o Art. 15.º, regular atividades específicas públicas, estando também ao alcance das IES a elaboração destes regulamentos próprios. Estes códigos servem para regular atividades específicas, como seja a educação, o ensino e/ou a saúde, as quais devem ter em linha de conta as necessidades de regulação existentes na Administração Pública.

No capítulo VI desta lei, podemos apreender sobre algumas situações específicas de tratamento de dados pessoais, e que dado a particularidade dos mesmos, e a título de exemplo, temos a publicação de dados pessoais (nomes de pessoas) em jornal oficial nacional, já que a minimização da informação pessoal (limitação dos dados) é sempre a melhor opção aquando da divulgação e/ou publicação oficial.

De acordo com o objeto desta lei de execução nacional, que não exclui nada nem ninguém, a sua aplicação assegura a realização com segurança do tratamento de dados, dentro e fora do território nacional, que afetem direta ou indiretamente os titulares de dados. Possuindo residência ou não em Portugal, as atividades existentes ou com ligações

aos portugueses residentes ou não em território português, e/ou no estrangeiro, são também reguladas por esta lei.

3. A Proteção de Dados no Ensino Superior (numa Instituição de Ensino Superior)

O Ensino Superior em Portugal é constituído por um sistema binário que combina por um lado o sistema de ensino superior universitário, e pelo outro o ensino superior politécnico, sendo ministrado em instituições de ensino superior públicas e privadas. Esta dualidade no sistema de ensino superior português rege-se também com regras distintas para as universidades e para os politécnicos, tendo a lecionação de alguns ciclos de estudo sido distinguida e separadaem dois sentidos.

Na Figura 1 (abaixo) podemos analisar esta dualidade entre o ensino superior português e verificar que as universidades não lecionam ciclos de estudo curto (como sejam os Cursos Técnico Superiores Profissionais) bem como os Politécnicos não ministram Doutoramentos. Esta situação dos Doutoramentos sofreu uma alteração recente porque foi ultimamente publicada legislação que permite aos Politécnicos, em parceria com Universidades, a lecionação conjunta de um Doutoramento.

Mais se pode conferir que os ciclos de estudo confinantes aos Politécnicos são os Ciclos de Estudos Curtos e ainda o 1.º e 2.º Ciclos de Estudos (Licenciaturas e Mestrados), enquanto que as Universidades estas podem ministrar os Doutoramentos, Licenciaturas e Mestrados e ainda os Mestrados Integrados.

Nesta linha de seguimento seria de pensar porque é que havendo um sistema de ensino binário, também poderia haver duas formas distintas de efetuar a proteção dos dados nas Universidades e/ou nos Politécnicos. O que se passa é que todas as IES (de ensino público e/ou privado) são passíveis de utilizar o mesmo código de conduta, uma vez que este último serve os mesmos interesses e vem proteger os direitos de todos estudantes de ensino superior em geral, independentemente do ciclo de estudos ou da IES em causa.

Podemos ver abaixo a Figura 1, onde está esquematizado o sistema de ensino superior português (com a dualidade das Universidades versus Politécnicos).

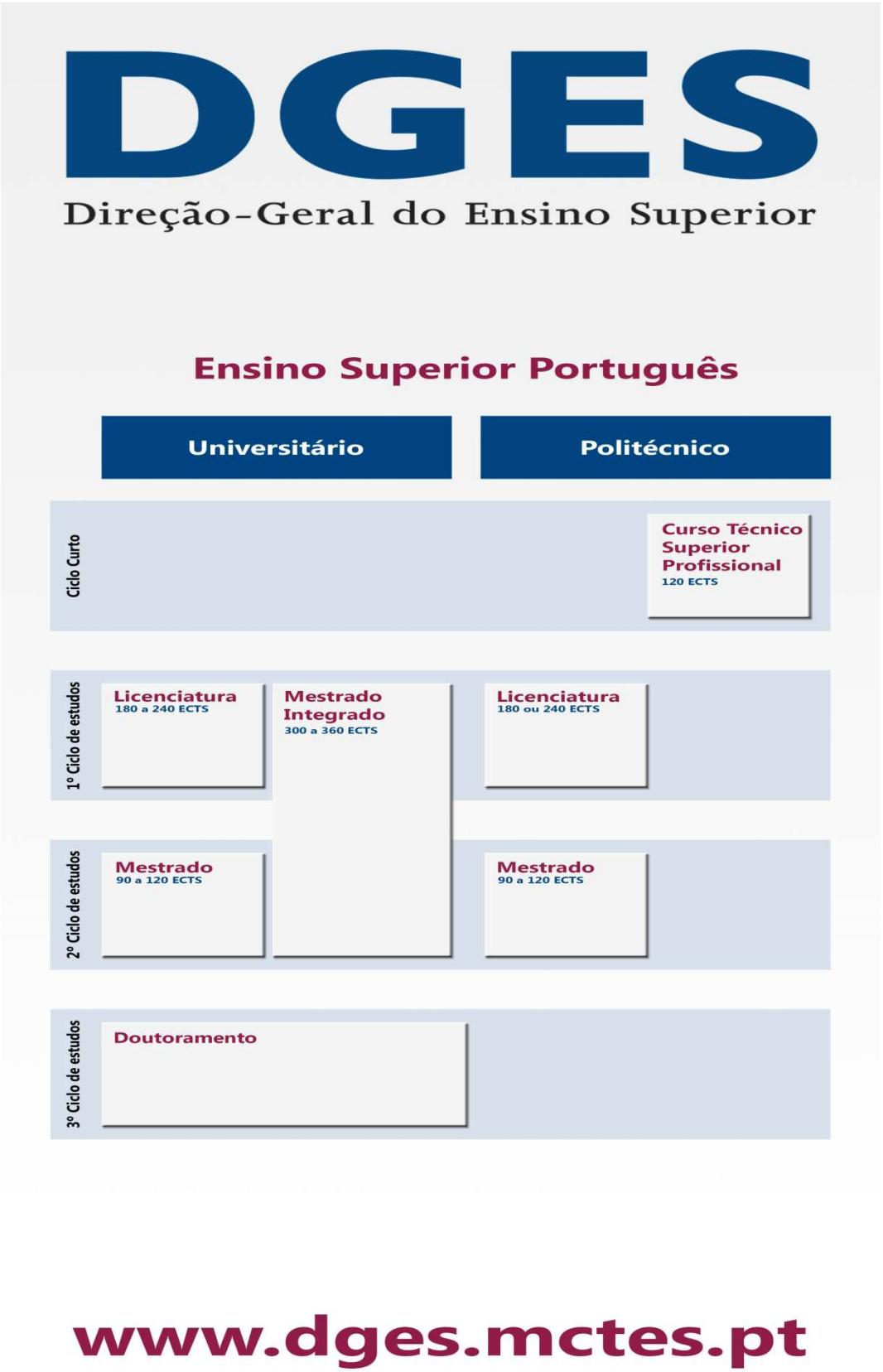


Figura 1 – Sistema de ensino superior português

Uma IES reúne uma série de informações pessoais de toda uma comunidade académica que abrange desde os dados pessoais aos académicos, bem como a troca de dados entre IES. Toda esta panóplia de dados é, e deve ser assim mesmo, alvo de proteção da informação.

Podemos ver na figura abaixo (Figura 1), que a proteção de dados engloba desde os dados pessoais, aos dados académicos, até à troca dos mesmos com outras IES, e toda este fluxo de informação tem de ser protegido condignamente.

Quadro geral da proteção de dados das IES

Figura 2 – Dados a proteger nas IES

Nas IES,o curso da informação é bastantedinâmicoe intenso.A informaçãonecessita de ser protegida, devido à própria difusão da mesma e ainda àdisponibilização pelos canais de comunicação existentes na Instituição. No entanto, não inviabiliza de que muitos dos dados pessoais sejam canalizados para departamentos próprios da Instituição, em que haja uma

separação de toda essa informação destinada a tratar ou a regulamentar, com tramitação específica.

Podemos observar na figura abaixo (Figura 2), uma tabela que reflete a separação dos dados por categorias de informação, existentes numa IES, uma vez que os dados dos estudantes não podem ser tratados de igual forma aos dados dos docentes, assim como é legítimo que também se distinga o tratamento dos dados dosfuncionários não docentes do dos docentes e dos estudantes. Os dados de cada uma destas categorias diferem também em termos de tratamento específico e de proteção dos mesmos bem como os seus prazos legais.

Para cada um dos grupos existentes numa IES, há dados diferentes a conservar e a tratar, no entanto, os princípios-base do tratamento e a proteção dos dados são os mesmos para toda a informação ou dados pessoais a tratar, independentemente de quem são os dados e de onde vêm os dados que são para tratamento.

Na figura abaixo (Figura 2) podemos analisar os diversos intervenientes no processo de dados pessoais e informações que estão sujeitos a proteção, e cuja privacidade dos mesmos é legítima e adequada. No entanto, os grupos fundamentais são vários, mas o grupo primordial são os estudantes de uma IES, uma vez que é este grupo que a caracteriza e cujos dados são de extrema importância e fundamentais à vida da própria instituição.

Informação a protegernas IES por grupos

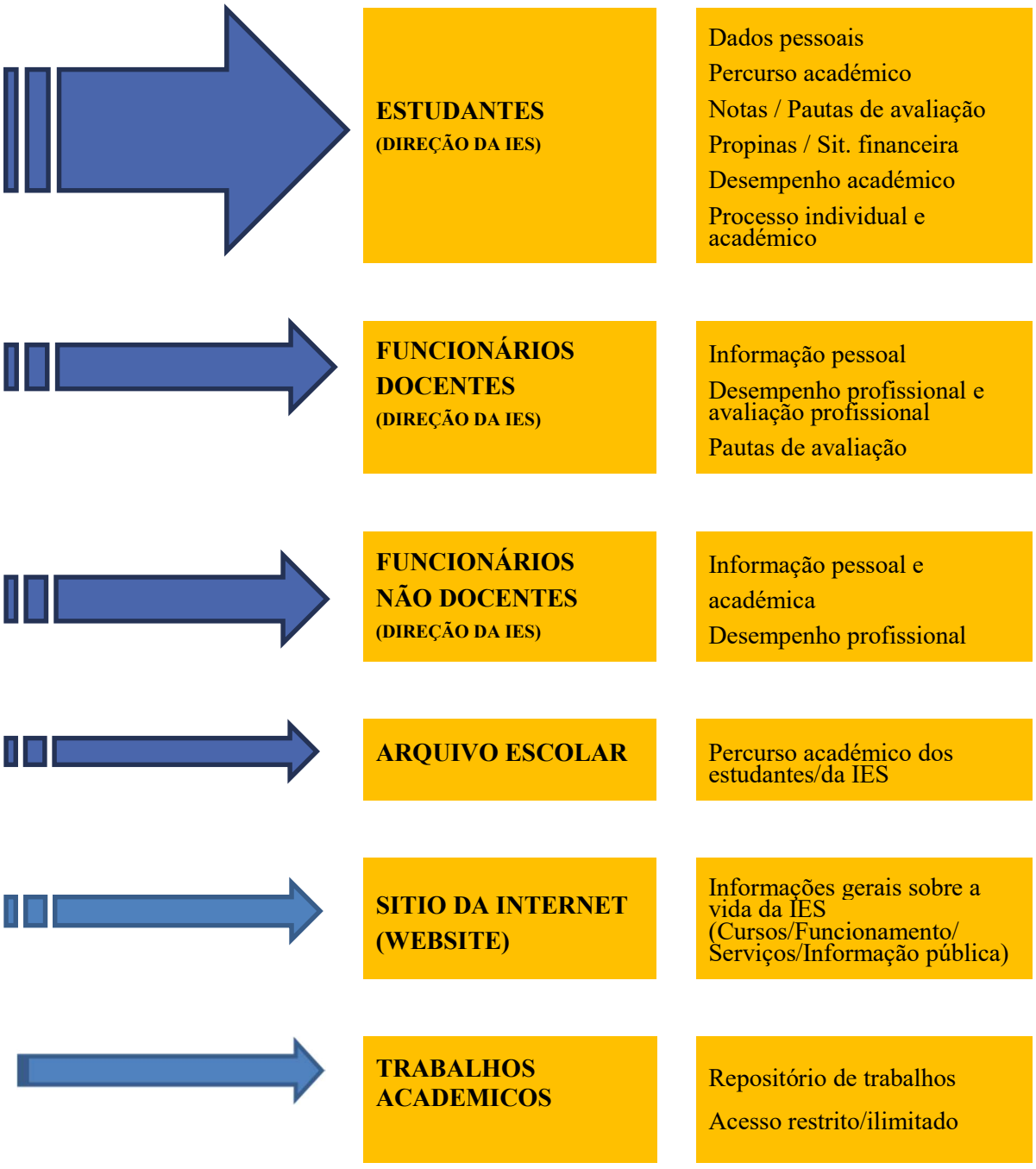


Figura 3 – Caracterização dos dados das IES por grupos

Observando a figura acima (Figura 2) verificamos que existem três grandes grupos: Estudantes, Funcionários Docentes e Funcionários Não Docentes, sendo que existe um dado em comum nestes três grandes grupos: a Direção da IES. Esta última (a Direção da IES) tem acesso a informação privilegiada destes três grupos principais, mas esta informação é transversal, no entanto, confidencial, dentro de cada um dos três grupos da IES.A Direção da IES tem acesso a informação singular e diferenciada por via de informações e/ou dados que precisam de análise e/ou ainda de resposta, bem como de serem tratados pelos superiores hierárquicos (pela Direção da IES). A Direção da IES tem um acesso mais alargado e generalizado (em toda a dimensão da IES), nomeadamente, para a resolução de situações académicas, ou de situações internas da própria IES, que geralmente necessitam de um tratamento específico e diferenciado.

3.1 Estudantes

Neste grupo, o maior e o mais importante de uma IES, existem vários dados pessoais (várias tipologias de informação) que é necessário proteger e garantir, como seja, a confidencialidade da informação destes estudantes. Dentro da informação de cada estudante, conforme indicámos na Figura 2, temos os dados pessoais, os dados académicos, os dados relativos às propinas, o desempenho académico e todo um processo individual do estudante e que é nada mais que o fator crucial da IES. Uma IES sem estudantes é como uma empresa sem clientes, trata-se de uma ligação fundamental, é o que dá a vida à IES.

Os estudantes (e os seus dados), tratando-se do grupo mais importante, também geram vulnerabilidades e os seus dados têm de ser protegidos. Há que refletir sobre a tipologia dos dados dos estudantes, nomeadamente sobre os dados pessoais e os dados académicos: estes últimos englobam informações específicas da sua vida académica, da sua privacidade e da esfera pessoal do estudante. Convém também saber que, entre os dados de um estudante há informações que nunca podem ser solicitadas ou tratadas, tais como os dados relativos à saúde ou dados genéticos bem como aorientação ou vida sexual,

ou aindaos dados biométricos. Estes últimos, tratando-se de dados sensíveis dos estudantes, exigem uma reflexão adicional sobre os mesmos. No entanto, há dadosna esfera da saúde dos estudantes que por vezes são tratados no âmbito da vida académica e que, sendo sensíveis, devem ter um tratamento específico. Refiro-me nomeadamente a algumas características específicas ou doenças limitativas, que podem interferir direta ou indiretamente com a sua aprendizagem, ou com asua normal formação.Estas informações são muitas vezes transmitidas ao corpo docente da IES, com vista a um tratamento diferenciado pelos mesmos e de acordo com a tipologia referenciada e comprovada, estes dados devem ser sempre protegidos uma vez que dizem respeito à saúde e caracterização pessoal específica dos estudantes.

Podemos observar de seguida uma tabela com os dados pessoais e académicos, onde a sua análise e leitura, nos dão um panorama geral das tipologias de dados dos estudantes,divididas por uma ordenação classificativa.

	DADOS PESSOAIS	**DADOS ACADÉMICOS**	**DADOS CONFIDENCIAIS**
TIPOLOGIAS DE DADOS	▪ Nome e nº estudante ▪ Morada ▪ N.º Identificação civil, fiscal ou social ▪ Data e local nascimento/Idade ▪ N.º Telefone/ Telemóvel ▪ Contacto de e-mail ▪ Informações s/ o agregado familiar	▪ Notas ▪ Faltas (n.º) ausências e Presenças (n.º) ▪ Avaliação / Exames metodologias e épocas de avaliação ▪ Curso/unidades curriculares inscritas ▪ Aproveitamento escolar/transição de ano ▪ Propinas (valores e prestações por curso/aluno) ▪ Bolsa de estudos / bolsa de mérito	▪ Dados relativos à Saúde (informações s/ doença/s - vacinação) ▪ Informação s/ Necessidades Educativas Especiais ▪ Pagamento de propinas por estudante (valores pagos/ dívidas) ▪ Informações biométricas ▪ Situação económico-financeira do agregado familiar

Tabela 1 – Tipos de dados dos estudantes

De acordo com a Tabela 1 temos a diferenciação entre: os dados pessoais, os dados académicos e ainda os dados confidenciais. Neste sentido, todos estes dados são recolhidos e tratados pelas IES. Não obstante, parece-me que deve haver uma distinção em termos de segurança, proteção e privacidade dos mesmos. Sendo considerados todos os dados acima como dados pessoais, há, no entanto, informações de caráter pessoal, e algumas outras informações que são mais sensíveis umas do que outras.

Dentre todos os estudantes de uma IES, podemos atualmente destacar duas grandes tipologias de estudantes, ou seja, os estudantes nacionais (residentes em Portugal) e os estudantes internacionais (ou que não residam permanentemente em Portugal). Estes últimos frequentam as IES, mas naturalmente encontram-se em mobilidade de estudos (Erasmus) eestão vinculados através de parcerias internacionais entre as IES, ou são estudantes internacionais que por último não são originais do nosso País ou não-residentes em Portugal, mas que se encontram a estudar temporariamente no nosso País.

Nestes dois grupos de estudantes: nacionais e/ou internacionais, há que fazer uma reserva de informação, mas devemos tratá-la com a mesma privacidade. As "culturas" de outros países são diferentes da nossa, e aquilo que por vezes em Portugal é uma simples informação, pode ser considerada por outros como dados invasivos da sua privacidade (desses mesmos estudantes). Refiro-me, por exemplo, ao estado civil de uma pessoa, que é uma informação pessoal *sui generis* e que pode ser um dado suscetível de "não-resposta". Em Portugal é muito comum nos formulários e inquéritos ser questionado o estado civil doindivíduo, no entanto, há quem considere que esta informação só diz respeito à vida privada, daí que na minha opinião, se possa tratar de um dado pessoal sensível.

3.1.1 Plataformas de *E-Learning*

Nas IES é muito frequente os estudantes terem à sua disposição plataformas de ensino e aprendizagem à distância, onde são colocadas virtualmente todas as matérias lecionadas nas aulas, bem como informações importantes das unidades curriculares em

estudo, conteúdos programáticos e ainda os sumários, e todo um manancial de informações relevantes das unidades curriculares. Os estudantes têm acesso a estas plataformas através de uma password que lhes permite a entrada e visualização da informação de cada unidade curricular, que compõe o seu plano de estudos semestral e/ou anual.

Dentro das plataformas eletrónicas de apoio ao ensino ou plataformas de *E-Learning* há diferentes acessos (login = entradas digitais) porque, por exemplo,um docente acede e tem permissões diferentes das de um estudante, bem como de um(s) técnico(s) que dá apoio associado a estas plataformas. Neste sentido, o estudante pode aceder em qualquer parte do mundo aos seus conteúdos académicos, bem como pode consultar, estudar, avaliar e gerir as informações que tem à sua disposição virtualmente,relativas à sua ligação a uma determinada IES. Usualmente também são colocadas on-line nas plataformas as avaliações e classificações relativas aos estudantes de cada unidade curricular, com os dados "mínimos" relativos a esses estudantes. E aqui entende-se que os dados "mínimos" devem ser os estritamente necessários à identificação do estudante, como seja o nome, a turma, a classificação final dessa unidade curricular. Assim parece-me que com estes dados haverá forma de avaliar a igualdade bem como a justiça social (e académica) dos estudantes porque podem aferir e comparar, entre todos, os resultados obtidos e as diferentes classificações.

Nas plataformas,o acesso deve ser restrito e limitado enquanto membros da IES, uma vez que o acesso livre e sem restrições a qualquer pessoa externa da IES compromete e pode ameaçar a segurança digital da plataforma, bem como a segurança dos seus utilizadores e da informação contida nestas plataformas.

3.2 Funcionários docentes

Um funcionário docente é um professor/formador da IES. É um membro efetivo do segundo grupo mais importante da IES.

Dentro da sua atividade profissional, um funcionário docente tem de avaliar a aprendizagem dos seus estudantes de acordocom parâmetros definidos para o efeito. Assim, são criadasas pautas de avaliação que devem conter algumas informações dos estudantes: as indispensáveis e com os mínimos dados adicionais possíveis; de acordo com o princípio da minimização dos dados pessoais - (alínea c) do n.º 1 do artigo 5.º do RGPD).

Na sequência da publicação da Diretriz n.º 1/2018 da CNPD "Disponibilização de dados pessoais dos estudantes, dos docentes e demais trabalhadores no sítio da Internet das instituições de ensino superior", este documento analisa e adverte sobre a disponibilização das pautas de avaliação dos docentes aos estudantes, bem como sobre os relatórios dos inquéritos pedagógicos dos docentes. Estes últimos devem ser anónimos, bem como confidenciais, e a sua publicitação deve estar confinada à instituição de ensino superior e aos demais docentes envolvidos. Neste âmbito, os avaliadores e o/s avaliado/s deve/m estar anonimizado/s e a sua divulgação (publicitação) deve estar restrita à comunidade da IES.

Relativamente às pautas de avaliação dos estudantes,entre os seus dados pessoais temos informações-base como o nome completo, o número de estudante, a nota obtida, e a turma. Estes últimos são os dados essenciais necessários para a disponibilização (publicitação) aos estudantes. Ao tornar públicas estas pautas, deve-se ter sempre em linha de conta que não devem estar em sítio web aberto e desprotegido, e de fácil acesso a qualquer pessoa, tendo por regra-base alguns filtros de encaminhamento, até à disponibilização total para o utilizador (estudante). Nas pautas não devem figurar (publicamente) informações adicionais sobre o estudante, como sejam a tipologia do aluno, a informação das faltas (exceto se for condição para a avaliação a frequência de um número mínimo de aulas), a situação financeira das propinas do aluno,e se é bolseiro/candidato a apoio social ou se tem alguma condição diferente enquanto estudante da IES. Com estas regras básicas de respeito pela vida privada dos estudantes, pretende-se que no âmbito da publicitação das notas, estes vejam acautelados os seus direitos de privacidade, que visam garantir os princípios da transparência e controlo da atividade de avaliação. No entanto, e por outro lado, há a mais-valia de haver uma pauta geral para comparabilidade de todos os estudantes dessa turma, através de listagem dos resultados obtidos pelos estudantes. Os princípios da imparcialidade, da justiça e da igualdade entre

todos os estudantes, são objetivos a atingir aquando da publicitação de uma pauta de turma. Assim, pretende-se responder ao paradoxo de limitação da privacidade versus publicação dos dados pessoais, duas premissas importantes para responder com assertividade ao direito primordial da privacidade dos dados académicos de um qualquer estudante. Esta é uma matéria muito sensível para os docentes de uma IES, porque quando a publicitação de resultados académicos não é bem estruturada e organizadapela IES, pode afetara privacidade e confidencialidade dos resultados dos estudantes enquanto "proprietários" de dados académicos.

Em virtude da publicitação dos dados académicos (resultados de avaliações), há que ter em linha de conta de que informações como o apoio social, as faltas e ainda outros dados sobre o estudante, será sempre informação excessiva relativamente ao objetivo que a pauta visa cumprir. Deve-se ter em linha de conta sempre o princípio da minimização dos dados, princípio que está consagrado no RGPD, uma vez que os dados devem ser limitados às necessidades específicas, em estrita consonância com as finalidades pretendidas.

Desta forma, a transparência e o controlo da atividade de ensino, bem como os princípios da justiça e da igualdade entre estudantes, faz com que o princípio da minimização dos dados seja um objetivo cada vez mais utilizado. Para responder a todas estas questões de proteção dos resultados, devem as pautas ser simples, lineares e com o mínimo de informações adicionais e complementares sobre os estudantes.

Os docentes estão então encarregados e obrigados, assim como qualquer profissional, ao sigilo profissional, uma vez que as informações pessoais e académicas, e nomeadamente os resultados obtidos pelos alunos, são do foro privado e pessoal de cada estudante.

3.3 Funcionários não docentes

Os funcionários não docentes são os administrativos ou técnicos que trabalham em prol da boa atividade administrativa e académica da IES. A eles,entre outras tarefas, competeo tratamento dos dados dos estudantes, mediante sigilo profissional e ainda usando a pseudonimização (tratamento de dados que permite não identificar os dados pessoais com os seus titulares). Também é através destes profissionais que são trocadas as informações estatísticas com outras IES ou com os órgãos de chefia ou órgãos coordenadores das IES.

No âmbito do sigilo profissional, um funcionário não docentenecessita de seguir o código deontológico e assumir comportamentos éticos, que deverão seros pilares basilares de atuação deste profissional. Assim, um administrativo/técnico não pode divulgar quaisquer dados ou listas, bem como informações pertencentes aos estudantes ou docentes dessa mesma IES. Todos os trabalhos e tarefas relativos, tanto aos estudantes,como aos docentes, são da responsabilidade dos seus funcionários, e os dados emanados, trocados ou tratados devem permanecer na esfera académica ou educativa dessa IES. As informações pessoais, tanto dos estudantes como dos docentes, ou ainda dos funcionários não docentes, devem ser guardadas e limitadas,e o seu acesso deve serrestrito de forma a que estejam protegidas de uma utilização livre e indiscriminada por qualquer pessoa internaou externa da IES. Um funcionário não docente recebe e trata informações de toda a comunidade académica, sendo que estas devem estar protegidas e serem limitadas para as finalidades em causa. Não pode um técnico/administrativo,por seu livre e espontâneo arbítrio, divulgar, destruir, acrescentar ou suprimir informações, sem que estas estejam de acordo com as linhas de orientação informacional e institucional da IES, e devem estar consignadas à execução dasua atividade profissional.

Cada vez mais, temos na informática um recurso precioso e útil, que ajuda substancialmente na elaboração rápida dos documentos académicos, entre outros. Para que não haja insegurança informática e informacional, devem as IES trabalhar em rede corporativa, uma vez que é necessária a colaboração de todos os departamentos, em prol do

bom desenvolvimento e da boa atividade da IES. Nesta linha de pensamento, uma IES funciona como uma equipa multidisciplinar em que todos departamentos trabalham uns para os outros, sempre com o objetivo primordial de protegerem a IES, tornando-a uma instituição de sucesso e segura acima de tudo.

4. Implementação do RGPD numa Instituição de Ensino Superior

A matéria de proteção de dados e privacidade do RGPD e a sua aplicação numa IES carece de um pressuposto, de que é necessário implementar e transferir para a IES todos os procedimentos da proteção de dados, para que esta funcione em conformidade com o RGPD.

Santos, A., 2017, pág. 1, escreve que a informação é uma matéria tão importante "daí ser necessária a sua proteção adequada, desde a proteção de informação de um indivíduo à proteção de informação de um Estado, uma vez que uma simples fuga de dados pode desencadear graves crises locais e mundiais". No seguimento do que foi anteriormente referido, uma boa proteção da informação pessoal de um indivíduo (ou de um estudante) leva a que se desencadeie uma boa proteção de uma comunidade académica global, com segurança e confidencialidade, o que leva à dupla garantia de privacidade pessoal de qualquer estudante ou comunidade de uma IES.

A introdução e/ou implementação do RGPD numa IES pressupõe a aplicação de um plano de ações a desenvolver dentro da IES, com os seguintes objetivos (cinco) específicos, e pela ordem apresentada abaixo:

1.º Designação de um EPD;

2.º Mapeamento dos dados pessoais objeto de tratamento;

3.º Priorização das ações a desenvolver;

4.º Organização dos processos internos;

5.º Documentação da conformidade com o RGPD.

Na implementação do RGPD numa IES, deve-se começar pela nomeação do EPD ou DPO para que este possa verificar e mapear todos os dados pessoais que são objeto de tratamento pela IES. Seguidamente há que priorizar as ações a desenvolver, caracterizando as mais importantes, para estarem em primeiro na linha de ações a executar. Depois de estarem as prioridades analisadas e identificadas, deve-se organizar os processos internos, para por último verificar a conformidade com o RGPD e se todos os processos e procedimentos respeitam e estão de acordo com as regras do RGPD.

Assim, como acontece na área da qualidade, também a segurança e proteção da informação tem uma norma internacional que é a ISO 27701 (Sistema de gestão de segurança e proteção da informação). Esta norma deriva da ISO 27001 (Sistema de gestão e segurança da informação) que procede à certificação das organizações na área da segurança da informação. O seu objetivo principal é o de implementar um sistema de gestão composto por um conjunto de requisitos, processos, procedimentos, e controlos para a segurança da informação. Na implementação de uma norma de cariz internacional como esta, uma organização tem de possuir um conjunto de requisitos, e ajustar os seus controlos da informação às normas impostas pela entidade certificadora.

No que respeita a esta norma internacional (ISO 27701), esta direciona-se sobre a gestão da privacidade da informação, em conformidade com as regras da proteção de dados do RGPD. No art. 42.º do RGPD - Certificação, podem as organizações adotar a criação de procedimentos de certificação, com vista a garantirem o cumprimento dos requisitos impostos pelas normas internacionais de proteção de dados. Assim como nas empresas se adotam normas reguladoras, com padrões e procedimentos bem definidos, para serem certificadas, também a segurança dos dados pessoais e a proteção da informação é um objetivo para uma IES.

Pode-se ver na Figura 4 (abaixo) que há todo um conjunto de requisitos importantes para estar em conformidade com a ISO 27001. Desde o contexto da organização até à melhoria contínua, e passando pela avaliação de desempenho e bem como pela liderança,

há todo um manancial de regras e requisitos que a organização tem de possuir, para que o sistema de gestão e segurança de informação funcione.

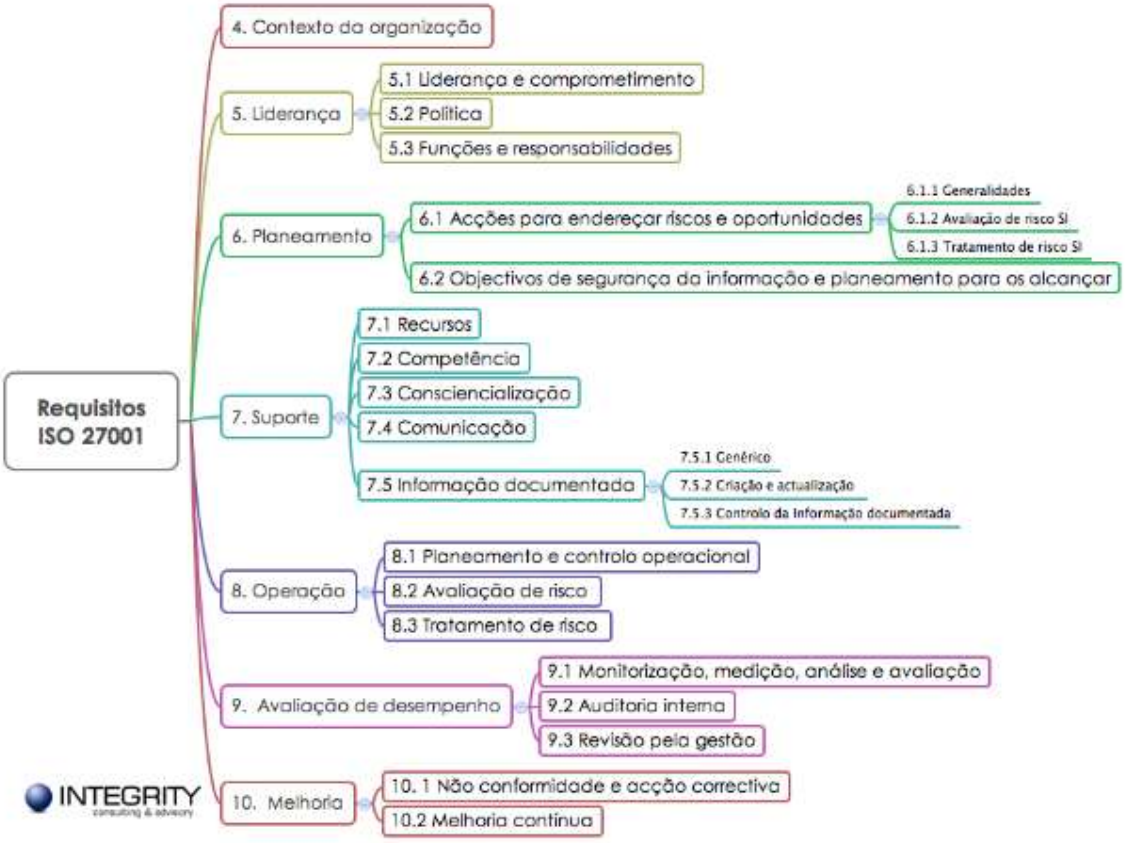


Figura 4 – ISO 27001 – Requisitos

[Imagem retirada de: https://www.27001.pt/iso27001_3.html]

Na figura acima, estão listados os requisitos necessários para a implementação na norma ISO 27001, que como se pode ver, estão definidos e elencados bem como especificados e enumerados por operações e suboperações. A título de exemplo, um dos requisitos acima visíveis é a avaliação de desempenho que pressupõe que haja a monitorização, medição, análise e avaliação, uma auditoria interna e a revisão pela gestão.

Já na imagem seguinte, Figura 5 (figura abaixo), estão enunciados um conjunto de controlos da ISO 27001 que as organizações devem possuir, para que a norma produza efeitos positivos e se revele eficaz. Entre os vários pontos que se podem analisar abaixo, destaca-se a segurança de recursos humanos, a existência de políticas de segurança, as

relações com os fornecedores e a conformidade das práticas e procedimentos que a IES deve ter. É de notar que estas figuras dos requisitos e dos controlos da norma ISO 27001 estão direcionadaspara o nível empresarial, no entanto,o objetivo desta análise foi transpor para uma organização como uma IES. Ora, entende-se que com uma norma destas, uma IES precisaria de responder com os requisitos, para poder controlar as diferentes áreas específicas que condicionam à boa operacionalização de uma norma certificadora de qualidade da segurança e da proteção de dados.

Figura 5 – ISO 27001 - Controlos

[Imagem retirada de: https://www.27001.pt/iso27001_3.html]

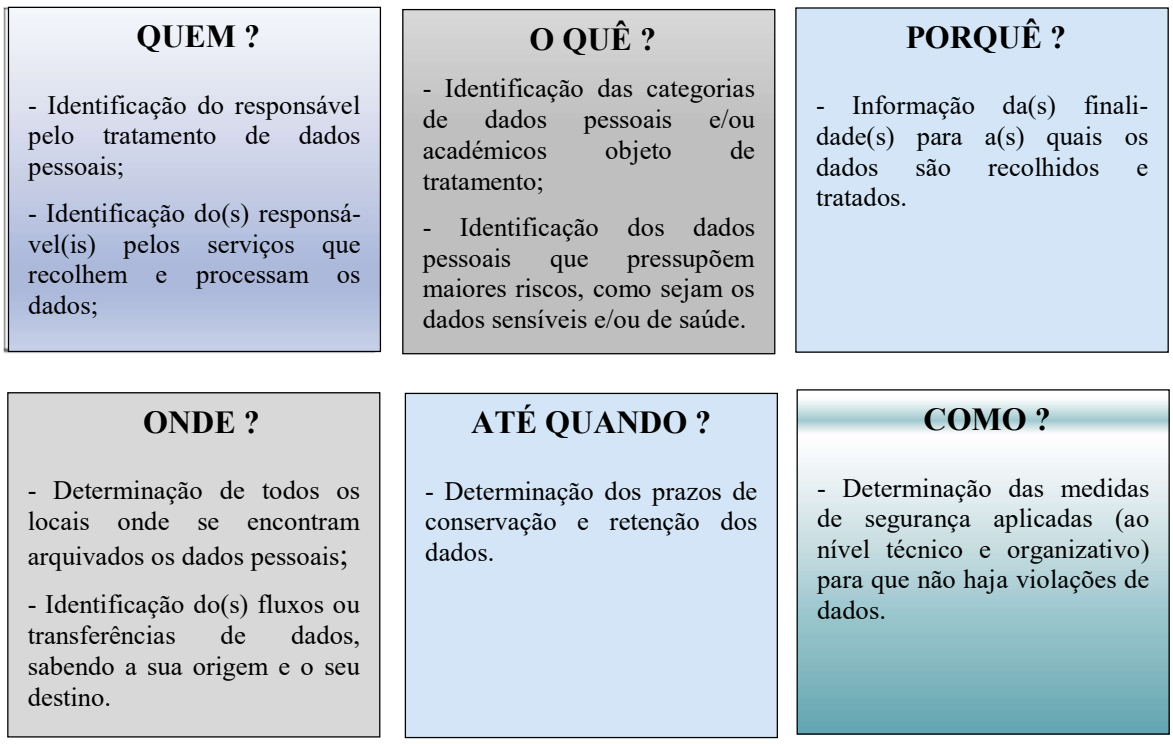
Nesta imagem acima, pode-se verificar a existência de 14 tipos de controlos que diferem entre eles, nos diversos âmbitos de atuação de uma organização, no entanto, a totalidade dos mesmos faz com que na esfera global, a norma tenha sucesso e o sistema de gestão e de segurança da informação se revele eficaz.

Com o controlo dos acessos de todos os funcionários docentes e não docentes, com a verificação da conformidade da regulamentação existente com o RGPD, com as relações

bem definidas com os fornecedores, com uma boa gestão da informação e segurança das comunicações, com todos estes e outros fatores controlados, assim se consegue minimizar o risco de ameaças e violações da privacidade da informação de uma IES.

4.1 O mapeamento dos dados

Na implementação e adequação do RGPD para uma IES, há que fazer o levantamento completo e prévio de todos os dados pessoais tratados pela mesma. Para este levantamento completo de dados é necessário conseguir responder às seguintes questões de natureza informacional:



Na operação de mapeamento dos dados pessoais e/ou académicos, uma IES possui uma ilimitada gama de dados pessoais dos seus estudantes, bem como os dados académicos ou estatísticos, e ainda os dados dos docentes, e dos funcionários não docentes, bem como informação específica de fornecedores ou ainda informação económico-financeira da própria vida da IES, entre outros dados.

Assim apresentam-se abaixo listadas as tipologias de dados que uma IES possui, bem como efetua o tratamento dos seguintes dados:

_____dados pessoais _____

DE QUEM ? (origem)

Estudantes

Não Docentes

Docentes

Fornecedores

Entidades supervisoras

Outras IES

QUE TIPOS DE DADOS ? (categorização de dados)

Informações pessoais

Informações académicas

Informações profissionais

Informações de cariz familiar

Informações económico-financeiras

Informações contabilísticas e fiscais

Dados estatísticos da(s) IES

Informações relativas à saúde

Dados sensíveis

Dados biométricos

Dados internos da IES

PARA QUÊ ? (finalidades)

Constituição dos processos dos estudantes

Finalidades académicas

Gestão de Recursos Humanos

Efeitos fiscais

Finalidades económico-financeiras

Qualificação/Valorização académica e profissional

Transferência de dados entre IES

Informações estatísticas para entidades supervisoras

PARA QUEM ? (destino)

Estudantes

Não Docentes

Docentes

Fornecedores

Outras IES

Entidades supervisoras

CANAIS DE COMUNICAÇÃO ?

Internet

Correio eletrónico

Linha telefónica

Redes sociais

Imprensa local, regional ou nacional

Publicidade e/ou Marketing

4.2 Avaliação de risco

A implementação do RGPD numa IES, assim como em todas as áreas de negócio, gera riscos que necessitam de ser avaliados e previstos. O risco é o "efeito da incerteza no alcance dos objetivos da organização". Pensar a implementação do RGPD sem pensar os riscos e as oportunidades daí resultantes, é "entregar o ouro ao bandido", quer isto dizer que não se pensou numa avaliação global da implementação de uma qualquer medida e/ou processo novo. Prever e avaliar a gestão dos riscos de um procedimento/processo novo é antever as possibilidades e/ou probabilidades, bem como as ameaças ao bom desenvolvimento desse processo. A avaliação de risco prevê, considera e questiona a abordagem e o aparecimento de resultados indesejáveis, ou de ameaças previsivelmente existentes.

Chiarini, A., 2017 refere que o processo "aplica não só o pensamento baseado no risco nos resultados indesejáveis, mas também às oportunidades que são identificadas através do processo de análise do risco". Assim, há que identificar oportunidades que surgem através da análise do risco, como sejam os fatores indesejáveis, as ameaças, e a enumeração dos riscos (que devem ser identificados, classificados, considerados e controlados) para minimizar todo o processo de implementação de um novo procedimento/bem/serviço.

Na Figura 6 (abaixo) podemos analisar o conceito de risco e como está definido, bem como,ele aparece na implementação de algum bem ou serviço novo. Ao criar e propor uma regulamentação nova numa IES, o risco aparece quando se interligam todos os fatores: a vulnerabilidade, a ameaça e o ativo (bem/processo ou serviço). Na interligação destes fatores, o sucesso global será maior quanto menor for o risco (mínimo risco). Veja-se abaixo a Figura 6, cuja imagem nos dá um "desenho" de como surge o risco:

Figura 6 – O risco (definição)

[Imagem retirada de: https://thumbs.dreamstime.com/z/avaliação-de-risco-24484063.jpg]

A interligação dos três fatores (Figura 6) identificados abaixo produz o aparecimentodo risco:

- Ameaças
- Vulnerabilidade
- Ativo(s)

A avaliação de risco é um procedimento imprescindível e muito importante, porque através dos fatores mencionados acima, poderemos verificar e identificar se há um risco máximo ou mínimo, de acordo com as condicionantes apresentadas anteriormente e das quais depende a quantificação e/ou mensuração do risco. Analise-se a imagem abaixo: Figura 7 – Avaliação de risco, onde é percetível a quantificação maior ou menor do risco.

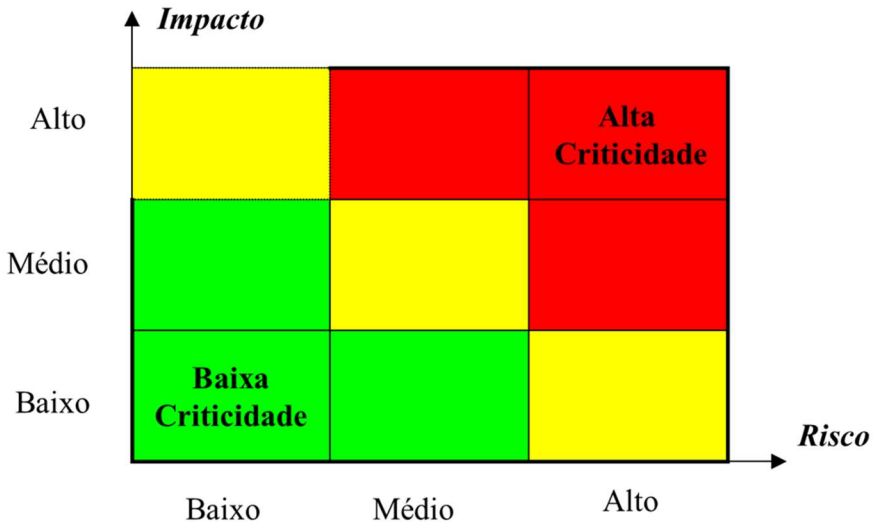


Figura 7 – Avaliação de risco

[Imagem retirada de: https://minutodaseguranca.blog.br/ciso-chief-information-security-officer/criticidade/]

Pode-se analisar na figura acima, que quanto maior for o impacto maior é nível de risco associado ao processo, e vice-versa: quando o impacto é baixo, o nível de risco baixa também. Assim há baixa criticidade quando o fator de impacto é menor.

4.3 Implementação

Para a implementação de uma Política de Privacidade numa IES, como foi anteriormente explicado, é necessário saber quais são os dados que possuímos (mapeamento de dados) e ainda devemos conseguir avaliar o risco: saber se ele é mínimo ou não. Com a introdução deste novo regulamento, este deveria garantir que a diminuição do risco era expectável. No entanto e como pudemos analisar anteriormente a implementação de algo novo pressupõe uma avaliação do impacto e consequentemente se o risco envolvido é máximo ou mínimo.

4.3.1 Arquivo e conservação de documentos

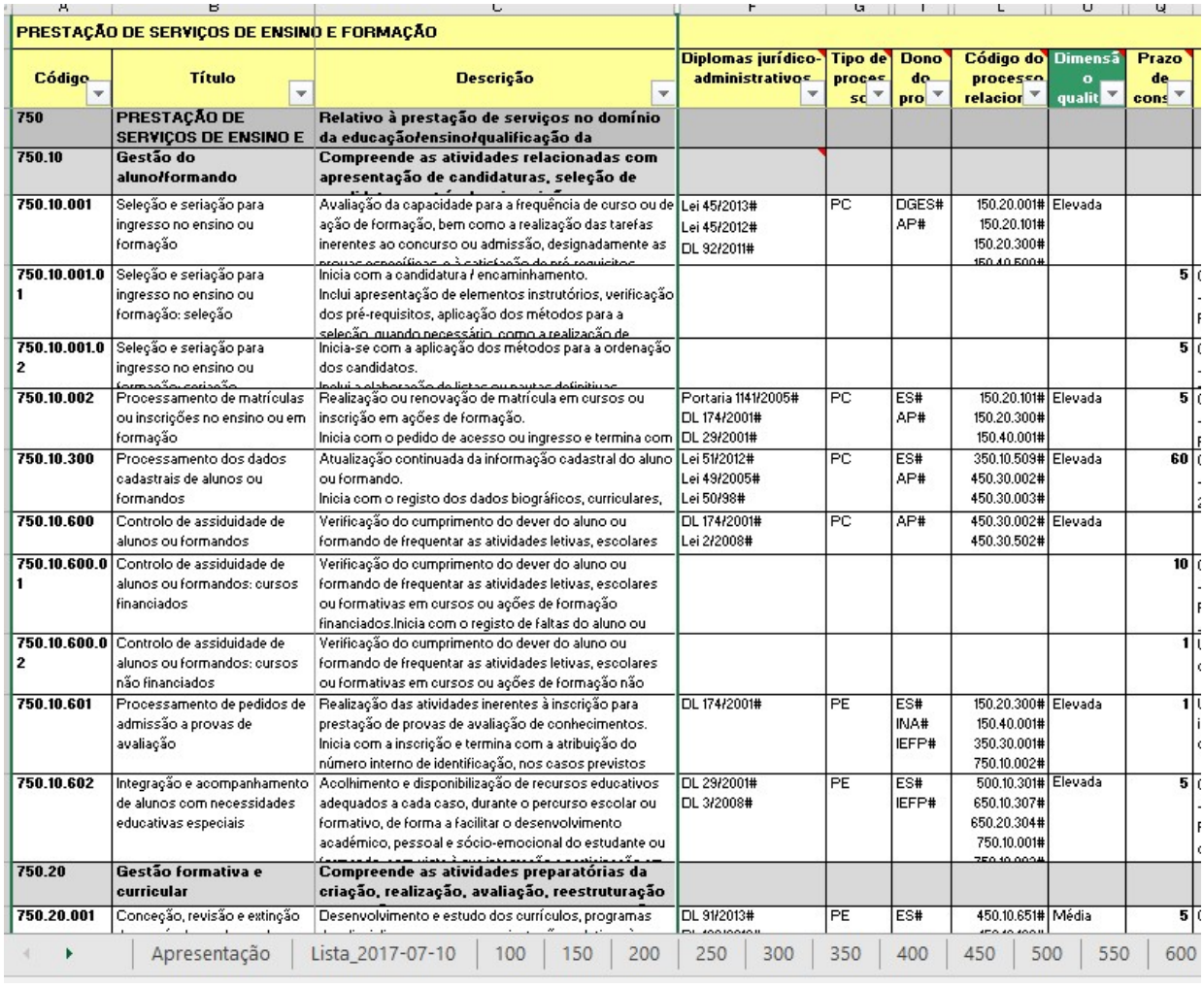
Muitos são os documentos emanados por uma IES, e todos com informação distinta e de interesse académico, profissional e também arquivístico. Sendo que o arquivo e a conservação dos documentos são da responsabilidade da IES, esta entidade distribui pelos seus departamentos esta responsabilidade de maneira partilhada. No entanto, há um departamento e/ou pessoa responsável pelo arquivo, cujas orientações e diretrizes seguem a filosofia da IES, bem como a legislação aplicável nesta matéria. Também há regulamentação legal avulsa que determina o tempo que os documentos devem ser conservados nos locais de arquivo, bem como a separação por áreas de interesse e a frequência de consulta previsível, ou seja, a importância arquivística desses mesmos documentos.

O arquivo é tão importante que, a necessidade de consultar documentos bem arquivados, tornar-se-á tão fácil quanto se assemelha ao acesso de forma digital (localização rápida de ficheiro digitais). Um bom arquivo produz uma sensação de organização e orientação para resultados rápidos e eficazes. Com um sistema de gestão funcional e organizado do arquivo, facilmente se consegue aceder aos documentos arquivados em local próprio, uma vez que estão catalogados e classificados, de acordo com as normas arquivísticas da IES e/ou as normas gerais legais de organização, catalogação e classificação da informação.

Atualmente já há uma sensibilização ecológica para a redução do papel (impressões/documentação em papel), para que ao nível ambiental, não se produza nem se consuma tanto papel como estava a ser consumido. Com as orientações nacionais e internacionais para um ambiente mais sustentável, há que ponderar a importância de imprimir ou não um documento, uma vez que também se pode arquivar digitalmente nos computadores (através de discos externos ou nuvens – *clouds* ou outros locais de arquivo digital).

No âmbito da organização e classificação da informação, temos a nível nacional o classificador da Administração Pública: MEF (Macroestrutura Funcional) que tem estipulado ao nível da AP determinados prazos de conservação administrativa e decisão final quanto ao destino dos documentos. Neste classificador nacional (a MEF) conseguimos ver uma lista integrada de documentos administrativos da AP, cujos prazos de arquivo e de conservação estão previamente definidos, e sobre os quais sabemos o seu prazo de retenção na organização.

Na figura abaixo pode-se verificar os documentos (tipologias) e quais os prazos de conservação associados a cada documento específico.

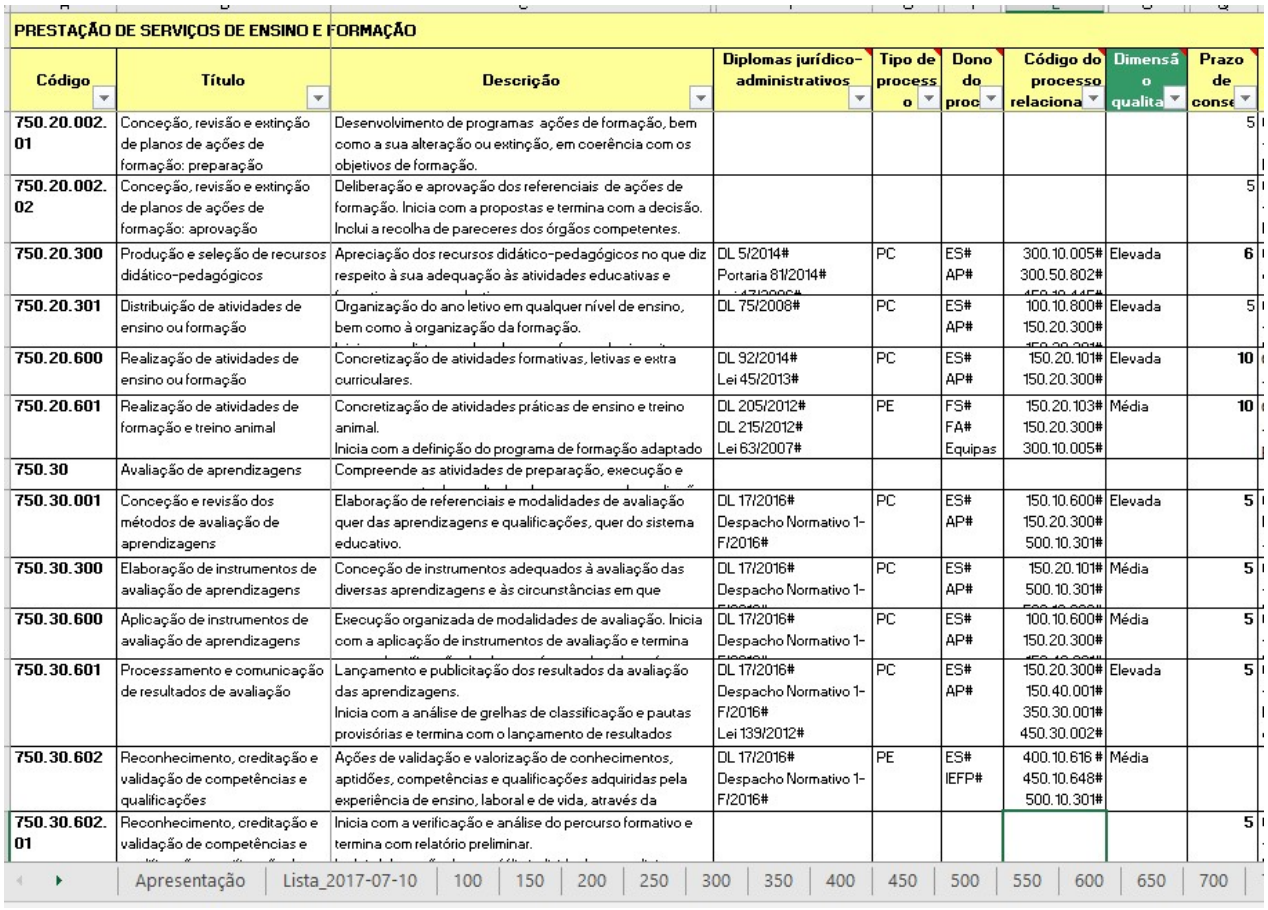


PRESTAÇÃO DE SERVIÇOS DE ENSINO E FORMAÇÃO								
Código	**Título**	**Descrição**	**Diplomas jurídico-administrativos**	**Tipo de proces so**	**Dono do pro**	**Código do processo relacior**	**Dimensã o qualit**	**Prazo de cons**
750	**PRESTAÇÃO DE SERVIÇOS DE ENSINO E**	**Relativo à prestação de serviços no domínio da educação/ensino/qualificação da**						
750.10	**Gestão do aluno/formando**	**Compreende as atividades relacionadas com apresentação de candidaturas, seleção de**						
750.10.001	Seleção e seriação para ingresso no ensino ou formação	Avaliação da capacidade para a frequência de curso ou de ação de formação, bem como a realização das tarefas inerentes ao concurso ou admissão, designadamente as	Lei 45/2013# Lei 45/2012# DL 92/2011#	PC	DGES# AP#	150.20.001# 150.20.101# 150.20.300#	Elevada	
750.10.001.01	Seleção e seriação para ingresso no ensino ou formação: seleção	Inicia com a candidatura / encaminhamento. Inclui apresentação de elementos instrutórios, verificação dos pré-requisitos, aplicação dos métodos para a						**5**
750.10.001.02	Seleção e seriação para ingresso no ensino ou	Inicia-se com a aplicação dos métodos para a ordenação dos candidatos.						**5**
750.10.002	Processamento de matrículas ou inscrições no ensino ou em formação	Realização ou renovação de matrícula em cursos ou inscrição em ações de formação. Inicia com o pedido de acesso ou ingresso e termina com	Portaria 1141/2005# DL 174/2001# DL 29/2001#	PC	ES# AP#	150.20.101# 150.20.300# 150.40.001#	Elevada	**5**
750.10.300	Processamento dos dados cadastrais de alunos ou formandos	Atualização continuada da informação cadastral do aluno ou formando. Inicia com o registo dos dados biográficos, curriculares,	Lei 51/2012# Lei 49/2005# Lei 50/98#	PC	ES# AP#	350.10.509# 450.30.002# 450.30.003#	Elevada	**60**
750.10.600	Controlo de assiduidade de alunos ou formandos	Verificação do cumprimento do dever do aluno ou formando de frequentar as atividades letivas, escolares	DL 174/2001# Lei 2/2008#	PC	AP#	450.30.002# 450.30.502#	Elevada	
750.10.600.01	Controlo de assiduidade de alunos ou formandos: cursos financiados	Verificação do cumprimento do dever do aluno ou formando de frequentar as atividades letivas, escolares ou formativas em cursos ou ações de formação financiados.Inicia com o registo de faltas do aluno ou						**10**
750.10.600.02	Controlo de assiduidade de alunos ou formandos: cursos não financiados	Verificação do cumprimento do dever do aluno ou formando de frequentar as atividades letivas, escolares ou formativas em cursos ou ações de formação não						**1**
750.10.601	Processamento de pedidos de admissão a provas de avaliação	Realização das atividades inerentes à inscrição para prestação de provas de avaliação de conhecimentos. Inicia com a inscrição e termina com a atribuição do número interno de identificação, nos casos previstos	DL 174/2001#	PE	ES# INA# IEFP#	150.20.300# 150.40.001# 350.30.001# 750.10.002#	Elevada	**1**
750.10.602	Integração e acompanhamento de alunos com necessidades educativas especiais	Acolhimento e disponibilização de recursos educativos adequados a cada caso, durante o percurso escolar ou formativo, de forma a facilitar o desenvolvimento académico, pessoal e sócio-emocional do estudante ou	DL 29/2001# DL 3/2008#	PE	ES# IEFP#	500.10.301# 650.10.307# 650.20.304# 750.10.001#	Elevada	**5**
750.20	**Gestão formativa e curricular**	**Compreende as atividades preparatórias da criação, realização, avaliação, reestruturação**						
750.20.001	Conceção, revisão e extinção	Desenvolvimento e estudo dos currículos, programas	DL 91/2013#	PE	ES#	450.10.651#	Média	**5**

Apresentação | Lista_2017-07-10 | 100 | 150 | 200 | 250 | 300 | 350 | 400 | 450 | 500 | 550 | 600

Figura 8– MEF – Prestação de serviços de ensino e formação_1

[Imagem retirada de: http://arquivos.dglab.gov.pt/servicos/documentos-tecnicos-e-normativos/lista-de-documentos/]



PRESTAÇÃO DE SERVIÇOS DE ENSINO E FORMAÇÃO

Código	Título	Descrição	Diplomas jurídico-administrativos	Tipo de processo	Dono do proc	Código do processo relaciona	Dimensão qualita	Prazo de conse
750.20.002.01	Conceção, revisão e extinção de planos de ações de formação: preparação	Desenvolvimento de programas ações de formação, bem como a sua alteração ou extinção, em coerência com os objetivos de formação.						5
750.20.002.02	Conceção, revisão e extinção de planos de ações de formação: aprovação	Deliberação e aprovação dos referenciais de ações de formação. Inicia com a propostas e termina com a decisão. Inclui a recolha de pareceres dos órgãos competentes.						5
750.20.300	Produção e seleção de recursos didático-pedagógicos	Apreciação dos recursos didático-pedagógicos no que diz respeito à sua adequação às atividades educativas e	DL 5/2014# Portaria 81/2014#	PC	ES# AP#	300.10.005# 300.50.802#	Elevada	6
750.20.301	Distribuição de atividades de ensino ou formação	Organização do ano letivo em qualquer nível de ensino, bem como à organização da formação.	DL 75/2008#	PC	ES# AP#	100.10.800# 150.20.300#	Elevada	5
750.20.600	Realização de atividades de ensino ou formação	Concretização de atividades formativas, letivas e extra curriculares.	DL 92/2014# Lei 45/2013#	PC	ES# AP#	150.20.101# 150.20.300#	Elevada	10
750.20.601	Realização de atividades de formação e treino animal	Concretização de atividades práticas de ensino e treino animal. Inicia com a definição do programa de formação adaptado	DL 205/2012# DL 215/2012# Lei 63/2007#	PE	FS# FA# Equipas	150.20.103# 150.20.300# 300.10.005#	Média	10
750.30	Avaliação de aprendizagens	Compreende as atividades de preparação, execução e						
750.30.001	Conceção e revisão dos métodos de avaliação de aprendizagens	Elaboração de referenciais e modalidades de avaliação quer das aprendizagens e qualificações, quer do sistema educativo.	DL 17/2016# Despacho Normativo 1-F/2016#	PC	ES# AP#	150.10.600# 150.20.300# 500.10.301#	Elevada	5
750.30.300	Elaboração de instrumentos de avaliação de aprendizagens	Conceção de instrumentos adequados à avaliação das diversas aprendizagens e às circunstâncias em que	DL 17/2016# Despacho Normativo 1-	PC	ES# AP#	150.20.101# 500.10.301#	Média	5
750.30.600	Aplicação de instrumentos de avaliação de aprendizagens	Execução organizada de modalidades de avaliação. Inicia com a aplicação de instrumentos de avaliação e termina	DL 17/2016# Despacho Normativo 1-	PC	ES# AP#	100.10.600# 150.20.300#	Média	5
750.30.601	Processamento e comunicação de resultados de avaliação	Lançamento e publicitação dos resultados da avaliação das aprendizagens. Inicia com a análise de grelhas de classificação e pautas provisórias e termina com o lançamento de resultados	DL 17/2016# Despacho Normativo 1-F/2016# Lei 139/2012#	PC	ES# AP#	150.20.300# 150.40.001# 350.30.001# 450.30.002#	Elevada	5
750.30.602	Reconhecimento, creditação e validação de competências e qualificações	Ações de validação e valorização de conhecimentos, aptidões, competências e qualificações adquiridas pela experiência de ensino, laboral e de vida, através da	DL 17/2016# Despacho Normativo 1-F/2016#	PE	ES# IEFP#	400.10.616 # 450.10.648# 500.10.301#	Média	
750.30.602.01	Reconhecimento, creditação e validação de competências e	Inicia com a verificação e análise do percurso formativo e termina com relatório preliminar.						5

Apresentação | Lista_2017-07-10 | 100 | 150 | 200 | 250 | 300 | 350 | 400 | 450 | 500 | 550 | 600 | 650 | 700

Figura 9 – MEF – Prestação de serviços de ensino e formação_2

[Imagem retirada de: http://arquivos.dglab.gov.pt/servicos/documentos-tecnicos-e-normativos/lista-de-documentos/]

Nestas duas imagens estão catalogados documentos emanados dos serviços de ensino e formação (a título exemplificativo) e conseguimos saber através das tabelas visíveis, nas duas imagens acima, qual a importância do documento bem como o prazo de conservação associado ao mesmo. Tratam-se de duas imagens onde estão explanados os títulos dos documentos e ainda uma descrição do processo, bem como os diplomas legais associados aos documentos, e na coluna mais à direita da imagem, aparecem os prazos de conservação de cada um desses documentos.

4.3.2 Prazos de retenção

Como boa organização que é suposto ter, também para a documentação que está ao nosso dispor tem prazos de retenção ajustados à importância que os documentos possuem. Quer-se com isto dizer que um documento mais importante terá um prazo de retenção superior a outro de menor importância. Pudemos ver acima que há uma Macroestrutura Funcional (classificador MEF) na Administração Pública que também estipula o prazo de conservação/retenção dos documentos. Não é suposto ter prazos de retenção superiores aos previstos na Lei, em virtude de que uma retenção ou conservação superior à prevista também traz inconvenientes. Quando a retenção dos documentos acontece num prazo maior do que o previsto há a desvantagem de que aquele espaço de conservação não pode ser renovado ou reciclado para outra documentação. Também é inegável que se os prazos de conservação são maiores, menor é o fluxo de arquivo de documentos produzidos ou recebidos pela IES.

5. Criação de uma Política de Privacidade para uma Instituição de Ensino Superior

Uma IES tem um bem precioso que são os dados pessoais dos estudantes, e não somente estes, naturalmente que há outros dados a resguardar: dados académicos, dados relativos às propinas (pagamentos), dados relativos à saúde (por via da justificação de faltas), etc. Entre outros, um documento como um regulamento ou código de conduta e política de proteção de dados será concerteza um recurso útil para uma IES.

Esta política de privacidade surgiu da ideia de uma lacuna que era a inexistência desta ferramenta por parte das IES portuguesas, sendo que muitas não dispunham deste documento, até ao momento da publicação do RGPD. Poucas entidades tinham em 2016 um regulamento de privacidade, e fui consolidando esta informação com as minhas pesquisas, uma vez que a maior parte das IES só tinham no seu website uma página (folha A4) com algumas regras simples sobre a privacidade dos seus dados. Nos websites que consultei, pude verificar que as políticas de privacidade eram simples e tinham pequenos trechos de informação do RGPD, bem como também eram muito limitativas e restritivas quanto ao teor da informação contida.

Na minha ótica uma Política de Privacidade é um regulamento interno que rege a proteção de dados das IES, ou seja, trata-se de um conjunto de artigos destinados a regulamentar e a proteger a privacidade dos dados pessoais dos estudantes. Com este documento estão organizadas e salvaguardadas todas as premissas para que não haja uma "falha" de segurança, por parte dos estudantes e para eles, nomeadamente para elevar a proteção dos seus dados.

Uma IES sem uma política de proteção de dados é como uma sociedade sem uma política de segurança, trata-se de uma ferramenta essencial ao bom desenvolvimento e crescimento duma Instituição.

Assim ao proceder à introdução de uma Política de Privacidade, uma IES está a munir-se de uma ferramenta importante que a ajudará a manter-se protegida de fatores indesejáveis, como seja a segurança da informação, ou mais especificamente a falta dela, ao nível dos dados pessoais ou académicos dos estudantes. Este regulamento/política ajudará a regular a proteção de dados da IES, de maneira a que os dados estejam preservados e limitados de influências e/ou lacunas informáticas ou possível insegurança (exposição fraudulenta) das informações conservadas e resguardadas pelas IES. Este documento também ajudará no controlo e disseminação ou troca de informação académica por quem trabalhe na IES, tanto seja pelos funcionários docentes, bem como pelo pessoal não docente da Instituição, uma vez que irá regulamentar e explicar, através de normas e artigos explícitos, toda a conduta e política de privacidade que a Instituição deve seguir.

Por ser importante, criou-se a Política de Proteção de Dados abaixo, que de forma genérica vai regulamentar a área da proteção de dados de uma IES. Na criação da regulamentação que se apresenta abaixo, este segue todas as orientações do RGPD e demais legislação nesta matéria, e o seu objetivo principal é o de criar uma ferramenta imprescindível para uma qualquer IES.

Assim, na proposta de documento abaixo – Política de Privacidade, podemos distinguir quatro matérias principais a proteger: que são os deveres e os direitos dos estudantes bem como os deveres e os direitos das IES, e ainda toda a informação geral sobre a aplicabilidade da privacidade, bem como as funções gerais do DPO/EPD. Há ainda lugar para definir como efetuar a fiscalização e propostas de sanções para situações de incumprimento. De um modo geral o documento abaixo apresenta um conjunto de regras de privacidade para serem seguidas por todos os intervenientes de uma IES, que conduzem indubitavelmente à segurança e proteção das mesmas.

No âmbito deste projeto apresenta-se de seguida uma proposta de Política de Privacidade (para o caso particular dos estudantes) para uma qualquer IES portuguesa. Investiu-se todo o esforço pessoal e académico para que esteja o mais legal e jurídico possível, no entanto, uma vez que não possuo formação académica na área do Direito, poderão registar-se algumas lacunas legais e jurídicas no documento abaixo proposto.

6. Proposta de uma Política de Privacidade para uma Instituição de Ensino Superior

(o caso particular dos estudantes)

POLÍTICA DE PRIVACIDADE

(INSTITUIÇÃO DE ENSINO SUPERIOR)

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto

1. A presente política de proteção de dados estabelece as regras de conduta relativas à proteção dos dados pessoais e académicos, ou outros dados relativos aos estudantes de uma Instituição de Ensino Superior, doravante designada por IES, e ainda defende os direitos e as liberdades fundamentais dos estudantes em termos de proteção da privacidade estudantil.

Artigo 2.º

Âmbito de aplicação

1. O presente regulamento aplica-se a toda a comunidade académica bem como à comunidade docente e não docente das IES nomeadamente no que respeita ao tratamento e transferência de dados e à livre circulação dos mesmos, sendo a IES a entidade responsável, ao abrigo da legislação em vigor.

Artigo 3.º

Aplicabilidade

1. A presente política de privacidade aplica-se a todos os estudantes da IES, independentemente do seu perfil, nacionalidade, raça, religião, origem ou finalidades académicas.

CAPÍTULO II

(DIREITOS E DEVERES DOS TITULARES DE DADOS)

Secção I – Direitos dos titulares dos dados

Artigo 4.º

Direito de Informação e Acesso aos Dados Pessoais

1. Os estudantes têm o direito a saber quem é o responsável pelo tratamento dos seus dados dentro da respetiva IES.
2. Têm ainda o direito, às seguintes informações sobre a recolha e o tratamento dos seus dados:

a) as finalidades;

b) as categorias;

c) os destinatários dos dados recolhidos que foram ou serão tratados e/ou divulgados;

d) ou no caso de troca de informações com entidades terceiras, no âmbito da respetiva transferência dos seus dados pessoais;

3. Os estudantes podem solicitar o acesso ou a consulta aos seus dados pessoais ou académicos.

Artigo 5.º

Direito de Retificação

1. Os estudantes têm o direito a solicitar a retificação, a correção ou a alteração dos seus dados pessoais por estaremerrados, inexatos ou incompletos.

Artigo 6.º

Direito ao Apagamento dos Dados («direito a ser esquecido»)

1. Os estudantes têm o direito de requerer o apagamento dos seus dados pessoais ou que sejam eliminadas as suas informações, quando tenham desaparecido os fundamentos de licitude do seu tratamento, ou quando tenham sido recolhidos ou tratados ilicitamente, ou ainda quando suceder de ser retirado o consentimento obrigatórioem que baseia o tratamento dos dados pessoais ou académicos.

Artigo 7.º

Direito de Oposição

1. Os estudantes têm o direito de se oporem em qualquer momento, por motivos pessoais e/ou académicos, ao tratamento dos seus dados pessoais e transferência dos mesmos para outras entidades, nomeadamente se não concordarem com o prosseguimento ou finalidades desse tratamento.

Artigo 8.º

Direito de notificação e comunicação

1. Todos os estudantes de uma IES têm o direito, em caso de violação dos seus dados pessoais, de que seja notificada a autoridade de controlo, e informada sobre a situação específica,que resultou na violação da segurança e privacidade dos mesmos.

2. 2.Caso a violação dos dados seja relevante e implicar um elevado risco para os direitos dos estudantes, estes devem ser informados desta ocorrência, sem demora injustificada, nomeadamente da quebra de segurança e da privacidade previamente estabelecida.

Secção II – Deveres dos titulares de dados

Artigo 9.º

Dever de prestar informação correta e verdadeira

1. Os estudantes da IES, têm o dever de facultar todas as informações corretas e verdadeiras sobre si, necessárias aos fins a que se destinam.
2. As falsas informações/declarações prestadas são puníveis pela legislação em vigor.

Artigo 10.º

Dever de prestar o consentimento

1. Os estudantes da IES têm o direito de prestar o seu consentimento escrito, através de uma declaração, relativa ao tratamento e transferência dos seus dados pessoais e/ou académicos.
2. Se o consentimento do estudante disser respeito a outros assuntos, o pedido de consentimento deve ser apresentado de forma clara e inequívoca e que distinga claramente essas outras finalidades, como sejam a transferência de dados para outras organizações protocoladas com a IES.
3. O estudante pode em qualquer momento retirar o consentimento, o qual não compromete o que tiver sido efetuado/tratado até essa data, e esta operação deve ser tão fácil (retirar) como foi a de dar.

CAPÍTULO III

(DIREITOS E DEVERES DAS INSTITUIÇÕES DE ENSINO SUPERIOR)

Secção I – Direitos das Instituições de Ensino Superior

Artigo 11.º

Acesso à informação do estudante

1. A IES para o prosseguimento dos seus objetivos e finalidades tem o direito que lhe sejam facultados todos dados pessoais e académicos dos estudantes matriculados/inscritos nessa IES, bem como pode e deve realizar o tratamento desses dados dos estudantes.

Secção II – Deveres das Instituições de Ensino Superior

Artigo 12.º

Consentimento

1. Para alcançar as suas finalidades e em linha de orientação com a missão da IES,esta tem o dever de pedir o consentimento dos estudantes, quando seja necessário, para a o tratamento dos dados pessoais e/ou académicos dos mesmos.

Artigo 13.º

Recolha de dados pessoais

1. Uma IES,na prossecução das suas finalidades,tem de proceder à recolha dos dadospessoais e/ou académicos dos seus estudantes, dados esses que devem ser

osestritamente necessários para cumprimento de exigências legais, e ainda devem ser exatos, atualizados everdadeiros.

Artigo 14.º

Tratamento de dados pessoais

1. Após a recolha dos dados pessoais, a IES tem o dever de tratar corretamente e com segurança os dados, garantindo a sua proteção e confidencialidade, bem como a manutenção, conservação e o apagamento, caso seja necessário, ou através de solicitação do titular dos dados pessoais, dentro dos limites previstos por lei.

Artigo 15.º

Manutenção e conservação de dados pessoais

1. No âmbito das atribuições das IES, estas têm o dever de tratar e conservar os dados pessoais recolhidos dos estudantes, obedecendo aos prazos legais de conservação e retenção dos documentos, de acordo com as normas arquivísticas existentes na IES e demais legislação aplicável.

Artigo 16.º

Imparcialidade e Isenção

1. Todos os profissionais da IES (docentes e não docentes) devem ser isentos e imparciais, no cumprimento das atribuições relativas ao tratamento dos dados pessoais e/ou académicos dos estudantes.

Artigo 17.º

Dever de pedir consentimento ao titular dos dados pessoais

1. A IES (ou os seus responsáveis) dentro das competências que lhe são atribuídas, deve solicitar, no âmbito dotratamento dos dados dos estudantes, o respetivo consentimento explícito aos seus titulares de dados, informando desde logo a finalidade da recolha e tratamento desses dados.

Artigo 18.º

Dever de sigilo, proteção e confidencialidade dos dados pessoais

1. A IES, através dos seus responsáveis ou dos seus funcionários, tem o dever de protegere guardar com segurança a informação pessoal e/ou académica dos seus estudantes, no âmbito da prossecução das suas finalidades.

Artigo 19.º

Dever de Informação

1. A IES tem o dever de informar os estudantes quando solicitado pelospróprios, ede permitir o acesso à informação pessoal e académica dos mesmos,bem comode corrigir ou apagar, caso a informação não esteja correta e/ou verdadeira.

Artigo 20.º

Responsável pelo tratamento dos dados pessoais

1. A IES é responsável pela recolha,armazenamento, retificação, tratamento e proteção, garantindo a segurança e confidencialidadedos dados pessoais dos estudantes.
2. A IES tem o dever de nomear o Encarregado de Proteção de Dados (EPD/DPO).

CAPÍTULO IV

(ENCARREGADO DE PROTEÇÃO DE DADOS - *DATA PROTECTION OFFICER*)

Artigo 21.º

Funções do Encarregado de Proteção de Dados – EPD*(DPO)*

1. O EPD (ou *DPO – Data Protection Officer*) de uma IES tem o dever de informar e aconselhar a IES ou o seu subcontratante, bem como todos os profissionais da IES (docentes e não docentes) que efetuem o tratamento de dados, em relação às suas obrigações e deveres profissionais, no âmbito da prossecução dos objetivos da IES, nomeadamente sobre a legislação vigente em matéria de proteção e privacidade dos dados;
2. Deve controlar e coordenar a conformidade do tratamento dos dados com as disposições legais da proteção dos mesmos e assegurar a segurança da informação da própria IES;
3. Tem também de prestar aconselhamento, no caso de lhe ser solicitado, no âmbito da proteção dos dados e efetuar recomendações importantes, a todos os profissionais da IES, bem como de apoiar ou prestar aconselhamento, quando tal for solicitado,em relação à avaliação de impacto sobre a proteção de dados (e controla a sua realização, de acordo com o elencado no artigo 35.º do RGPD);
4. Por último, deve cooperar com a autoridade de controlo, e em caso de dúvidasconsultar esta entidade/autoridadecom o objetivo de assegurar a melhor proteção e privacidade dos dados pessoais dos estudantes dessaIES.

CAPÍTULO V

(DOS NORMATIVOS LEGAIS APLICADOS ÀS INSTITUIÇÕES DE ENSINO SUPERIOR)

Artigo 22.º

Controlo dos dados pessoais

1. No prosseguimento das suas atribuições, a IES deve de controlar e tratar os dados pessoais e/ou académicos dos seus estudantes e em caso de violação dos dados pessoais deve notificar a autoridade de controlo.

Artigo 23.º

Notificação à autoridade de controlo

1. Quando ocorra a violação de dados pessoais e/ou académicos dos estudantes, a IES tem o dever de notificar, no prazo de 72 horas, a entidade de controlo respetiva, relatando e reportando a situação ocorrida.

Artigo 24.º

Autoridade de Controlo

1. A entidade de controlo com competências definidas é a CNPD – Comissão Nacional de Proteção de Dados.

Artigo 25.º

Prazos de conservação e retenção dos dados pessoais e/ou académicos

1. Os dados pessoais e/ou académicos devem ser conservados pelo tempo estritamente necessário para cumprir a finalidade do seu tratamento, no âmbito da prossecução da missão da IES;
2. A IES deve fazer uma verificação e revisão organizativa periódica aos documentos administrativos emanados;

3. De acordo com o classificador MEF, a IES terá à sua disponibilidade um quadro de referência nacional para identificar, classificar e definir o prazo de conservação dos documentos dos estudantes.

CAPÍTULO VI

(FISCALIZAÇÃO E SANÇÕES)

Artigo 26.º

Entidade fiscalizadora

1. A entidade competente, a nível nacional, é a CNPD que poderá aplicar sanções e/ou coimas, consoante a gravidade da infração da proteção de dados pessoais e/ou académicos.

CAPÍTULO VII

(DISPOSIÇÕES FINAIS)

Artigo 27.º

Cumprimento do dever de proteção de dados

1. No caso de violação da proteção de dados pessoais e/ou académicos e a IES falhar no dever de privacidade e/ou proteção dos dados dos seus estudantes, sobre ela incorrerá aaplicação de sanções, multas ou coimas ou ainda estará sujeita ao poder de correção/supervisão e/ou advertência da CNPD.

Conclusão

Com a realização deste projeto, cujo tema da privacidade e proteção de dados é atual, interessante e está na "moda" falar do RGPD, regulamento tornado público há três anos atrás, mas cuja transformação e adaptação para o mundo empresarial e para a administração pública ainda irá durar mais algum tempo. Esta temática foi inicialmente abordada na sala de aulas do 1º ano do Mestrado em Administração Pública, e logo aí despertou o interesse e criou a motivação para uma investigação mais alargada e profunda do valor da proteção da privacidade do ser humano.

"Deixamos vestígios digitais em tudo o que fazemos. Com a reforma da proteção de dados na União Europeia, a nossa legislação estará preparada para o futuro e para a era digital." – Comissão Europeia, 2012. A era digital chegou e está para ficar, logo tem o sistema digital poderes absolutos e soberanos para uma evolução e imposição cada vez maior nas nossas sociedades atuais. A era digital revestiu-se de qualidades e mais-valias, a rapidez digital revolucionou a administração pública uma que vai conseguindo cada vez mais uma evolução administrativa e menos burocrática, o que atrai cada vez mais os jovens estudantes. A era digital corre o mundo, de uma ponta à outra em poucos minutos, e aquilo que se passa na China hoje, ainda hoje chega a outro continente longínquo na outra ponta do planeta. A difusão da informação não tem limites e neste âmbito o RGPD é considerado por muitos como o "salvador" da difusão segura e protegida da informação, que todos os dias é produzida em todo o mundo.

A Política de Privacidade proposta neste projeto é uma das ferramentas indispensável para as IES, ao nível da proteção dos dados dos seus estudantes. Foi extremamente difícil e tornou-se numa das limitações deste trabalho, a inexistência de base académica jurídica para a elaboração de um Código mais completo e generalizado à dimensão não só académica, mas aquela que é exigida por uma IES no seu todo – um Código/Regulamento geral e adequado a uma qualquer Instituição de Ensino Superior.

Devido a ser um tema muito atual e com muita informação recente para ser disseminada, verifico agora que um ano nesta área de estudo é pouco relevante e produtivo para um trabalho desta envergadura, principalmente porque esta temática tem muitas derivações e áreas de interesse tão ou mais importantes do que aquela que foi escolhida – a proteção de dados no ensino superior.

Com este projeto conclui-se que a matéria de proteção de dados no ensino superior, ainda está longe da verdadeira investigação científica e trabalhos nesta área da privacidade dos dados deveriam ser mais frequentes e atualizados. A balança da desigualdade da privacidade é notória e ao nível empresarial considero haver um maior entusiasmo e estudo autónomo, o que já não acontece com as organizações públicas.

Trabalhos futuros, como por exemplo, regulamentos internos de privacidade para as entidades/organizações são, na minha ótica, uma boa aposta académica, no entanto a dificuldade é atingir e focar nesta temática específica porque há demasiada informação dispersa e espalhada na internet.

Esta página foi intencionalmente deixada em branco

Bibliografia

- Calvão, F. U.(2018),*Direito da Proteção de Dados Pessoais – Relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina*, Porto:Universidade Católica Editora;

- Canotilho, J. J. G. e Moreira, V. (2007),*CRP – Constituição da República Portuguesa Anotada*, Coimbra: Coimbra Editora;

- Santos, A. (2017), *As Diretivas Comunitárias de Proteção de Dados Pessoais e a sua Aplicação em Portugal: Barreiras e Facilitadores*, Trabalho Final de Mestrado em Gestão e Políticas Públicas, Lisboa: Universidade de Lisboa;

Bibliografia digital

- https://www.27001.pt/iso27001_4.html - ISO 27001 - Sistema de Gestão de Segurança da Informação, consultado em 14/09/2019;

- https://www.cnpd.pt/- *"A CNPD - Perguntas Frequentes – Direitos dos Titulares – Revista Forum – Decisões – Diretrizes da CNPD",*consultado em 10/08/2019;

- https://eugdpr.org/- *"GDPR Faqs – Privacy Policy",* consultado em 07/01/2019;

- https://www.integrity.pt/pt/iso27001.html - ISO 27001 - *Integrity* – consultado em 14/09/2019;

- https://www.itgovernance.co.uk/iso-27701- ISO 27701 -The international standard for privacy information management, consultado em 14/09/2019;

- https://eur-lex.europa.eu- *"Acessoao Direito da União Europeia – Regulamento(EU) 2016/679 (RGPD)",*consultadoem 07/01/2019

- https://gdpr-info.eu -"*General Data Protection Regulation* – Quick Access (Intersoft Consulting)",consultado em 07/01/2019

- https://www.insidehighered.com*"Privacy"* consultado em 07/01/2019;

- http://www.openlimits.pt/pt/thinking-ahead-blog/glossario-rgpd-regulamento-europeu-protecao-dados/?all=1 – Openlimits – "RGPD – Glossário: Todos os termos que precisa de conhecer", consultado em 14/09/2019;

- https://www.portaldodpo.pt/*"RGPD – Portaldo DPO – Encarregadode Proteção de Dados – Categorias de Dados – Dados Pessoais – Glossário – Penalizações – Conformidade"*(2019) Tiago Nascimento, consultadoem 16/06/2019;

- http://www.sg.pcm.gov.pt/media/33592/04.pdf - "Secretaria-Geral da Presidência do Conselho de Ministros", Regulamento Geral de Proteção de Dados Pessoais, consultado em 12/09/2019;

- https://www2.le.ac.uk/legal/privacy*"Privacy"* University of Leicester, consultadoem 10/08/2019;

- http://blog.fullfabric.com/implementing-the-gdpr-at-your-university-a-talk-by-lothar-fritsch*"Implementing the GDPR at your university - a Talk by Lothar Fritsch"* consultadoem 10/08/2019;

- https://www.northwestern.edu/ - *"University Compliance – GDPR - Northwestern's Compliance Program",*consultadoem 10/08/2019;

- https://www.researchgate.net/publication/317777738_Implementing_GDPR_-_The_impact_of_GDPR_in_Higher_Education *"Implementing GDPR - The impact of GDPR in Higher Education"* (2017) Dr. Lothar Fritsch, consultadoem 11/08/2019;

- https://www.stir.ac.uk/about/faculties-and-services/policy-and-planning/legal-compliance/data-protectiongdpr/ - "Privacy Notices", University of Stirling, consultadoem 11/08/2019;

- https://www.insidehighered.com/news/2018/03/13/colleges-are-still-trying-grasp-meaning-europes-new-digital-privacy-law - "European Rules (and Big Fines) for American Colleges", Inside Higher Ed, consultadoem 10/08/2019;

- https://www.ox.ac.uk/students/life/it/studentrecord/data?wssl=1 – "Oxford Students – Oxford Life – IT Services – Personal Data",Universityof Oxford, consultadoem 11/08/2019;

- https://comum.rcaap.pt/bitstreau/10400.26/1218/1/NeD117_AnaVaz.pdf - 2007, "Segurança da Informação, Protecção da Privacidade e dos Dados Pessoais", Ana Vaz, consultado em 11/09/2019;

- https://solvimm.com/blog/como-avaliar-um-risco-de-seguranca-da-informacao/ - "Como avaliar um risco de segurança da informação", Solvimm, consultado em 12/09/2019;

Legislação e Jurisprudência

- Carta dos Direitos Fundamentais da União Europeia;
- Código do Procedimento Administrativo;
- Constituição da República Portuguesa;
- Convenção Europeia dos Direitos do Homem;
- Regulamento (EU) 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;
- Retificação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 23 de maio de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;
- RJIES - Lei nº 62/2007 de 10 de setembro;

Esta página foi intencionalmente deixada em branco

Anexos

Esta página foi intencionalmente deixada em branco

Glossário de termos do RGPD

Neste glossário pode ver-se abaixo as definições dos termos mais importantes do RGPD, termos esses que foram transcritos diretamente do RGPD:

1. **Autoridade de controlo –** uma autoridade pública independente criada por um Estado-Membro (nos termos do art. 51.º) a quem cabe a responsabilidade pela fiscalização da aplicação do presente regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União;

2. **Consentimento** – uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

3. **Dados pessoais** – informação relativa 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;

4. **Dados biométricos –** dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;

5. **Dados genéticos –** os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa;

6. **Dados relativos à saúde –** dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de súde, que revelem informações sobre o seu estado de saúde;

7. **Definição de Perfis –** qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento localização ou deslocações;

8. **Destinatário –** uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou dos Estados-Membros não são consideradas destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento;

9. **Direito de acesso à informação pelo titular dos dados –** o titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações: as finalidades dos tratamento dos dados; as categorias dos dados

pessoais em questão; os destinatários; o prazo previsto de conservação dos dados pessoais;

10. **Direito à limitação do tratamento –** o titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, quando não houver exatidão, quando o tratamento for ilícito, quando o responsável pelo tratamento já não precisar dos dados pessoais ou caso o titular se tenha oposto ao tratamento, por motivos legítimos;

11. **Direito ao apagamento dos dados («direito a ser esquecido») –** o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando os dados deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento, ou o titular retira o consentimento, ou os dados foram tratados ilicitamente, ou ainda o titular dos dados se opõe porque não existem interesses legítimos;

12. **Direito de retificação –** o titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.

13. **Direito de oposição –** o titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, e incluindo a definição de perfis;

14. **Direito de portabilidade dos dados –** o titular dos dados tem 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;

15. **Encarregado de Proteção de Dados / *Data Protection Officer* (EPD / DPO) –** é uma pessoa designada pelo responsável pelo tratamento ou pelo subcontratante que se envolve, de forma adequada e em tempo útil, em todas as questões relacionada com a proteção de dados pessoais;

16. **Ficheiro –** qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;

17. **Limitação do tratamento –** a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro;

18. **Minimização dos dados –** significa que os dados pessoais recolhidos devem ser limitados ao que é necessário e relativamente às finalidades para as quais são tratados;

19. **Pseudonimização –** o tratamento de dados pessoais de forma que deixem de poder ser atribuído 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;

20. **Privacidade por defeito –** o responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais

recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

21. **Privacidade desde a conceção –** tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento 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, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados;

22. **Representante –** uma pessoa singular ou coletiva estabelecida na União que, designada por escrito pelo responsável pelo tratamento ou subcontratante, representa o responsável pelo tratamento ou o subcontratante no que se refere às suas obrigações respetivas;

23. **Responsabilidade do responsável pelo tratamento –** tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o RGPD;

24. **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;

25. **Sigilo (obrigações) –** Os Estados-Membros podem adotar normas específicas para estabelecer os poderes das autoridades de controlo previstos no art. 58º, relativamente a responsáveis pelo tratamento ou a subcontratantes sujeitos, nos termos do direito da União ou do Estado-Membro ou de normas instituídas pelos organismos nacionais competentes, a uma obrigação de sigilo profissional ou a outras obrigações de sigilo equivalentes, caso tal seja necessário e proporcionado para conciliar o direito à proteção de dados pessoais com a obrigação de sigilo. Essas normas são aplicáveis apenas no que diz respeito aos dados pessoais que o responsável pelo seu tratamento ou o subcontratante tenha recebido, ou que tenha recolhido no âmbito de uma atividade abrangida por essa obrigação de sigilo ou em resultado da mesma.

26. **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;

27. **Terceiro –** a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais;

28. **Transferências –** qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente RGPD forem respeitadas pelo responsável pelo tratamento e pelo

subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional;

29. **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;

30. **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;