Universidade do Minho
Escola de Direito

Sara Adriana Rodrigues Duarte

APLICAÇÃO DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS (RGPD): CASO DE ESTUDO DE UMA IPSS

Outubro de 2018

UMinho | 2018 Sara Duarte **APLICAÇÃO DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS (RGPD): CASO DE ESTUDO DE UMA IPSS**

Universidade do Minho
Escola de Direito

Sara Adriana Rodrigues Duarte

APLICAÇÃO DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS (RGPD): CASO DE ESTUDO DE UMA IPSS

Dissertação de Mestrado
Mestrado em Direito e Informática

Trabalho efetuado sob a orientação do
Professor Doutor Pedro Miguel Freitas

e do
Professor Doutor Henrique Dinis Santos

Outubro de 2018

Declaração

Nome: Sara Adriana Rodrigues Duarte

Número de Cartão de Cidadão: 14166398 7ZY4

E**ndereço Eletrónico**: saraduarte02@gmail.com

Título da Dissertação de Mestrado: APLICAÇÃO DO REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS (RGPD): CASO DE ESTUDO DE UMA IPSS

Orientadores: Professor Doutor Pedro Miguel Freitas e Professor Doutor Henrique Dinis Santos

Ano de Conclusão: 2018

Designação do Mestrado: Mestrado em Direito e Informática

Universidade do Minho, 31 outubro 2018

Assinatura: _____

(Sara Duarte)

Agradecimentos

Ao Professor Doutor Henrique Santos e ao Professor Doutor Pedro Miguel Freitas, orientadores desta dissertação, quero agradecer a dedicação, disponibilidade e apoio ao longo desta dissertação. Agradeço ainda a partilha dos seus conhecimentos que me fizeram crescer enquanto aluna e como pessoa, tal como a confiança transmitida para que fosse possível ultrapassar os obstáculos que surgiram ao longo deste percurso.

Um agradecimento especial à minha família e amigos por todo o apoio transmitido e pelo entusiasmo que demonstraram durante a realização da presente dissertação.

Aos participantes da IPSS, pela disponibilidade que me demonstraram e pela simpatia e força que me transmitiram durante toda a partilha das suas experiências. Ao Fernando Pires de Carvalho que me auxiliou nas questões de segurança da implementação do Regulamento. Foram todas/os essenciais para a concretização desta dissertação.

“In a time of deceit telling the truth is a revolutionary act.”

George Orwell

Resumo

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados) relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE é um documento jurídico que abrange todas as empresas e organizações. O Regulamento tem como objetivos uniformizar a legislação e as práticas em matéria de proteção de dados na União Europeia, proteger os direitos dos cidadãos e aumentar a transparência no tratamento dos seus dados.

A presente dissertação propõe-se a estudar e implementar o Regulamento Geral sobre a Proteção de Dados numa Instituição Particular de Solidariedade Social, mais precisamente numa creche.

Abstract

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC is a legal document that applies to all businesses and organizations. The purpose of the Regulation is to standardize legislation and data protection practices in the European Union, protect citizens' rights and increase transparency in the processing of their data.

The present dissertation proposes to study and implement the General Data Protection Regulation in a Private Institution of Social Solidarity, particularly in a kindergarten.

Índice

Índice de Figuras

Abreviaturas

AIPD – Avaliação de Impacto sobre a Proteção de Dados

CNPD – Comissão Nacional de Proteção de Dados

CRP – Constituição da República Portuguesa

EEE – Espaço Económico Europeu

EPD – Encarregado para a Proteção de Dados

IPSS – Instituição Particular de Solidariedade Social

RGPD – Regulamento Geral sobre a Proteção de Dados

UE – União Europeia

Introdução

Atualmente, a informação dos cidadãos está maioritariamente armazenada em massa, ou seja, em grandes bases de dados que contêm informações sobre várias categorias dos indivíduos. [1]

A questão em torno das bases de dados é descrita por jornalistas, juristas e políticos como uma metáfora do livro "*Big Brother"* de George Orwell. Na narrativa de Orwell o Governo conhece tudo sobre os seus cidadãos e de forma persistente vigia e regula todos os aspetos das suas vidas, baseando-se sobretudo na monitorização constante e na espionagem. A metáfora do *Big Brother* é uma constante no discurso de quem estuda as questões relacionadas com a informação e a privacidade. Para muitos desses estudiosos, as bases de dados têm os mesmos propósitos do que é ilustrado no livro de George Orwell, nomeadamente, o controlo social e a supressão da individualidade, uma vez que se socorrem das mesmas técnicas, respetivamente, a vigilância e monitorização. [2]

Aliás, o que acontece atualmente na sociedade moderna foi largamente previsto por grandes autores literários, para além de George Orwell, Franz Kafka no livro "O Processo" descreve os graves problemas de uma sociedade burocrática. A metáfora de Kafka baseia-se na forma como o processo burocrático trata os seus indivíduos e as suas informações. O seu argumento pauta-se pela ideia de que a burocracia é benéfica para a sociedade e os processos e procedimentos não podem acontecer de forma aleatória mas, por vezes, também apresentam fortes problemas. [3]

Os órgãos estatais como agentes de controlo, mas também de garante de segurança, não têm preparado os seus funcionários de forma apropriada para as questões ligadas à segurança dos dados pessoais dos cidadãos. Neste seguimento, um dos problemas das bases de dados é o facto de estas retirarem poder aos cidadãos sobre os seus próprios dados, ficando desta forma vulneráveis e sem controlo das suas informações pessoais. [4]

---

[1] Katherine J. STRANDBURG, Daniela Stand RAICU(EDS.), *Privacy and technologies of identity: a cross-disciplinary conversation,* Springer, 2006, p. 4. Acesso disponível através da Springer Link. Disponível em http://link.springer.com/book/10.1007/0-387-28222-X

[2] *Idem,* P.9-10.

[3] *Ibidem.*

[4] Katherine J. STRANDBURG, Daniela Stand RAICU(EDS.), *Privacy and technologies of identity: a cross-disciplinary conversation, cit.,* p. 4.

A proteção de dados e a privacidade sempre foram questões debatidas e de preocupação generalizada nas sociedades, no entanto, com o crescimento da tecnologia e da economia dos dados essa preocupação tem vindo a aumentar. Neste contexto de exponencial desenvolvimento tecnológico surgiu o Regulamento Geral sobre a Proteção dos Dados do Parlamento Europeu que veio permitir a proteção dos cidadãos europeus contra abusos na utilização dos seus dados pessoais.

O Regulamento Geral sobre a Proteção de Dados é um documento jurídico, mas tem algumas especificidades técnicas tendo em consideração o seu escopo. A presente dissertação propõe-se a aplicar este novo instrumento jurídico numa das instituições abrangidas pelo mesmo. Em particular, o Regulamento Geral sobre a Proteção de Dados será implementado numa IPSS (Instituição Particular de Solidariedade Social)) portuguesa. Dito isto, o primeiro capítulo irá versar-se sobre a evolução do conceito de privacidade, bem como da legislação sobre este tema, quer nacional quer da União Europeia. Seguindo-se o segundo capítulo com uma breve abordagem às questões da segurança da informação. Por fim, o terceiro capítulo será a descrição dos passos e do processo de aplicação do Regulamento na IPSS, como supramencionado.

Capítulo I – Privacidade e Proteção de Dados

1. Enquadramento histórico

A privacidade antes do surgimento das novas tecnologias tinha o seu conceito um pouco melhor definido, uma vez que a possibilidade de existir uma derrogação da mesma era menor. Contudo, com o aparecimento e o desfreado desenvolvimento das mesmas o seu âmbito de delimitação e de controlo ficou um pouco mais difícil.

O conceito de privacidade não se constitui unânime, uma vez que é uma noção que ainda não encontrou uma ordem. A sua definição ainda não foi estabilizada. Constitui-se como um conceito peculiar. Existem imensas teorias acerca do mesmo e verifica-se uma tendência a que se incluam ou agrupem outras palavras e significados em volta do mesmo. [5]

Assim, nos pontos seguintes (1.1. a 1.5) explanar-se-á as várias conceções do conceito de privacidade e a sua evolução.

"Right to privacy"

Nos ordenamentos jurídicos anglo-americanos a expressão "*right to privacy*", isto é, direito à privacidade foi inserido em 1980, pelos autores como Samuel Warren e Louis Brandeis. Este direito também foi reclamado em outros ordenamentos jurídicos, nomeadamente no francês, no texto "*Loi relative à la presse"*, isto é, a Lei Relativa à Imprensa, em maio de 1868, onde proibia a publicação dos factos relativos à vida privada dos indivíduos, a não ser que esses factos já sejam públicos, ou então, com o consentimento dos mesmos. Warren e Brandeis defenderam que este direito devia ser igualado ao "*the right to be let alone*", ou seja, o direito a ser deixado sozinho. [6]

O direito à privacidade, nos tribunais norte americanos, é entendido como uma defesa contra qualquer intrusão física "irrazoável" ("*unreasonable"*) em casa, nos papéis e pertences privados e pessoais da pessoa, em consonância com a Quarta Emenda da Constituição Norte-

[5] Glória González FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014, p. 21.
[6] *Idem,* p. 27.

Americana.[7] Contudo, na sociedade moderna, as intrusões da privacidade não se esgotam nos anteriormente numerados, devido sobretudo, à imensidão de tecnológica que rodeia a sociedade. Em 1890, Warren e Brandeis levantaram questões acerca da privacidade, tendo que ver, sobretudo, com o aumento nos jornais e das fotografias, sendo possível através das tecnologias de impressão e as primeiras câmaras e caracterizando a privacidade como direito a estar sozinho, acrescentando a tudo isto, o incrível desenvolvimento, a nível das telecomunicações. [8]

Outra escola americana, em 1960, de William L. Prosser publicou um artigo que revia todo o conhecimento do direito à privacidade desde a publicação de Warren e Brandeis, onde descrevia a existência de quatro tipos de danos à privacidade, designadamente, a intrusão na solidão ou reclusão de uma pessoa; a apropriação para fins comerciais do nome ou imagem da pessoa; a divulgação pública de factos embaraçosos da vida privada de um indivíduo; ou a publicidade que coloca a pessoa no domínio público. [9]

A proteção da privacidade no ordenamento jurídico norte-americano não aconteceu apenas no domínio da lei ordinária, mas também na lei constitucional. Embora, a Constituição Americana não faça uma referência direta à privacidade, existem variadíssimos aspetos onde a privacidade é considerada como um bem a proteger pelos tribunais. [10]

Brandeis tornou-se juiz da Suprema Corte dos Estados Unidos, de onde argumentou que os redatores da Constituição dos Estados Unidos já reconheciam o direito de ser deixado sozinho e que esse direito era o mais amplo e mais estimado de todos.[11]

O Supremo Tribunal dos Estados Unidos, em 1965, declarou que os indivíduos tinham o direito constitucional à privacidade que se encontra em zonas de liberdade, a partir de uma interpretação expansiva do *Bill of Rights.* Desta feita, a privacidade pode ser considerada como um direito de ser livre da inferência governamental, o que conduziu à fomentação da ideia de que existem liberdades além das que se encontram sob o controlo do

---

7 *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*.

8 Demetrius KLITOU, *Privacy-Invading Technologies and Privacy by Design – Safeguarding Privacy, Liberty and Security in the 21st Century,* Springer, 2014, p. 15-16.

9 Glória González FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, *cit.,* p. 27-28.

10 *Idem.*

11 *Ibidem*.

domínio estatal e até das democracias. Assim, o direito à privacidade abarca tanto uma proteção negativa e o escudo de proteção e ainda o direito à autonomia e à autodeterminação.[12]

Neste seguimento, em 1960, o termo privacidade adquiriu nos Estados Unidos dois significados mais relevantes, numa primeira perspetiva, foi utilizado pela lei civil como referência sintética dos sistemas judiciais, exemplificando, a intrusão em assuntos privados da pessoa ou a divulgação de factos privados ou o uso da imagem de uma pessoa, por outro lado, no âmbito constitucional como uma referência dos direitos dos indivíduos que recusam interferências do poder estatal. [13]

Privacidade e os computadores

Em 1965, nos Estados Unidos surgiram as questões e ligações entre a privacidade e os computadores. As primeiras máquinas de processamento eletrónico de dados surgiram no mercado uma década depois e, até 1960, não existia nenhuma menção à ligação entre a privacidade e os computadores. Contudo, o avanço das tecnologias já se configurava bastante acelerado, mas em 1950 já se verificavam testemunhos de pessoas que se mostravam resistentes ao processamento de dados relacionados com os cidadãos. Por exemplo, religiosos e organizações que defendiam as liberdades civis protestaram contra a introdução de uma pergunta acerca da preferência religiosa dos cidadãos nos censos, argumentando que a introdução de tal questão constituía uma violação da liberdade religiosa e da separação entre o Estado e a Igreja, o que constituía uma invasão da privacidade e da consciência dos cidadãos. As discussões acerca do desenvolvimento de um sistema de identificação pessoal universal também causaram um alvoroço na generalidade das populações. Contudo, apenas em 1960, quando os computadores começaram a ter uma grande importância social, e sobretudo, quando se compreendeu que os computadores podiam constituir uma ameaça no que respeitava à autonomização de informação acerca dos indivíduos e que os computadores eram capazes de a sustentar e banalizar.[14]

---

[12] Glória González FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, *cit.,* p. 28-29.
[13] *Idem.*
[14] *Ibidem*.

Os primeiros a alertar para os perigos dos computadores à privacidade foram os especialistas em computadores que alertavam para a grande capacidade e pouco dispendiosa capacidade de os computadores processarem informação, unindo-se a esta conjuntura à disponibilidade dos dados das agências governamentais e das organizações privadas. [15]

No início dos anos de 1960, o debate sobre a privacidade aumentou substancialmente, devido ao impacto do aparecimento de tecnologias como as escutas telefónicas, testes psicológicos e o uso de polígrafos para detetar mentiras. [16]

Em 1962, o *Special Commitee on Science and Law of the Association of the Bar* de Nova Iorque, preocupado com o impacto dos novos dispositivos na privacidade, propôs uma investigação sobre o tema, denotando que existiram enormes avanços eletrónicos, óticos, acústicos, entre outros serviços que comprometiam privacidade individual dos cidadãos. [17]

Os resultados desta investigação foram publicados em 1967, através de um livro com o título de *Privacy and Freedom* de Alan F. Westin, onde se constatava que os computadores colocam graves problemas à privacidade, no entanto, o escritor assume que o pensamento necessário para abordar esta questão ainda não tinha sido alcançado. Contudo, os seus estudos demostraram-se relevantes para definir o termo privacidade. A sua definição foi construída para ser aplicada à privacidade em geral, mas esta foi concebida através dos princípios da computorização, nas palavras de WESTIN, "*privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and what extent information about them is communicated to others",* isto é, a privacidade refere-se à reivindicação dos indivíduos, grupos ou instituições que determinam por si mesmos quando, como e em que medida a informação sobre eles é comunicada a outro. Sendo o autor pioneiro na ideia do controlo da privacidade. [18]

A definição de privacidade fornecida por WESTIN veio introduzir uma nova ideia, nomeadamente a ideia que se devem estabelecer limites de proteção de privacidade na lei norte-americana. Na perspetiva deste autor, a privacidade tem raízes ancestrais e constitui uma necessidade funcional nos estados democráticos. Os esforços para impor limites à

[15] Glória González FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, *cit.,* p. 30.
[16] *Idem.*
[17] *Ibidem.*
[18] *Idem,* p. 31.

vigilância em nome da privacidade retratam a luta das sociedades ocidentais pela liberdade. [19]

Outro livro, com bastante relevância nesta temática foi publicado em 1971, de Arthur R. Miller's, com o nome de *The Assault on Privacy,* onde reforçou a ligação entre a privacidade e os computadores revendo diferentes ameaças de intrusão computorizada. Segundo, WESTIN que apresentou o direito à privacidade como a capacidade que os indivíduos têm para controlar a informação que tem que ver com ele mesmo, o problema dos computadores tem que ver com o facto da informação ser armazenada, e o indivíduo (a quem essa informação diz respeito) perde o controle da mesma. [20]

Privado como oposto ao que é público

Partindo do pressuposto que o termo público se refere àquilo que se concede ao conhecimento do Estado ou da sociedade em geral, e por outro lado, privado relaciona-se com aquilo que não diz respeito ao domínio público, não pertence à *res publica*, ou seja, não é uma coisa pública, como por exemplo, aquilo que tem que ver com a vida familiar. Ainda dentro deste entendimento, perceciona-se como público aquilo que é partilhado, comum, aquilo que é exposto, e privado aquilo que pertence a um espaço ou domínio fechado, não exposto, resguardado, escondido, confidencial, secreto, aquilo que está relacionado com a introspeção de cada um, o que é inacessível e fora do alcance. Assim, a privacidade pode ser entendida com a proteção daquilo que está previsto como privado em oposto daquilo que é público.[21]

Depreende-se que o significado de privacidade e privado é muitas vezes associado e construído em oposto aquilo que é público, mas nem sempre é assim. Na noção legal de privacidade em muitos sistemas jurídicos tem sido muitas vezes associada com aquilo que é "privado" no sentido de individual, pessoal e próprio. [22]

---

[19] Glória González FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, *cit.,* p. 32.
[20] *Ibidem.*
[21] *Idem,* P. 22
[22] *Ibidem*.

Privacidade, liberdade e segurança

Na tentativa de definição de privacidade temos de ter em consideração três conceitos, a privacidade, liberdade e a segurança uma vez que são conceitos que se inter-relacionam entre si. [23] A definição deve abarcar todas as vertentes da privacidade, nomeadamente o que constitui uma violação da privacidade e quais os méritos da proteção de dados. O que podemos desde já concluir é que o produto da construção do conceito é a sua inerente flexibilidade e a significativas divergências de opinião entre juristas e entre as suas diferentes gerações. Exemplificando, a Geração X [24] pode ter em geral uma opinião acerca da privacidade e da sua importância e valor do que a Geração Y [25]. Além disso, temos de ter em consideração vários fatores, designadamente as mudanças sociais quer sejam de normas e de valores, as opiniões públicas, as tendências ideológicas, as tecnologias e infraestruturas disponíveis, as circunstâncias políticas e outras situações que se verificam atualmente (como o caso, a taxa da criminalidade elevada ou as consequências dos ataques terroristas). O conceito de privacidade e a sua crença no seu valor e importância varia de pessoa para pessoa, consoante a sua personalidade, as suas vivências, os seus interesses e ainda, tendo em conta a sua posição e a sua função na sociedade.

A privacidade não pode estar dissociada do termo liberdade, devido ao facto de ser entendida como uma fortaleza da liberdade pessoal, como uma garantia de uma liberdade para estabelecer os caminhos da vida e uma forma importante para resistir às interferências da liberdade, é uma liberdade individual e uma própria proteção da própria liberdade. O termo privacidade está ainda conectado com o termo de individualidade, como resultado da construção da pessoa, teve a sua origem no Cristianismo primitivo sendo desenvolvido na Idade Média e consolidada no Iluminismo como princípio do constitucionalismo moderno. Privacidade que não seria entendida apenas sobre os limites que separam o que pertence ao Estado e aquilo que diz respeito à vida de cada indivíduo, mas uma barreira que protege os

[23] Demetrius KLITOU, *Privacy-Invading Technologies and Privacy by Design – Safeguarding Privacy, Liberty and Security in the 21st Century,* cit., p.14.
[24] Designação conferida às pessoas nascidas durante os anos de 1960 e 1970. Atribui-se a esta geração uma maior e melhor compreensão da tecnologia uma vez que se apresenta como a primeira geração que domina os computadores, sendo reflexo da Era da Informação.
[25] Designação atribuída às pessoas nascidas durante os anos de 1980 e 1990 também conhecida por *Echo Boomers* e *Millennials.* Apresenta-se como uma geração que conviveu fortemente com a tecnologia e com os seus avanços (computadores, telemóveis).

cidadãos contra as arbitrariedades do poder estatal. Assim, a privacidade também se encontra associada à autonomia.[26]

Entendida como uma realização dos próprios indivíduos, foi ainda unida à noção de dignidade humana, nesta perspetiva, depreende-se que a privacidade se constitui como inerente à condição humana para que os indivíduos se possam desenvolver livremente, e à condição humana deve-se pressupor o reconhecimento de um grau de autodeterminação. Assim, a individualidade é associada ao completo desenvolvimento da personalidade, conceito esse associado ao ser humano. A privacidade afigura-se necessária ao completo desenvolvimento do ser humano e da pessoa e está frequentemente associada ao conceito de identidade, que se configura como uma noção multifacetada, com uma série de conceitos relevantes, nomeadamente a personalidade ou a individualidade, mas também pode permitir a identificação ou a individualização ou ainda, a possibilidade de se constituir numa soma de indentificadores pessoais. Por sua vez, a identidade é indicada como a solução para a relação entre a privacidade e a liberdade. [27]

O direito à privacidade quando comparamos constituições apresenta-se como tardio. Sendo precedida de outras noções, tais como a inviolabilidade do domicílio, a confidencialidade, noções mais tarde enquadradas no direito geral à privacidade. [28]

Estas diferentes conceções de privacidade levaram a uma sobreposição do conceito. Pode-se argumentar, por exemplo, que para os indivíduos serem efetivamente capazes de viver livremente, precisam de assegurar que alguns factos das suas vidas devem permanecer em segredo. Deste ponto de vista, a inviolabilidade do domicílio e a confidencialidade das comunicações surgiram associadas à liberdade pessoal. O respeito pela privacidade assim como da sua própria vida no sentido de permitir uma reflexão pessoal e um desenvolvimento das suas próprias atitudes, para serem livres, os indivíduos necessitam que certas facetas da sua vida se mantenham privadas. [29]

De forma distinta, pode suceder que as ramificações descritas do conceito de privacidade podem ocasionalmente entrar em conflito. Existem conceções de privacidade

---

[26] Glória González FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, *cit.,* p. 23.
[27] Glória González FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, *cit.,* p. 23.
[28] *Idem,* 23-24
[29] *Ibidem.*

que advertem contra a demasiada ênfase aos entendimentos que aquilo que é privado é oposto aquilo que é público, uma vez que alguns estudos têm prosseguido a ideia de que para que os cidadãos sejam efetivamente livres não podem dissociar aquilo que é social e público. Para desfrutar da vida privada no sentido da vida de cada um, os indivíduos necessitam mais do que uma vida privada, devem incluir a dimensão do indivíduo que deve ser exteriorizada. Para ser livres, os indivíduos não as devem separar. [30] [31]

A privacidade e a liberdade estão relacionadas devem ser protegidas e integradas. A OECD (*Organisation for Economic Co-operation and Development* ou Organização para a Cooperação e Desenvolvimento Económico) aponta que a proteção da privacidade e das liberdades individuais constitui uma sobreposição legal dos aspetos que envolvem a proteção de dados. Para Gavison, em 1980 a privacidade auxilia a liberdade sendo benéfica para uma sociedade democrática livre. Neste sentido, o Supremo Tribunal do Canadá proferiu numa decisão em afere que "a privacidade é o coração da liberdade num Estado moderno". [32]

Associada à privacidade estará sempre o conceito de segurança, uma vez que para que um sistema seja seguro e, para que os nossos dados que constam no sistema estejam protegidos, é necessário que este seja seguro ou, pelo menos, o mais seguro possível. [33]

A segurança é também um direito humano fundamental, como se encontra plasmado no artigo 6.º da Carta Europeia dos Direitos Fundamentais da União Europeia. [34]

A segurança pública tem que ver com a proteção das cidades que normalmente se encontra ao cargo dos diferentes órgãos do poder estatal. A segurança inclui a proteção dos cidadãos contra os vários ataques que as sociedades estão sujeitas e para o combater, as autoridades estatais socorrem-se de vários métodos, tradicionalmente, as sociedades socorrem-se da adoção de normas criminais, ficando ao encargo das instituições de fazer cumprir a lei e punir quem não a cumpre. Recentemente, esses métodos têm auxílio da tecnologia, quer sejam tecnologias de vigilância públicas, tecnologia de imagem avançada,

[30] Glória González FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, *cit.,* p. 23-24.
[31] Demetrius KLITOU, *Privacy-Invading Technologies and Privacy by Design – Safeguarding Privacy, Liberty and Security in the 21st Century,* p.19
[32] *Idem*, P. 14-19.
[33] *Idem,* P.21
[34] *Ibidem.*

tecnologia forense e infraestruturas e tecnologias de ICT (Tecnologias de Informação e Comunicação). [35]

Dentro da segurança pública tem de ser realizada uma avaliação da mesma que tem que ver com a segurança em aeroportos e em aviões, incluindo as pessoas que se encontram a bordo. A avaliação foca-se inicialmente na prevenção para que nenhuma arma ou conteúdo explosivo estejam a bordo e para tal, socorre-se a vários meios, tais como, a triagem de passageiros e das bagagens, a segurança dos documentos de identificação, medidas impeditivas de entradas indesejadas no aeroporto (por exemplo, câmaras de CCTV, sistemas de deteção de intrusão ou detetores de movimento e barreiras "inteligentes". [36]

Ainda, a segurança das infraestruturas críticas é muito importante no que respeita à segurança nacional. A segurança nacional inclui proteção as centrais nucleares, distribuição de eletricidade, reservatórios de água, barragens, rios, aeroportos, portos, estradas de ferro, contra-ataques terroristas e ciberataques. Os métodos utilizados para proteger esses ataques têm que ver com a implementação de forças policiais, a utilização de tecnologia de controle de acesso físico, entre outros. [37]

Por vezes, a privacidade pode entrar em conflito com a segurança e das liberdades individuais, por exemplo, os terroristas podem beneficiar das vulnerabilidades de revista, uma vez que podem usufruir dos requisitos legais da privacidade corporal e do princípio da privacidade. O anonimato online e a incorporação de tecnologias criptográficas (o tipo de tecnologia que protegem a privacidade) podem melhorar a comunicação não detetadas entre terroristas escondida através da proteção de dados. [38]

Teoria das esferas

A mistura entre a noção de privacidade e a sua noção jurídica coincidente pode conduzir a algumas ambiguidades. Por exemplo, o termo esfera. Os estudiosos e políticos têm usado a imagem de esferas concêntricas para descrever os diferentes graus de individualismo relacionado com a política, têm representado a existência de uma esfera

[35] Demetrius KLITOU, *Privacy-Invading Technologies and Privacy by Design – Safeguarding Privacy, Liberty and Security in the 21st Century,* p. 22
[36] Demetrius KLITOU, *Privacy-Invading Technologies and Privacy by Design – Safeguarding Privacy, Liberty and Security in the 21st Century,* p. 22
[37] *Ibidem*
[38] *Idem,* P. 23

íntima, uma esfera privada, uma esfera social e uma esfera pública. Contudo, a imagem da esfera foi utilizada para transmitir a ideia de algo que não é primeiramente sobre a delimitação, demarcação ou ofuscamento e contribuindo para a subjetividade. [39]

Neste sentido, a Constituição Alemã foi influenciada por aquilo que designa de "*theory of the spheres",* isto é, a teoria das esferas, o Tribunal Constitucional Federal Alemão, em 1950, entendeu que os círculos concêntricos ou as esferas permitiam delimitar as diferentes áreas tendo em conta os graus distintos de privacidade, nomeadamente em *Individualsphäre* (Esfera Individual), em *Privatsphäre* (Privacidade) e *Intimsphäre* (Vida Privada ou Intimidade).

Contudo, este modelo foi abandonado pelo Tribunal Constitucional Federal Alemão em 1983, mas esta doutrina foi amplamente marcada não só na literatura alemã. [40]

A doutrina das esferas foi bastante desenvolvida na doutrina alemã o que permitiu desenvolver várias questões como o direito geral à personalidade, reconhecendo ainda o direito à inviolabilidade da dignidade humana e o direito ao desenvolvimento da personalidade. O direito geral à personalidade é descrito como imprescindível à liberdade abarcando o direito geral de livre ação e sendo comparado com o direito à privacidade. A noção do direito geral à privacidade gerou alguma desorientação, uma vez que não deve ser confundido com as noções de direito civil de personalidade ou com "direitos pessoais", muitas vezes retratado como uma espécie de direito humano reconhecido pela lei civil e onde a literatura o tem relacionado com as discussões em volta da privacidade. [41]

Violações de privacidade

O incremento e evolução tecnológica constante dificulta a definição do que constitui uma violação da privacidade, contudo, parece correto afirmar que, uma violação da privacidade constitui qualquer não autorizada intrusão da mente ou corpo da pessoa, a coleta e ou divulgação de qualquer dado pessoal sem consentimento ou conhecimento ou sem qualquer justificação, uma ilegal (desproporcional) vigilância e uma inferência desproporcionada no direito de ser deixado sozinho.

---

[39] Glória González FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, p. 24-26
[40] *Idem.*
[41] *Ibidem*

Definir o que constitui uma violação da privacidade, tendo em conta a exaustiva lista do que constituem dados pessoais, existindo assim, muitos tipos diferentes de violações de dados pessoais. SOLOVE desenvolveu a ideia de uma "taxonomia da privacidade", para tal classificou o alcance da violações da privacidade em quatro grupos, nomeadamente a recolha de informações, o processo das informações, divulgação da informação e invasão e, ainda, em dezasseis subgrupos, designadamente, vigilância, interrogação, agregação, identificação, insegurança, utilização secundária, exclusão, quebra do sigilo, divulgação, exposição, aumento da acessibilidade, chantagem, apropriação, distorção, intromissão e inferência na decisão. [42]

Privacidade e o Direito

A privacidade foi reconhecida como um direito em muito textos legislativos de grande importância a nível europeu e a nível internacional, designadamente, no artigo 12.º da Declaração Universal dos Direitos Humanos, no artigo 17.º do Pacto Internacional sobre os Direitos Civis e Políticos, no artigo 8.º da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais, no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, no artigo 11.º da Convenção Americana dos Direitos do Homem, no artigo 16.º da Convenção dos Direitos da Criança e no artigo 14.º da Convenção Internacional sobre a Proteção dos Direitos de Todos os Trabalhadores Migrantes e dos Membros das suas Famílias. [43]

Quando se compara todos estes instrumentos internacionais com a exceção do Carta Europeia dos Direitos do Homem, no seu artigo 8.º, frequentemente encontra-se o termo privacidade associado à reputação e à honra, o direito à privacidade é visto como um elemento essencial para a realização da dignidade pessoal, pelo respeito para consigo próprio e dos outros. [44]

[42] Demetrius KLITOU, *Privacy-Invading Technologies and Privacy by Design – Safeguarding Privacy, Liberty and Security in the 21st Century,* p. 17.
[43] *Idem.*
[44] *Idem,* p. 18 e 19.

Consagração constitucional

Em 1970, começaram a surgir nos vários ordenamentos jurídicos europeus diferentes textos jurídicos que regulamentavam o processamento automático de dados. E essa proteção foi efetuada basicamente de duas formas, nomeadamente através de normas *ad hoc* ou através de proteção ao nível constitucional. Ambas visavam uma proteção dos indivíduos face à nova realidade do processamento automatizado de dados. [45]

Vários países adotaram a proteção por via *ad hoc,* nomeadamente a Alemanha, a Suécia, a Franca. Portugal foi um dos vários países a par da Áustria e da Espanha que optaram pela proteção ao nível constitucional. [46]

Portugal foi o primeiro país a incorporar na sua Constituição disposições normativas relativas ao processamento automático de dados, sendo por isso, considerado pioneiro nesta matéria, uma vez que a Constituição Portuguesa de 1976, na perspetiva do direito comparado, empregou uma considerável proteção neste domínio devido à longitude e ao grau de detalhe com que o legislador descreve os direitos e liberdades fundamentais que estabelece. O artigo 35.º da CRP, onde no seu título dispõe, "Utilização Informática" garante a todos os cidadãos o direito à informação que está contida nas bases de dados à cerca dos mesmos, em segundo, proíbe um processamento automatizado de dados que contenha informação acerca das convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica dos cidadãos, exceto se os dados estejam configurados de forma a não permitir a identificação do indivíduo e, por fim, a proibição da utilização do número de identificação pessoal nacional para a interconexão ou para correlacionar dados. [47]

O artigo 35.º foi importantíssimo para que anos mais tarde alguns ordenamentos jurídicos empregarem um reconhecimento constitucional para o acesso a dados pessoais, sendo que inspirou outros países a estabelecer proteção neste domínio, por exemplo, no caso da Constituição Brasileira de 1988,que introduziu uma nova questão ao introduzir uma nova questão, o *habeas data*, que constitui o processo que garante aos cidadãos ou acesso a informações que constem nas bases de dados de instituições públicas ou governamentais

[45] Demetrius KLITOU, *Privacy-Invading Technologies and Privacy by Design – Safeguarding Privacy, Liberty and Security in the 21st Century,* p. 55.
[46] *Idem,* p. 56-69.
[47] *Idem,* p. 66-67.

sobre os próprios. No mesmo sentido a Constituição da República Angolana que possui no seu artigo 69.º com a epígrafe *Habeas Data*. [48] [49] [50]

A Constituição da República Portuguesa consagra os Direitos, Liberdades e Garantias nos seus artigos 24.º a 57.º. O artigo 26.º (Outros direitos pessoais) consegue reunir nove direitos diferenciados que têm em comum o facto de estarem ao serviço da proteção da esfera nuclear das pessoas e da sua vida contendo essencialmente os direitos de personalidade. Estes direitos de personalidade gozam de tutela penal e constituem um limite a outros direitos fundamentais. [51]

Neste contexto revela-se importante fazer uma distinção entre privacidade e reserva da vida privada e familiar sendo que a privacidade é um direito geral de personalidade que abrange a liberdade da vida privada. O direito à reserva da intimidade da vida privada e familiar que se encontra no artigo 26.º (nº1, *in fine,* e n.º 2) que se examina em dois direitos menores, primeiro o direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar e o segundo, o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem. Sendo que alguns direitos fundamentais operam como garantias deste, como é o caso do direito à inviolabilidade do domicílio e da correspondência, artigo 34.º da CRP e a proibição do tratamento informático de dados referentes à vida privada, artigo 35.º, nº3 da CRP. [52]

Salienta-se que a delimitação entre a esfera da vida privada e familiar e aquilo que se pode considerar mais aberto à publicidade afigura-se como uma tarefa árdua. Embora, uma parte da jurisprudência diferencia a *esfera pessoal íntima* considerando-se aquela que é absolutamente protegida e a *esfera privada simples* diz respeito aquela que se encontra relativamente protegida uma vez que quando se encontra em conflito com outro interesse ou bem público pode se abdicar ou conceder parte desta. O conceito de esfera da vida privada

---

[48] Demetrius KLITOU, *Privacy-Invading Technologies and Privacy by Design – Safeguarding Privacy, Liberty and Security in the 21st Century,* p. 66-67.

[49] Constituição da República de Angola.
Consultado a 01-07-2018 e disponível em: http://www.consuladogeralangola-porto.pt/download/pt/constituicao-da-republica-de-angola.pdf

[50] Constituição da República Federativa do Brasil.
Consultado em 01-07-2018 disponível em:
https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf

[51] J.J. Gomes CANOTILHO, Vital MOREIRA, *Constituição da República Portuguesa: anotada,* 4.ª Edição, Coimbra, Coimbra Editora, 2007, p. 461.

[52] *Idem,* p. 467-468.

da pessoa deve ter em conta os conceitos de «privacidade» artigo 26.º, nº1 e «dignidade da pessoa humana», artigo 26.º, nº2. O conceito normativo de reserva da intimidade da vida privada e familiar deve delimitar-se como conceito da vida privada que tem em conta três aspetos, o respeito pelos comportamentos, o respeito pelo anonimato e o respeito pela vida em relação, que devem ser solicitadas quando se abdica à proteção da vida privada. [53]

A teleologia dos direitos de personalidade fundamenta-se no «direito ao segredo do ser», ou seja, o direito à imagem, o direito à voz, o direito à intimidade da vida privada, o direito a praticar atividades da esfera íntima sem videovigilância. Contudo, demonstra-se problemática a inserção nestes direitos de personalidade o «direito ao segredo de ter», ou seja, a inserção do direito ao segredo bancário, o segredo dos recursos financeiros e patrimoniais, o segredo de aplicações de dinheiro e o segredo fiscal, sendo que não existe nenhum princípio ou regra constitucional que abarque o «segredo do ter». Ao consentir o «segredo do ter» como dimensão do direito de personalidade estas terão sempre maiores restrições do que o «segredo do ser». Outro conceito que aqui poderá ter relevância tem que ver com o conceito de segredo no sentido de valor pessoal estritamente ligado à privacidade, nomeadamente o segredo de profissão, o segredo médico o segredo testamentário que tem como principais destinatários todos aqueles em razão do seu estatuto, ofício, emprego, profissão ou arte têm o dever de não revelar segredos alheios, artigo 195.º do Código Penal. A conexão do segredo com deveres de sigilo profissional aponta também para a dimensão objetiva do segredo como bem jurídico supra-individual. [54]

O artigo 26.º, nº 2 estabelece uma imposição que vincula o legislador impondo que este estabeleça garantias contra a obtenção e utilização abusiva ou contrária à dignidade humana, de informações relativas às famílias, ou seja, refere-se a uma garantia efetiva do Estado à reserva da intimidade e da vida privada. O Estado não pode violar este direito assim como está obrigado a instituir mecanismos que impeçam a violação do mesmo quer por entidades publicas, quer por entidades privadas. [55]

As garantias podem ser sanções penais ou de caráter civil. Nos artigos 190.º e ss. do Código Penal tipificam e penalizam comportamentos que violam a intimidade (violação do domicílio, da correspondência, das conversas, artigos 190.º e 194.º), que «gravem»

[53] J.J. Gomes CANOTILHO, Vital MOREIRA, *Constituição da República Portuguesa: anotada, cit.*, p.468.
[54] *Idem,* p.468-469.
[55] *Idem,* p.471.

dimensões da vida privada (registros de imagens, de conversas, de informações nominativas de ficheiros informáticos) ou que tornem públicos aspetos da intimidade (revelação de segredos, transmissão e publicação de palavras ou imagens). [56]

No nº3 do artigo 26.º o legislador constitucional inicia esta disposição com uma imposição fazendo uma densificação normativa da *bioconstituição*, sendo muito importante neste domínio a identidade genética do ser humano. Aliás, em consonância com um conjunto de documentos importantes nesta matéria a nível internacional e comunitário, tais como, Diretiva 98/44/CE do Parlamento Europeu e do Conselho de 6 de julho de 1998 relativa à proteção jurídica das invenções biotecnológicas e a Declaração Universal sobre o Genoma Humano e os Direitos Humanos elaborada pelo Comité Internacional de Bioética da UNESCO. [57]

No que respeita ao artigo 35.º da Constituição, este consagra a proteção dos cidadãos perante o tratamento de dados pessoais informatizados. Contudo, não abrange apenas o tratamento, a individualização, a fixação e a recolha dos dados, mas também a sua conexão, transmissão, utilização e publicação. [58]

Na revisão constituição de 1997 este artigo sofreu alterações devido ao aparecimento das redes informáticas e da telemática. [59]

O desenvolvimento da tecnologia e o aumento da utilização de mecanismos eletrónicos que deixam as «pegadas eletrónicas» quer pela movimentação de contas bancárias, comércio eletrónico, portagens eletrónicas entre outros demonstra-se cada vez mais importante as garantias contra o tratamento e a utilização abusiva de dados pessoais informáticos. O mesmo acontece com outras tecnologias tais como, o «sistema de *chips*» ou de «cartão-*chip*» utilizados para identificação assim como o ADN que são lidos em equipamentos próprios.[60]

Os direitos fundamentais relacionados com o tratamento informático de dados pessoais extraem de alguns «direitos-mãe» em sede de direitos liberdades e garantias como o direito à dignidade da pessoa humana, do desenvolvimento da personalidade, da integridade

---

[56] J.J. Gomes CANOTILHO, Vital MOREIRA, *Constituição da República Portuguesa: anotada, cit.*, p. 471.
[57] *Idem,* p.472-473.
[58] *Idem,* p. 550.
[59] *Idem.*
[60] *Ibidem.*

pessoal e da autodeterminação informativa. A designação «dados pessoais» revela a conexão entre os direitos e o tratamento informático declarando que quanto mais os dados se relacionam com a dignidade, a personalidade e a autodeterminação das pessoas mais restrições se impõe quanto à sua utilização e recolha. Aqui, surgem dois problemas relativos ao processamento de dados informáticos, a determinação das categorias de dados e a graduação das ingerências necessárias à proteção de outros bens constitucionais.[61]

Em matéria de defesa contra o tratamento informático de dados pessoais a Constituição reconhece e garante um conjunto de direitos, nomeadamente o direito de acesso das pessoas aos registros informáticos para o conhecimento dos seus dados pessoais deles constantes, artigo 35.º, nº1, assim como a retificação e complementação dos mesmos, o direito ao sigilo em relação aos responsáveis de ficheiros automatizados e a terceiros dos dados pessoais informatizados e o direito à não interconexão, artigo 35.º, nº 4, o direito ao não tratamento informático de certos tipos de dados pessoais, artigo 35.º, nº3. A proibição do número nacional único, artigo 35.º.nº5 que funciona como garantia daqueles direitos dificultando o tratamento informático de dados pessoais e a sua interconexão que seria simplificada como um indentificador numérico comum. [62]

O direito ao conhecimento dos dados pessoais existentes em registos informáticos é uma espécie de direito básico na matéria de *habeas data* que se desdobra em vários direitos, tais como, o *direito de acesso* o direito a saber quais os dados que contam nos registros informáticos quer sejam públicos quer sejam privados, o *direito ao conhecimento da identidade dos responsáveis, bem como o direito ao esclarecimento* sobre a finalidade dos dados, o *direito de contestação,* isto é, o direito à retificação dos dados e sobre a identidade e o endereço do responsável, o *direito de atualização* nomeadamente a correção de conteúdos dos dados em cado de desatualização, e por fim, o *direito à eliminação* dos dados cujo o registro é interdito. O direito de acesso é universal, ou seja, vale para entidades privadas e públicas e não pode ficar dependente de condições que limitem o seu exercício, como por exemplo, o pagamento de uma taxa onerosa. [63]

Para que todos estes direitos estejam efetivamente funcionais afigura-se necessário que a informatização de dados pessoais obedeça a certos princípios que a doutrina tem

[61] J.J. Gomes CANOTILHO, Vital MOREIRA, *Constituição da República Portuguesa: anotada, cit.*, p.551.
[62] *Idem.*
[63] *Ibidem,* p.551-552.

salientado, designadamente a *publicidade,* ou seja, o conhecimento da criação e manutenção de registros informáticos, a *justificação social,* o que significa que a criação e manutenção de ficheiros, bases de dados e bancos de dados deve ter um objetivo geral e o usos específicos dos mesmos devem ser socialmente aceites, a *transparência,* isto é, deve existir clareza dos registros, quanto às espécies ou categorias de dados recolhidos e tratados, quanto à existência ou não de fluxos de informação, quanto ao tempo de tratamento e quanto à identificação do responsável do ficheiro, a *especificação das finalidades,* o que significa que as finalidades da recolha e do processamento devem ser especificados no momento da recolha, a *limitação da recolha* que deve ser elaborado por meios lícitos, o que significa que o conhecimento pessoa em causa ou autorização legal e ainda, a restrição aos dados necessários para as finalidades especificadas, onde se enquadram os princípios da necessidade, adequação e proporcionalidade, o *princípio da fidelidade,* ou seja, os dados devem ser exatos, completos e atuais, a *limitação da utilização* o que significa que os dados depois de recolhidos devem ser apenas utilizados para a prossecução dos fins especificados no momento da recolha, as *garantias de segurança* o que implica a adoção de medidas que protegem e garantem que os dados são protegidos contra a perda, destruição e acesso a terceiros, a *responsabilidade* diz respeito à imposição de especiais deveres legais e deontológicos para os responsáveis dos ficheiros, o *princípio da política de abertura,* ou seja, os ficheiros, bancos e bases de dados devem garantir a transparência da ação administrativa, designadamente quanto à clareza dos registros, as espécies e categorias de dados recolhidos e tratados, a existência ou não de fluxos de informação, ao tempo de tratamento e à identificação do responsável pelo ficheiro e o *princípio da limitação no tempo,* os dados devem ser cancelados quando obtida a finalidade a que se propunham. [64]

Assim, o direito ao conhecimento de dados pessoais é reconhecido «nos termos da lei» o que deixa desde logo abertura para excluir certos tipos de registros informáticos de dados pessoais, por motivo justificado, nomeadamente por razões de segurança ou de investigação criminal, entre os quais consta o segredo de Estado. [65]

Quanto ao tratamento automatizado, conexão e transmissão e utilização de dados pessoais a Constituição impõe ao legislador a definição de um regime jurídico de proteção

[64] J.J. Gomes CANOTILHO, Vital MOREIRA, *Constituição da República Portuguesa: anotada, cit.*, p. 552-553
[65] *Idem.*

aos particulares. Esta proteção estará a cargo dos órgãos públicos com competência geral para a defesa dos direitos, liberdades e garantias. Perante a insuficiência destes, na Revisão de 1997 faz-se expressa alusão à proteção através de uma autoridade administrativa independente, assim sendo tornou-se inquestionável a criação desta entidade. Desta forma, a lei institui a *Comissão Nacional de Proteção de Dados*, cuja atribuição existe para «controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, em rigoroso respeito pelos direitos da pessoa e pelas liberdades e garantias consagradas na Constituição e na lei», Lei 67/98, artigo 22.º, nº1. [66]

No nº 2 proíbe também a interconexão de ficheiros de bases e bancos de dados pessoais que remete para o artigo 193.º do Código Penal, aqui existe a pretensão de atenuar os três maiores perigos que a utilização informática representa para os direitos dos cidadãos, nomeadamente o *perigo da concentração* uma vez que o trabalho de conexão entre ficheiros informáticos (quer sejam um ficheiro fiscal, ficheiro da segurança social, ficheiro policial, entre outros) acabaria por conduzir à centralização e controlo completo dos cidadãos, o *perigo policial* uma vez que a partir da interconexão, os órgãos policiais acabariam por ter aceso a dados de novos processos secretos dos cidadãos, o *perigo da multiplicação de ficheiros* que ocorreria devido à acumulação de informações do indivíduo em um número incomparável de ficheiros. Salientando-se que estes perigos são maximizados pelos fluxos internacionais de dados. Contudo, a Constituição admite exceções a esta proibição, autorizando o legislador a definir os casos em que poderá haver acesso de terceiros e interconexões de dados (n.º 2 e 4 *in fine*). Aplica-se o regime das restrições aos direitos, liberdades e garantias do artigo 18.º da CRP que só terá lugar quando exigidos pela necessidade de defesa de direitos ou bens constitucionalmente protegidos, exemplificando, a defesa da existência de Estado, o combate à criminalidade, a proteção dos direitos fundamentais de outrem, entre outros. [67]

Quanto à forma adequada de proteção de dados pessoais no que respeita à utilização das redes informáticas de uso público, cabe ao legislador a sua determinação, artigo 35.º, nº 6. A proteção comporta diferentes níveis quando se referem a *dados sensíveis,* o seu tratamento pressupõe o consentimento de respetivo titular, relativamente aos *dados sujeitos*

[66] J.J. Gomes CANOTILHO, Vital MOREIRA, *Constituição da República Portuguesa: anotada, cit.*, p. 555.
[67] *Idem.*

a controlo prévio é obrigatório a autorização da CNPD, os *dados sujeitos a registo* em virtude da existência de uma obrigação de notificação e os *dados isentos de notificação.* Quanto aos dados sensíveis a Constituição estabelece uma *reserva de proibição* com possibilidade de autorização resumindo-se esta autorização ao *consentimento expresso do titular.* Nos dados sujeitos a autorização prevê-se uma *reserva de autorização* com possibilidade de proibição, explicitando que esta proibição deverá funcionar quando não existam garantias de não discriminação. A Constituição prevê também o caso dos *fluxos de dados transfronteiras* com a finalidade de proteger os dados pessoais e outros cujo interesse nacional justifique. [68]

Assim, o direito de privacidade refere-se a um direito universal assim como a larga maioria dos direitos, liberdades e garantias de natureza pessoal pelo que não há lugar para as reservar apenas para os cidadãos nacionais, mas também a estrangeiros, todas as pessoas, pelo facto de o serem gozam deste direito. [69]

2. Contexto Europeu

Tratado de Lisboa

As raízes legislativas da proteção de dados advêm em termos da União Europeia desde a Convenção do Conselho da Europa para a Proteção dos Indivíduos face ao tratamento automático de dados pessoais, a Convenção 108, de 28 de janeiro de 1981. [70]

O Tratado de Lisboa trouxe uma nova visão para a integração europeia, desde logo, os direitos fundamentais passaram a estar no centro. Em consonância com esta visão, a Carta dos Direitos Fundamentais da União Europeia, foi recebida com o mesmo valor formal que o Tratado da União Europeia e do Tratado do Funcionamento da União Europeia. Assim, com o artigo 8.º da Carta a proteção de dados pessoais enquanto direito à autodeterminação informacional foi constitucionalizada. [71]

---

[68] J.J. Gomes CANOTILHO, Vital MOREIRA, *Constituição da República Portuguesa: anotada, cit.*,p. 556-557.
[69] *Idem,* p. 557-558.
[70] David MASSENO, *O novo Regulamento Geral sobre a proteção de dados da União Europeia,* Recife, Brasil, 2016, p.4. Consultado em 01-02-2018 e disponível em: http://manueldavidmasseno.academia.edu/research#talks
[71] David MASSENO, *O novo Regulamento Geral sobre a proteção de dados da União Europeia, cit.,* p. 5.

O Tratado de Lisboa veio introduzir novos fatores no que respeita ao processamento e proteção de dados pessoais, nomeadamente no artigo 16.º do TFUE (Tratado de Funcionamento da União Europeia). [72]

O artigo 16.º, nº 2 introduz uma base forte para uma base comum no que respeita à proteção de dados pessoais que se aplica às instituições e organismos europeus e aos próprios Estados-Membros em certas circunstâncias. Definindo assim, «o Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes.»[73]

E, ainda, no Tratado da União Europeia é feita uma menção a este artigo, nomeadamente no seu artigo 39.º "em conformidade com o artigo 16.º do Tratado sobre o Funcionamento da União Europeia e em derrogação do n.º2 do mesmo artigo, o Conselho adota uma decisão que estabeleça as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relativas à aplicação do presente capítulo e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes." [74]

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

A União Europeia tem demonstrado preocupação em matéria de proteção de dados pessoais ao longo dos tempos, designadamente, através da Diretiva 95/45/CE, onde ficaram plasmados princípios básicos de processamento de dados pessoais e verifica-se a tentativa de manter a maior transparência possível e assegurar o controlo individual do processamento de

[72] Ángeles Guitiérrez ZARZA, *The Emergence of Information and Data Protection in Cross-border Criminal Proceedings in Europe,* New York, Springer, p. 25.
[73] *Idem,* p.26.
[74] *Ibidem.*

dados pessoais seja o mais eficiente possível.[75] O Parlamento Europeu com a Diretiva de 1995 estabeleceu regras mínimas no que respeita à proteção de dados pessoais sendo um importante texto legislativo no que respeita a estas questões cujo objetivo era a harmonização da legislação europeia com as legislações nacionais. [76] [77] [78]

A Diretiva não se aplicava apenas aos Estados Membro da União mas ao EEE (Espaço Económico Europeu), incluindo a Islândia, o Listenstaine e a Noruega. [79]

A Diretiva 95/45/CE foi um texto legislativo muito importante no que respeita à proteção de dados devido ao tempo em que esteve em vigor e por todas as questões que levantou ao longo do tempo em que esteve em vigor. O *Working Party* 29, Grupo de Trabalho Artigo 29.º, estabelecido no âmbito da Diretiva 95/45/CE como órgão consultivo independente no âmbito da proteção de dados e que tinha essencialmente quatro objetivos, conforme o artigo 30.º: analisar quaisquer questões relativas à aplicação das disposições nacionais tomadas nos termos da presente diretiva, com vista a contribuir para a sua aplicação uniforme; dar parecer à Comissão sobre o nível de proteção na Comunidade e nos países terceiros; aconselhar a Comissão sobre quaisquer projetos de alteração da presente diretiva ou sobre quaisquer projetos de medidas adicionais ou específicas a tomar para proteger os direitos e liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais, bem como sobre quaisquer outros projetos de medidas comunitárias com incidência sobre esses direitos e liberdades e dar parecer sobre os códigos de conduta elaborados a nível comunitário. Teve uma grande importância no auxílio do entendimento destas questões através da Orientações que emitiu ao longo dos anos.

A Diretiva introduziu um conceito de dados pessoais ou a informação pessoal correspondem "qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser

---

[75] Ted DUNSTONE, Neil YAGER, *Biometric System and Data Analysis, Design, Evaluation and Data Mining,* Australia, Springer, 2009, p. 23.
[76] Richard JIANG,Somaya AL-MAADEED, Ahmed BOURIDANE, Prof. Danny CROOKES, Azeddine BEGHDADI, *Biometric Security and Privacy, in* Pedro Miguel FREITAS, Teresa Coelho MOREIRA, Francisco ANDRADE, *Data Protection and Biometric Data: European Union Legislation,* Switzerland, 2016, p. 420.
[77] Demetrius KLITOU, *Privacy-Invading Technologies and Privacy by Design – Safeguarding Privacy, Liberty and Security in the 21st Century,* p. 28.
[78]Manual da Legislação Europeia de Proteção de Dados, Agência dos Direitos Fundamentais da União Europeia, Conselho da Europa, 2014, p. 18. Consultado em 01-02-2018 e disponível em https://www.coe.int/en/web/data-protection/home
[79] *Idem,* p. 19.

identificado, direta ou indiretamente". Os dados pessoais incluem assim, o nome, a morada, a data de nascimento, o número de identificação, entre outros. Contudo, dados pessoais não se esgotam nos exemplos anteriormente referidos. Além destes, dados pessoais podem ser os hábitos de consumo da pessoa, os movimentos diários, os afazeres e atividades privadas, o registro de votos, as conversas privadas, as interações, as imagens, o histórico médico, o ADN, os dados financeiros, os dados biométricos e outros que aqui não se encontram referidos, uma vez que esta lista é bastante mais extensa. [80]

A Diretiva conferia grande atenção à transferência de dados para os países não pertencem à União Europeia e decreta a sua proibição da transferência dos dados para aqueles que não garantam um nível de proteção adequada. O artigo 25.º avaliando a adequação nível de proteção da privacidade no país deve se ter conta quatro critérios: a natureza dos dados, o propósito e a duração da operação ou operações de tratamento propostas, as regras jurídicas quer gerais e sectoriais e, ainda, as regras profissionais e as medidas de segurança cumpridas. [81] Esta diretiva não se aplica ao que respeita à cooperação policial e judicial da União Europeia artigo 3.º nº 2. [82]

A Diretiva enquadra-se na tipologia de atos normativos da União europeia, artigo 288.º do Tratado de Funcionamento da União Europeia (TFUE) também pode ser designada como uma norma indireta. Traduz-se num processo legislativo dividido em dois momentos uma vez que se dirige aos Estados, mas supõe um ato normativo nacional para a sua aplicação, pressupõe medida nacional para a sua execução. A Diretiva pode ser caraterizada como um ato normativo incompleto, pois vincula os Estados-membros, mas só com a sua transposição é que esta adquire caráter normativo. A Diretiva fixa os objetivos a cumprir, mas confere aos Estados-membros flexibilidade para os concretizar, carateriza-se por ser um processo maleável em contraste com o regulamento que se carateriza por ser mais rígido. Devido ao seu processo mais flexível de transposição para os ordenamentos jurídicos dos Estados-membros pode conduzir a discrepâncias de regulamentação e de interpretação destes

[80] Demetrius KLITOU, *Privacy-Invading Technologies and Privacy by Design – Safeguarding Privacy, Liberty and Security in the 21st Century,* p. 16
[81] *Idem*
[82] ÁNGELES GUTIÉRREZ ZARZA, *The Emergence of Information and Data Protection in Cross-border Criminal Proceedings in Europe,* Hargue, Springer, 2015, p. 23

atos normativos.[83] [84]A Diretiva 45/95/CE foi transposta para o ordenamento jurídico português pela Lei n.º 67/98, de 26 de outubro, alterada pela Lei 103/2015.

A Diretiva impunha a grandes exigências burocráticas às empresas através das exigências de autorização ou notificações prévias à autoridade de supervisão, em Portugal, a Comissão Nacional de Proteção de Dados representava custos burocrático às empresas de cerca de 130 milhões de euros por ano. A União Europeia com vista a facilitar o desenvolvimento de novos produtos e serviços e com o objetivo de simplificar o regime regulatório inicia em 2012, a discussão para a modificar o sistema legislativo à luz da evolução tecnológica. Após morosas e difíceis negociações dão origem ao novo Regulamento Geral sobre a Proteção de Dados, o Regulamento 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. [85] [86]

[83] Paulo Pitta de CUNHA, *Direito Europeu: instituições e políticas da União,* Coimbra, Almedina, 2006, p. 45.
[84] As fontes e o âmbito de aplicação do direito da União Europeia, Parlamento Europeu. Consultado a 01-03-2018 e disponível em; http://www.europarl.europa.eu/ftu/pdf/pt/FTU_1.2.1.pdf
[85] Maria Eduarda GONÇALVES, *O regulamento europeu sobre proteção de dados pessoais e o desafio do Big Data.* Consultado a 05-03-2018 e disponível em: http://boletim.oa.pt/oa-02/opiniao_maria-eduarda-goncalves
[86] Manual da Legislação Europeia de Proteção de Dados, *cit.,* p. 21.

Capítulo II – Novo Regulamento Geral sobre a Proteção dos dados

3. Fundamentos

O Novo Regulamento Geral sobre a Proteção de Dados, Regulamento(UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados ou RGPD) foi publicado no dia 4 de maio de 2016 e entrou em vigor no dia 25 de maio de 2018 e previu um período de dois anos de transição. Trata-se de um Regulamento e tem aplicação direta em todos os Estados Membros da União Europeia, em Portugal por força de o país integrar a União e por força dos artigos 7.º, nº 6 e 8.º, nº 4. [87] Os regulamentos são atos jurídicos da União Europeia, conforme do artigo 288.º do TFUE, têm caráter geral são obrigatórios em todos os seus elementos e é diretamente aplicável em todos os Estados-membros, isto é, por força automática produz efeitos jurídicos em todos os ordenamentos jurídicos da União Europeia, não necessita de atos nacionais de transposição. [88] [89]

O Regulamento tem como principais objetivos a harmonização, a cooperação e a coerência entre as Autoridades Nacionais, nesse sentido os artigos 62.º a 67.º, constituir uma resposta à globalização e evitar o *forum shopping* [90] dentro da União Europeia neste domínio e resulta como uma resposta ao facto do reconhecimento da Proteção de Dados como uma matéria ao nível da União, depois do Tratado de Lisboa. [91]

Âmbito territorial

O Regulamento constitui-se também como uma resposta às empresas que se aproveitavam da discrepância de regras ou da ausência delas em alguns países da União

[87] Alessandra SILVEIRA, *Princípios de Direito da União Europeia Doutrina e Jurisprudência,* 2.ª Edição, Lisboa, Quid Juris, p. 27.
[88] Paulo Pitta de CUNHA, *Direito Europeu: instituições e políticas da União, cit.,* p. 45.
[89] As fontes e o âmbito de aplicação do direito da União Europeia, Parlamento Europeu, *cit.*
[90] A pessoa intenta a ação pode ser tentada a escolher um foro não por ser o mais adequado para conhecer do litígio, mas porque as normas de conflitos de leis que este tribunal utilizará levarão à aplicação da lei que lhe é mais favorável. *In http://ec.europa.eu/civiljustice/glossary/glossary_pt.htm#Forum-shopping* data 28/06/2018
[91] David MASSENO, *O novo Regulamento Geral sobre a proteção de dados da União Europeia, cit.,* p. 11.

Europeia. Assim, de acordo com o artigo 3.º o Regulamento aplica-se ao tratamento de dados feitos fora do território dos Estados-membros da UE, por responsáveis pelo tratamento ou subcontratantes com estabelecimentos nestes, ao tratamento de dados de residentes na UE, por responsáveis pelo tratamento ou subcontratantes sem estabelecimentos na UE, se estes forem destinatários de ofertas de bens e serviços, mesmo sem pagamento direto, ou se existir controlo de seu comportamento, desde que na UE, n.º 2, alíneas a) e b). Aplicando-se assim aos sistemas IT (Tecnologias da Informação), aplicações e redes, em contexto empresarial ou corporativo e organizacional. [92]

Definições introduzidas pelo Regulamento

Para melhor compreensão do documento legislativo comunitário relativo à proteção de dados pessoais tem de se ter em consideração as várias definições fornecidas pelo artigo 4.º que iremos abordar nos pontos seguintes:

Conceito de dados pessoais

O RGPD profunda relativamente à Diretiva o conceito de dados pessoais definido pelo artigo 4.º, nº 1 "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 da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

Atualmente, o conceito de informação pessoal não se limita aquele que lhe foi conferido pelos direitos de personalidade, aliás o Tribunal Europeu dos Direitos do Homem adota uma conceção mais flexível do conceito. A privacidade não se constitui com o mesmo conceito de direitos pessoais, nem a proteção concedida pelo regime jurídico consagrado no artigo 80.º do Código Civil (CC) é parecida à consagrada pelo direito da proteção de dados, em todas as suas diferentes concretizações legislativas. Tanto se entende, como sendo pessoal, informação relativa à vida privada como à vida profissional e social. Por exemplo,

[92] A. Barreto Menezes CORDEIRO, *Dados Pessoais: Conceito, Extensão e Limites,* p. 12. Consultado em 05-03-2018 e disponível em: https://blook.pt/publications/publication/e38a9928dbce/

o facto de uma informação pessoal se desencadear no âmbito das relações laborais, isso, não altera o facto de se tratar de uma informação pessoal, o RGPD faz referência várias situações em matéria laboral, designadamente, os artigos 9.º, nº 2, alínea h), 77.º, nº 1 e o 88.º. [93]

Assim, informação pessoal podem ser: nome, data de nascimento, número de cartão de cidadão ou morada; características físicas como: género, altura, peso, cor dos olhos ou do cabelo; considerações íntimas como: crenças, opiniões, desejos, posições políticas ou religiosas; caraterísticas profissionais e académicas tais como: títulos e graus ou estatutos profissionais e laborais e caraterísticas patrimoniais como os casos dos direitos de propriedade. [94]

No artigo 9.º, nº 1 proíbe o tratamento de dados que "revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa". O Regulamento para além de definir o que são dados pessoais, possui também definições de dados genéticos, dados biométricos e dados relativos à saúde. Os dados genéticos encontram-se definidos no artigo 4.º, nº 13, "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". Os dados biométricos, de acordo com o disposto no artigo 4.º, nº 14 "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". Os dados relativos à saúde encontram-se descritos no artigo 4.º, nº 15, "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde".

Tratamento, limitação do tratamento e pseudonimização

Desde logo, deve-se ter em conta que tratamento dos dados pessoais deverá ser um direito para servir as pessoas. O direito à proteção de dados deve ser equilibrado com os

[93] A Barreto Menezes CORDEIRO, *Dados Pessoais: Conceito, Extensão e Limites, cit.,* p. 5.
[94] *Idem,* p. 6.

outros direitos fundamentais, em respeito pelo princípio da proporcionalidade uma vez que o direito à proteção de dados não é absoluto. O tratamento de dados pessoais deve obedecer aos princípios da proporcionalidade, da transparência e da minimização do tratamento. [95]

No n.º 2 do artigo 4.º define tratamento como uma operação ou um conjunto de operações efetuadas sobre os dados pessoais ou sobre conjuntos de dados pessoais, por meios autonomizados ou não autonomizados, 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 destruição.

No n.º 3, define limitação do tratamento como a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro.

O tratamento dos dados sendo o RGPD é norteado por um conjunto de princípios de acordo com o artigo 5.º, designadamente, o princípio da licitude, lealdade e transparência, o que implica que apenas podem ser objeto do tratamento de dados relativamente aos quais se verifique um dos fundamentos jurídicos para o tratamento inseridos no artigo 6.º. O tratamento, deve ainda, encontrar-se dentro dos limites dos quais foram transmitidos ao titular dos dados no momento da recolha. Outro princípio tem que ver com a limitação das finalidades e da conservação o que implica que os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados para finalidades distintas, a menos que um interesse superior prevaleça, como por exemplo, fins de arquivo público. Os dados deverão ser conservados durante o tempo estritamente necessário. O tratamento deve ser orientado pelo princípio da minimização dos dados, isto é, os dados pessoais devem ser adequados, pertinentes e limitados ao que é estritamente necessário. Os dados devem ser tratados tendo em conta o princípio da exatidão devendo estar atualizados sempre que necessário. Por fim, o tratamento deve seguir-se por o princípio da integridade e da confidencialidade, ou seja, os dados deverão ter tratados de uma forma que se garanta a sua segurança, compreendendo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental. Os princípios devem ser cumpridos

[95] Nesse sentido, Regulamento Geral sobre a Proteção de Dados, Considerandos 4, 39, 58, 78, 159.

e o responsável pelo tratamento deve ser capaz de demonstrar com evidências o cumprimento. [96]

O tratamento deve obedecer a critérios de licitude explanados no artigo 6.º que dispõe que o tratamento só será lícito quando, o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoas para uma ou mais finalidades específicas; o tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; o tratamento for necessário para o cumprimento de uma obrigação jurídica que o responsável do tratamento está sujeito; o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento ou quando o tratamento for necessário para os interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança, sendo portanto, estas as seis formas lícitas para o tratamento de dados pessoais.

A pseudonimização encontra-se definida no n.º 5 tem que ver com o tratamento dos 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. O RGPD alerta para o facto de que quando se recorre a esta técnica pode reduzir-se os riscos para os titulares dos dados, mas não exclui outras medidas de proteção. [97]

Definição de perfis e ficheiro

Definição de perfis é entendido como qualquer forma de tratamento autonomizado 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.

[96] Filipa MAGALHÃES, *Regulamento Geral de Proteção de Dados,* Ordem dos Contabilistas Certificados, 2018, p. 29.
[97] Nesse seguimento, Regulamento Geral sobre a Proteção de Dados, considerando 24.

O artigo 22.º confere ao titular dos dados o direito a não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que afete significativamente de forma similar, o n.º 2 do artigo confere as exceções.

O n.º 6 define ficheiro como qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico.

Responsável pelo tratamento, subcontratante e tratamento transfronteiriço

O n.º 7 define responsável pelo tratamento como a pessoa singular ou coletiva, 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, sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro.

O conceito de subcontratante encontra-se definido pelo n.º 8 como uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

O tratamento transfronteiriço encontra-se definido no n.º 28, alínea a) como o tratamento de dados pessoais que ocorre no contexto das atividades de estabelecimentos em mais do que um Estado-Membro de um responsável pelo tratamento ou um subcontratante da União, caso o responsável pelo tratamento ou o subcontratante esteja estabelecido em mais do que Estado-Membro ou b) o tratamento de dados pessoais que ocorre no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, mas que afeta substancialmente, ou é suscetível de afetar substancialmente, titulares de dados em mais do que um Estado-Membro.

A identificação da autoridade de controlo principal é pertinente apenas quando o responsável pelo tratamento procede ao tratamento transfronteiriço de dados pessoais, isto é, se uma organização dispuser de estabelecimentos em dois países da União Europeia (UE) e o tratamento dos dados ocorrer no contexto das atividades, estamos perante tratamento

transfronteiriço. Contudo, a organização poderá exercer as atividades de tratamento em apenas num estabelecimento da União Europeia, mas se a atividade afetar substancialmente ou for suscetível de afetar substancialmente os titulares dos dados em dois ou mais Estados-Membros, estamos perante um tratamento transfronteiriço. [98]

O Grupo de artigo 29.º veio auxiliar no entendimento do conceito de afeta substancialmente para as autoridades de controlo. Para tal, será necessário aferir o contexto do tratamento, o tipo de dados, a finalidade do tratamento e outros fatores, nomeadamente aferir se o tratamento:

a) causa, ou é suscetível de causar, danos, prejuízos ou transtornos às pessoas;

b) tem, ou é suscetível de ter, um efeito real em termos de limitação dos direitos ou negação das oportunidades;

c) afeta, ou é suscetível de afetar, a saúde, o bem-estar ou a paz de espírito das pessoas;

d) afeta, ou é suscetível de afetar, a situação financeira ou económica ou as circunstâncias das pessoas;

e) deixa pessoas expostas a situações de discriminação ou tratamento abusivo;

f) implica a análise das categorias especiais de dados pessoais ou de outros dados intrusivos, particularmente, dados pessoais de crianças;

g) causa, ou é suscetível de causar, uma alteração significativa no comportamento das pessoas;

h) tem consequências improváveis, imprevistas e indesejáveis para as pessoas;

i) cria embaraço ou outros resultados negativos, incluindo danos à reputação, ou

j) implica o tratamento de um vasto leque de dados pessoais. [99]

Destinatário e terceiro

Entende-se por 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

[98] Orientações sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou subcontratante, Grupo do Artigo 29.º para a Proteção de Dados, 16/PT, WP 244 rev.0, p. 3-4.
[99] *Idem.*

União ou dos Estados-Membros não são considerados destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir regras de proteção de dados aplicáveis em função dessas finalidades, segundo o n.º 9.

Terceiro define-se como 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 dados pessoais, de acordo com o n. º10.

Consentimento

O artigo 4.º, nº 11 define consentimento 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" é um dos fundamentos legais para o tratamento de dados pessoais. [100]

O consentimento constitui uma das seis bases legais para o tratamento de dados de acordo com o Regulamento. Quando o responsável pelo tratamento inicia o tratamento dos dados deve considerar se existe um motivo para o tratamento dos mesmos ou se deve escolher outro motivo. [101]

Regra geral, o consentimento só deve ser escolhido como uma base legal adequada para o tratamento de dados, quando se confere ao titular dos dados uma escolha genuína no que diz respeito à aceitação ou não dos termos oferecidos. Quando o responsável pelo tratamento solicita o consentimento deve avaliar se irá cumprir todos os requisitos de um consentimento válido. Quando o consentimento é obtido de uma forma válida e legal é um mecanismo que fornece ao titular dos dados um controlo sobre se os seus dados pessoais e se estes serão ou não processados, caso não se verifique este controlo, o consentimento é enganador e inválido e ilegal ou processamento. [102]

---

[100] Manual da Legislação Europeia de Proteção de Dados, Agência dos Direitos Fundamentais da União Europeia, Conselho da Europa, 2014, p. 59. Consultado em 01-02-2018 e disponível em https://www.coe.int/en/web/data-protection/home

[101] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP187, p.4.

[102] *Idem,* p.4-5.

O consentimento é do que um convite aos indivíduos para aceitar uma operação de tratamento dos seus dados pessoais que deve ser sujeito a requisitos rigoroso uma vez que se está perante direitos fundamentais dos titulares dos dados e o responsável pelo tratamento pretende sujeitar os dados a uma operação de tratamento que seria ilícita sem o consentimento. O papel do consentimento é sublinhado pelos artigos e 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia. Salienta-se que o facto de o responsável pelo tratamento obter o consentimento por parte do titular dos dados não anula ou diminui as obrigações do responsável pelo tratamento de observar os princípios de tratamento consagrados pelo Regulamento, especialmente no artigo 5.º no que respeita à equidade, necessidade e proporcionalidade e qualidade dos dados. [103]

O consentimento explícito também é uma das isenções à proibição de tratamento de categorias especiais de dados conforme o descrito no artigo 9.º. [104]

Segundo o artigo 4.º, n 11 o consentimento deve ser dado de forma livre, específica, informado, 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. [105]

Dado de forma livre

O elemento livre implica uma escolha e um controlo real para os titulares dos dados. Se a escolha não se constituir livre e sentir a obrigação de consentir ou caso contrário suportará consequências negativas se não fizer, nesses casos, o consentimento será inválido. Se o consentimento constituir uma parte não negociável dos termos e condições, não será válido. Assim, como se o titular dos dados não tiver a faculdade de o retirar a todo o tempo, sem prejuízo. [106]

[103] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP187, p. 5.
[104] *Idem,* p. 6.
[105] *Ibidem.*
[106] *Idem,* p. 6-7.

Desequilíbrio de poder

Logo no considerando 43 refere que o consentimento não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos que exista um desequilíbrio manifesto entre o titular dos dados e o responsável de tratamento, nomeadamente, quando o responsável pelo tratamento é uma autoridade pública. O Grupo Artigo 29.º considera que em princípio existem outras bases legais que são adequadas à atividade das autoridades públicas, tais como o artigo 6.º, nº 1 alínea c) e e). [107]

O desequilíbrio acontece também em contexto laboral devido à dependência que resulta da relação empregador e empregado. É improvável que a pessoa em causa possa negar o consentimento ao seu empregador para o tratamento de dados sem encarar medo ou risco real de efeitos prejudiciais com o ato da recusa. [108]

Condicionalidade

No sentido de aferir se o consentimento é dado livremente o artigo 7.º, n.º 4 desempenha uma função importante, dispondo o seguinte: "ao avaliar se o consentimento é dado livremente, há que verificar com máxima atenção se, designadamente, a execução do contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato. O artigo indica assim que as situações em que se integra o consentimento na aceitação de termos ou condições ou quando se vincula ao fornecimento de um contrato ou serviço o pedido de consentimento para processar dados pessoais que não são necessários para a execução desse contrato ou serviço, são situações consideravelmente indesejáveis. O consentimento não será considerado válido. [109] [110]

O objetivo do artigo 7.º, n.º 4 tem que ver com o garante da finalidade do tratamento de dados pessoais não seja mascarada ou camuflada com a prestação de um serviço para os

[107] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP187, p. 7.
[108] *Idem,* p. 8.
[109] *Idem,* p. 8-9.
[110] Considerando 43, "Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução".

quais os dados não se constituem necessários. As duas bases legais para o tratamento de dados, o consentimento e a execução do contrato não podem ser misturadas.

Relativamente, ao termo "necessário para a execução do contrato" deve ser interpretado de forma estrita, isto é, o tratamento de dados deve ser necessário para cumprir o contrato com cada assunto de dados individual, por exemplo, incluir a morada quando se compram bens online ou o tratamento de informações salariais e detalhe da conta bancário para o tratamento de salários. Assim, deve existir um vínculo direto entre o tratamento de dados e o propósito da execução do contrato. [111]

O responsável pelo tratamento processa dados pessoais que de facto sejam necessários para a execução do contrato é provável que a base legal correta seja o artigo 6.º, n. 1 alínea b). Assim, não é necessário usar outra base legal.[112]

O artigo 7.º coloca o ónus da prova no responsável pelo tratamento, "quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais". Esta disposição decorre do princípio geral da responsabilidade explanado em todo o Regulamento. Contudo, quando o consentimento é fornecido pelo artigo 7.º, n.º 4 será mais difícil para o responsável pelo tratamento provar que o consentimento foi fornecido livremente pela pessoa em causa. [113]

Granularidade – consentimento em propósitos separados

Quando se adquire um determinado serviço este pode implicar diferentes operações de tratamento para vários fins ou propósitos. Nos casos em que isso acontece, o titular dos dados deve ser livre para escolher quais os fins ou propósitos que aceita, não devem consentir em pacote ou todos juntos os fins do processamento. Pode ocorrer que dependendo do serviço pode ser necessário garantir vários consentimentos para oferecer um único serviço. [114]

No sentindo de auxiliar uma melhor interpretação o considerando 43 dispõe que "presume-se que o consentimento não é dado de livre vontade se não for possível dar o

[111] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP187, p. 8-9.
[112] *Idem,* p. 9.
[113] *Idem,* p.10-17.
[114] *Ibidem.*

consentimento separadamente para as diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso especifico, ou se a execução de um contrato, incluindo a prestação de serviços, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução". No mesmo sentido, o considerando 32 dispõe que "o consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins". [115]

Nos casos em que o responsável pelo tratamento acorda várias finalidades para o tratamento e não procurou o consentimento em separado para cada finalidade, tal facto, traduz uma falta de liberdade para o titular dos dados. A granularidade ou a separação de propósitos está relacionada com a necessidade de que o consentimento ser específico.

Quando o consentimento não é dado de forma separada para cada propósito de tratamento, será um consentimento inválido. [116]

Detrimento/ prejuízo

O responsável pelo tratamento deve ser capaz de demonstrar que o titular dos dados pode recusar ou retirar o consentimento sem prejuízo. Segundo o considerando 42 "sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance". O responsável pelo tratamento deverá provar que a retirada do consentimento não conduz a nenhum prejuízo ou dano ao titular dos dados e, portanto, não se verifica uma desvantagem clara para aqueles que retiram o consentimento. [117]

[115] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP187, p. 11.
[116] *Idem.*
[117] *Ibidem.*

Específico

O artigo 6.º, n.º 1, alínea a) prescreve que "o titular dos dados tiver dado o consentimento para o tratamento dos sus dados pessoais para uma ou mais finalidades específicas". O requisito de que o consentimento deve se configurar como "específico" tem como objetivo garantir o controlo e a transparência por parte do titular dos dados. Este requisito está ligado ao requisito do consentimento informado e, em simultâneo, deve ser interpretado com o princípio da granularidade para obter um consentimento livre. Portanto, para cumprir com o elemento da especificidade do consentimento, o responsável pelo tratamento deve ter em consideração, a especificidade da finalidade com salvaguarda contra o desvirtuamento da função, a granularidade ou os propósitos dos pedidos de consentimento e separação as informações relacionadas com a obtenção de consentimento para as atividades de processamento de dados das informações relacionadas com outros assuntos. [118] [119]

Quando o responsável pelo tratamento processa/trata os dados com base no consentimento e pretende processar os dados com base numa nova finalidade, o responsável pelo tratamento necessita de solicitar um novo consentimento do titular dos dados para o novo propósito de tratamento. [120]

Informado

O Regulamento reforça o requisito de que o consentimento deve ser informado. O artigo 5.º demostra que o requisito da transparência se constitui como um dos princípios fundamentais no tratamento de dados e intimamente ligado aos princípios da justiça e da legalidade. É essencial fornecer informações aos titulares dos dados antes da obtenção do consentimento para que lhes seja possível tomar uma decisão informada sobre a questão, sendo necessário que estes entendam com o que estão a concordar e que podem exercer o direito de retirar o seu consentimento. Se o responsável pelo tratamento não fornecer todas as informações, o controlo dos dados será aparente e enganador. Quando o responsável pelo

[118] Considerando 43, Regulamento Geral sobre a Proteção de Dados.
[119] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP187, p. 12.
[120] *Idem,* p. 12-13.

tratamento não cumpre os requisitos do consentimento informado implica que o consentimento seja inválido e poderá incorrer na violação do artigo 6.º. [121]

O consentimento seja informado tem requisitos mínimos para que se possa ser considerado informado, as informações necessárias são: a identidade do responsável pelo tratamento, o objetivo para cada uma das operações de tratamento para o consentimento é solicitado, que tipo de dados são recolhidos e usados, a possibilidade de retirada do consentimento, informações sobre a utilização de dados para decisões baseadas exclusivamente no processamento automatizado, incluindo definições de perfis, se o consentimento diz respeito a transferências, sobre os possíveis riscos de transferência de dados para países terceiros na ausência de uma decisão de adequação e salvaguardas apropriadas.

O Grupo de Artigo 29.º constata que no caso em que o consentimento deve ser solicitado deve ser invocado por múltiplos responsáveis pelo tratamento ou se os dados devem ser transferidos ou processados por outros responsáveis pelo tratamento a quem desejam confiar o consentimento original, essas informações devem ser nomeadas. Os subcontratantes não precisam ser nomeados como parte dos requisitos de consentimento, embora, nos artigos 13.º e 14.º disponham que os responsáveis pelo tratamento deverão fornecer uma lista completa de destinatários ou os vários recetores, incluindo os subcontratantes. O Grupo Artigo 29.º considera que dependendo das circunstâncias do caso, podem ser necessárias mais informações para permitir aos titulares dos dados compreendam completamente as operações de tratamento em causa. [122]

Relativamente à forma como a informação deve ser provida aos titulares dos dados para cumprir o consentimento informação o RGPD não fornece nenhum formulário, ou seja, estas podem ser apresentadas de várias formas, tais como, declarações escritas ou orais, mensagens de vídeo ou áudio. No entanto, os requisitos para o consentimento informado encontram-se previstos no artigo 7.º, n.º 2 e no considerando 32 o que impõe um alto padrão de clareza e de acessibilidade da informação. Aquando da solicitação do consentimento, os responsáveis pelo tratamento devem garantir a utilização de uma linguagem clara e simples, o que implica que a mensagem seja altamente compreensível para um cidadão comum, da

[121] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP187, p. 12-13.
[122] *Idem.*

mesma forma as políticas de privacidade não devem ser longas e ilegíveis. O consentimento deve ser claro e distinguido dos demais assuntos, também numa linguagem clara e acessível, o que significa que as informações relevantes para a toma de decisões informadas sobre a aceitação ou não do consentimento não podem ser ocultas nos termos e condições gerais. [123]

O consentimento deve ser um ato afirmativo claro, o implica que deve sempre ser dado por meio de uma ação ou declaração ativa devendo ser óbvio e notório que a pessoa em causa tenha consentido o tratamento específico. No contexto dos ambientes online, a utilização de operações padrões em que o titular dos dados fornece o seu consentimento com base no silêncio, não constitui um consentimento inequívoco. O consentimento pode ser obtido através de uma declaração oral e registada, com a devida antecedência do fornecimento das informações disponíveis para o titular dos dados antes da indicação do consentimento. O Grupo Artigo 29.º afirma que o uso de caixas *opt-in*[124] pré-marcas é inválido segundo o Regulamento, o silêncio ou inatividade por parte do titular dos dados, o simples prosseguimento do serviço, não podem constituir consentimento. [125]

O consentimento fornecido através de meios eletrónicos é problemático uma vez que muitos serviços precisam de dados pessoais para funcionar, os titulares dos dados recebem pedidos múltiplos de consentimento que precisam de respostas por meios de cliques o que pode conduzir a uma fadiga do indivíduo. O consentimento deve ser obtido antes do responsável pelo tratamento começar a processar dados pessoais para os quais o consentimento é necessário, artigo 4.º, nº 11, artigo 6.º, n.º 1 e artigo 40.º. [126]

A obtenção do consentimento explícito constitui-se necessário em certas situações em que surgem riscos graves de proteção de dados, isto é, onde existe um alto controlo do indivíduo sobre os seus dados pessoais é considerado apropriado. O consentimento explícito encontra-se plasmado no artigo 9.º e desempenha uma função importante no que respeita ao tratamento de categorias especiais de dados, nas disposições sobre a transferências de dados

[123] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP187, p. 13.
[124] *Opt-in* é uma expressão da vontade de um utilizador de meios tecnológicos, como por exemplo um sítio da internet, afastando-se a presunção de ter aceite algo pelo silêncio.
[125] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP187, p.13-18.
[126] *Ibidem.*

para países terceiros ou organizações internacionais na ausência de salvaguardas adequadas do artigo 49.º. [127] [128]

O RGPD estipula requisitos para que os responsáveis pelo tratamento assegurem medidas adicionais para garantir que obtêm, mantêm e demostrem que o consentimento é válido. O artigo 7.º estabelece as condições para um consentimento válido com disposições sobre a manutenção dos registos do consentimento e sobre o direito da retirada do consentimento de uma forma fácil. Como já foi anteriormente referido, o responsável deverá ser capaz de demostrar que o titular dos dados forneceu o seu consentimento, mas são livres para desenvolver métodos para cumprir esta disposição, o que significa que devem ser capazes de ter dados suficientes para demonstrar como o consentimento foi obtido enquanto que a operação de tratamento dos dados em questão decorre. Após, as atividades de tratamento terminar devem ser mantidas as provas do consentimento não mais do que a estritamente necessária para o cumprimento da obrigação legal ou para o estabelecimento, exercício ou defesa das reivindicações legais, segundo o artigo 17.º, n.º 3 alínea b) e e). [129]

Relativamente à retirada do consentimento, o artigo 7.º, nº 3 dispõe "o titular dos dados tem o direito a retirar o seu consentimento a qualquer momento", isto é, o consentimento deve ser tão fácil de dar quanto de retirar e em qualquer momento. Quando o consentimento é fornecido através de plataformas e ambientes digitais a retirada de consentimento deve ser realizada nos mesmos termos, e sem prejuízo para a pessoa em questão. [130]

Violação de dados pessoais

O artigo 4.º, n.º 12 dispõe que violação de dados pessoais constituiu uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou acesso, não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

---

[127] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP187, p. 19.
[128] Considerando 71, Regulamento Geral sobre a Proteção de Dados.
[129] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP187, p.18-21.
[130] *Idem.*

No âmbito das violações de dados pessoais o RGPD abarca mudanças nomeadamente na sua comunicação à autoridade de controlo e ao titular dos dados. Assim, o responsável pelo tratamento deverá informar sem demora injustificada, o titular dos dados da violação de dados pessoais quando for provável que esta resulte um elevado risco para os direitos e liberdades da pessoa singular, com o intuito de tomar as precauções necessárias. A comunicação deverá ter como conteúdo a natureza da violação dos dados pessoais e dirigir recomendações à pessoa singular em causa para atenuar potenciais efeitos adversos. A comunicação aos titulares dos dados deverá ser efetuada logo que seja razoavelmente possível, em estreita cooperação com a autoridade de controlo e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes. [131]

Quando ocorre uma violação dos dados tem de se verificar se todas as medidas tecnológicas de proteção e de organização foram aplicadas para informar o mais rapidamente possível a autoridade de controlo e o titular dos dados. A entidade/organização para comprovar que a notificação foi enviada sem demora injustificada deve-se ter em consideração, a natureza e a gravidade da violação dos dados pessoais e as relativas consequências e efeitos adversos para o titular dos dados. O envio da notificação pode ter como consequência uma intervenção da autoridade de controlo tendo em conta as suas funções e competências. [132]

A regras relativas ao formato e aos procedimentos das notificações das violações de dados pessoais deverão ter consideração as circunstâncias dessas violações, nomeadamente, a existência ou não de proteção dos dados pessoais através de medidas técnicas de proteção adequadas para reduzir eficazmente a capacidade de usurpação da identidade ou outras formas de utilização abusiva. As regras e procedimentos deverão ter conta os legítimos interesses das autoridades de polícia nos termos e caso em que a divulgação precoce de informações possa dificultar desnecessariamente a investigação das circunstâncias da violação de dados. [133]

No mesmo sentido, o artigo 33.º com a epígrafe "Notificações de uma violação de dados pessoais à autoridade de controlo" onde dispõe que o responsável pelo tratamento em caso de violação de dados pessoais notifica à autoridade de controlo competente, sem demora

[131] Nesse seguimento, considerando 86, Regulamento Geral sobre a Proteção de Dados.
[132] Nesse sentido, considerando 87, Regulamento Geral sobre a Proteção de Dados.
[133] Nesse sentido, considerando 88, Regulamento Geral sobre a Proteção de Dados.

justificada e sempre que possível no prazo de 72 horas após o conhecimento da mesma, a menos que da violação dos dados não resulte um risco para os direitos e liberdades das pessoas singulares. Quando não for possível a notificação no prazo de 72 horas, a justificação da demora deve ir acompanhada na notificação. O n.º 2 prescreve que o subcontratante notifica o responsável pelo tratamento sem demora injustificada após o conhecimento da violação.

Quanto aos requisitos da notificação, esta segundo o n.º 3 deve conter, pelo menos:

a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;

b) Comunicar o nome e os contatos do encarregado de proteção de dados ou de outro ponto de contato onde possam ser obtidas mais informações;

c) Descrever as consequências prováveis da violação de dados;

d) Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

Relativamente, à comunicação da violação dos dados pessoais ao titular dos dados esta deve ter lugar quando a violação for suscetível de implicar um elevado risco para os direitos e liberdades do indivíduo e sem demora injustificada. A comunicação deve ser feita numa linguagem clara e simples deve conter qual a natureza dos dados, identificar e comunicar o nome e os contatos do encarregado de proteção de dados ou de outro ponto de contato onde possam ser obtidas mais informações, descrever as consequências prováveis da violação de dados e descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos, segundo o artigo 34.º.

O considerando 75 auxilia no entendimento do que são riscos para os direitos dos cidadãos, assim os eventos cuja probabilidade e gravidade que resultem das atividades de tratamento de dados que possam causar danos físicos, materiais ou imateriais, em especial, quando o tratamento possa dar lugar à discriminação, à usurpação ou roubo de identidade, perdas financeiras, prejuízos para a reputação, perda de confidencialidade dos dados pessoais protegidos pelo sigilo profissional, a inversão não autorizada da pseudonimização ou

quaisquer outros prejuízos importantes de natureza económica e social, quando os titulares dos dados possam ficar privados dos seus direitos e liberdades do exercício do controlo sobre os respetivos dados pessoais, quando os dados tratados revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou condenações penais e infrações ou medidas de segurança conexa. Ainda, quando forem avaliados aspetos de natureza pessoal, em particular, as análises que digam respeito ao desempenho do trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, a fiabilidade do comportamento e a localização ou deslocações de pessoas, com a finalidade de definir ou fazer uso de perfis. Outro caso tem que ver quando o tratamento de dados relativos às pessoas singulares vulneráveis, em especial, as crianças ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número dos titulares dos dados.

O responsável pelo tratamento a fim de promover o cumprimento do RGPD nos casos em que as operações de tratamento sejam suscetíveis de resultar num elevado risco para os direitos e liberdades dos titulares dos dados este deverá se encarregar de realizar uma avaliação de impacto. [134]

Dados genéticos, biométricos e relativos à saúde e as categorias especiais de dados

Os dados genéticos são dados pessoais relativos às caraterísticas 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 em causa, nomeadamente da análise de cromossomas, ácido desoxirribonucleico(ADN) ou ácido ribonucleico (ARN), ou da análise de outro elemento que permita obter informações equivalentes. [135]

Os dados biométricos têm que ver com os dados pessoais resultantes de um tratamento técnico específico relativo às caraterísticas físicas, fisiológicas ou comportamentais de uma pessoa singular que permitem ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dactiloscópicos.

[134] Nesse sentido, considerando 84, Regulamento Geral sobre a Proteção de Dados.
[135] Nesse sentido, o artigo 4.º, nº 14 e considerando 34 do Regulamento Geral sobre a Proteção de Dados.

No que respeita aos dados relativos à saúde têm que ver com os dados pessoais relacionados com a saúde física e mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o estado de saúde, conforme a Diretiva 24/2011/EU do Parlamento e do Conselho, essa informação pode ser bastante vasta, designadamente, informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico *in vitro*.[136]

Relativamente às categorias especiais de dados o Regulamento dá margem de manobra aos Estados-Membros para especificarem as suas regras nestas matérias, sendo que o RGPD estabelece um nível de proteção mínimo. [137] O tratamento das categorias especiais de dados está previsto no artigo 9.º, o n.º 1 dispõe que "é proibido o tratamento de dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções filosóficas ou religiosas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual da pessoa", o n.º 2 prevê as derrogações à proibição do tratamento.

Segundo o artigo 10.º o tratamento de dados pessoais relacionados com condenações penais e infrações ou com medidas de segurança conexas, com base no artigo 6.º, n.º 1 só é efetuado sob o controlo de uma autoridade pública ou se o tratamento for autorizado por disposições do direito da União ou de um Estado-Membro que prevejam garantias adequadas para os direitos e liberdades dos dados. Os registos completos das condenações penais só são conservados sob o controlo das autoridades públicas.

Estabelecimento principal

O estabelecimento principal tem um papel importante quando a organização atua em mais do que um Estado-Membro. Assim, quando o responsável pelo tratamento com vários

[136] Nesse sentido, art. 14, nº 16 do RGPD.
[137] Nesse seguimento, considerando 10 RGPD.

estabelecimentos nos Estados-Membros, o local onde se encontra a administração central na União, será o estabelecimento principal, a não ser que as decisões sobre as finalidades e os meios de tratamento dos dados pessoais sejam tomadas noutro estabelecimento do responsável pelo tratamento na União e que este estabelecimento tenha competência para mandar executar tais decisões. O estabelecimento principal será o tiver tomado as referidas decisões. No caso dos subcontratantes com estabelecimentos em vários Estados-Membros, o local onde se encontra a sua administração central na União, ou nos casos, em que o subcontratante não tenha administração central na União, o estabelecimento principal deverá ser onde o subcontratante exerce as principais atividades de tratamento no contexto das atividades de um estabelecimento do contratante. [138] [139]

Representante, empresa, grupo empresarial, regras vinculativas aplicáveis às empresas

O representante afigura-se como uma pessoa singular ou coletiva estabelecida na União, que designada por escrito pelo responsável pelo tratamento ou subcontratante, nos termos do artigo 27.º representa o responsável pelo tratamento ou o subcontratante no que se refere às obrigações do Regulamento, conforme o disposto no artigo 4.º, n.º 17.

Empresa define-se nos termos do Regulamento como pessoa singular ou coletiva que independente da sua forma jurídica, exerce atividade económica, incluindo, sociedades, associações que exerçam atividade económica, de acordo com o artigo 4.º, n.º 18.

Grupo empresarial tem que ver com um grupo composto pela empresa que exerce o controlo e pelas empresas controladas, artigo 4.º, n.º 19.

As regras vinculativas aplicáveis às empresas são as regras internas de proteção de dados pessoais aplicados por um responsável pelo tratamento ou um subcontratante estabelecido no território de um Estado-Membro para as transferências de dados pessoais para um responsável ou subcontratante num ou mais países terceiros, dentro de um grupo empresarial ou de um grupo de empresas envolvidas numa atividade económica conjunta, segundo o artigo 4.º, n.º 20.

---

[138] Nesse sentido, o artigo 4.º, nº 16 e considerando 36 do Regulamento Geral sobre a Proteção de Dados.
[139] Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, 01197/11/EN, WP187, p. 7-10.

Autoridade de controlo e autoridade de controlo interessada

A autoridade de controlo conforme o artigo 4.º, n.º 21 diz respeito à autoridade pública independente criada por um Estado-Membro nos termos artigo 51.º a quem cabe a responsabilidade pela fiscalização e aplicação do Regulamento, com o intuito de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a circulação desses dados na União.

A autoridade de controlo interessada segundo o artigo 4.º, n.º 22 tem que ver com a autoridade de controlo afetada pelo tratamento de dados pessoais pelo facto de: a) o responsável pelo tratamento ou o subcontratante estar estabelecido no território do Estado-Membro dessa autoridade de controlo; b) os titulares dos dados que residem no Estado-Membro dessa autoridade de controlo serem substancialmente afetados, ou suscetíveis de o ser, pelo tratamento de dados; ou c) ter sido apresentada uma reclamação junto dessa autoridade de controlo.

Objeção pertinente e fundamentada, serviço da sociedade de informação e organização internacional

A objeção pertinente e fundamentada é uma objeção a um projeto de decisão que visa determinar se há violação do presente no Regulamento ou se a ação prevista relativamente ao responsável pelo tratamento ou o subcontratante está em conformidade com a legislação, demonstrando claramente a gravidade dos riscos que advêm do projeto de decisão para os direitos e liberdades fundamentais dos titulares dos dados e, eventualmente para a circulação de dados pessoais no território da União.[140]

Os serviços da sociedade de informação encontram-se definido no artigo 1.º, n.º 1, alínea b) da Diretiva 2015/1535/UE do Parlamento e do Conselho, "«Serviço» significa qualquer serviço da sociedade da informação, isto é, qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços. Para efeitos da presente definição, entende-se por: i) «à distância»: um serviço prestado sem que as partes estejam simultaneamente presentes; ii) «por via eletrónica»: um serviço enviado desde a origem e recebido no destino através de instrumentos

[140] Nesse sentido, o artigo 4.º, n.º 24 do Regulamento Geral sobre a Proteção de Dados.

eletrónicos de processamento (incluindo a compressão digital) e de armazenamento de dados, que é inteiramente transmitido, encaminhado e recebido por cabo, rádio, meios óticos ou outros meios eletromagnéticos; iii) «mediante pedido individual de um destinatário de serviços»: um serviço fornecido por transmissão de dados mediante pedido individual".

Por fim, nos termos do Regulamento entende-se por organização internacional, uma organização e os organismos de direito internacional público por ela tutelados, ou outro organismo criado por acordo celebrado entre dois ou mais países ou com base num acordo dessa natureza, segundo o artigo 4.º, n.º 26.

4. Direitos dos titulares dos dados

O RGPD elenca um conjunto de direitos que são conferidos ao titular dos dados, alguns desses direitos já se encontravam consagrados na Diretiva, mas surgem novos como o direito ao apagamento dos dados e o direito à portabilidade. Importa realçar que estes direitos não são absolutos, mas sim relativos.

Transparência e regras para o exercício dos direitos

O artigo 12.º estabelece que o responsável pelo tratamento deve tomar todas as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.º e 14.º e qualquer comunicação prevista nos artigos 15.º a 22.º e 34.º a respeito do tratamento deve ser efetuado de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações forem dirigidas a crianças. As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios. [141]

O responsável pelo tratamento fornece ao titular dos dados as informações sobre as medidas tomadas, mediante o pedido apresentados pelos titulares dos dados nos termos dos artigos 15.º a 20.º, sem demora injustificada e no prazo de um mês a contar da data de receção do pedido. O prazo pode ser prorrogado até dois meses, quando for necessário, considerando a complexidade e o número de pedidos. O responsável pelo tratamento deve informar o titular

[141] Guidance Paper, Articles 14-16 of the new Regulation 45/2001: Transparency rights and obligations, European Data Protection Supervisor, p. 6-12.

dos dados de alguma prorrogação e dos motivos da demora no prazo de um mês a contar da receção do pedido. Se o pedido da informação for pedido por meios eletrónicos, a informação sempre que possível é fornecida nos mesmos meios, salvo pedido contrário do titular. Se o responsável pelo tratamento não der seguimento ao pedido apresentado ao pedido apresentado pelo titular dos dados, informando-o sem demora e, o mais tardar no prazo de um mês a contar da data de receção do pedido, das razões que o levaram a não tomar medidas e da possibilidade de apresentar reclamação a uma autoridade de controlo e intentar uma ação judicial. [142]

As informações relativas aos artigos 13.º e 14.º assim como quaisquer comunicações e medidas tomadas nos termos dos artigos 15.º a 22.º e 34.º são fornecidas a título gratuito a não ser que os pedidos sejam manifestamente infundados ou excessivos, tendo em conta o caráter repetitivo. Nesses casos, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas, ou recusar-se a dar seguimento do pedido. O responsável do tratamento é que tem que demonstrar que o pedido é excessivo ou infundado.

Informações e acesso aos dados pessoais

Quando os dados pessoais forem recolhidos junto ao titular dos dados o responsável pelo tratamento, faculta-lhe, aquando da recolha desses dados pessoais, as seguintes informações, nos temos do artigo 13.º:

a) A identidade e os contatos do responsável pelo tratamento e, se for caso disso, do seu representante;
b) Os contactos do encarregado da proteção de dados, se for caso disso;
c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
d) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro;
e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;

[142] Nesse sentido, o artigo 12 e considerando 59 do Regulamento Geral sobre a Proteção de Dados.

f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.º ou 47.º, ou no artigo 49.º, n.º 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.

Além disso, para garantir um tratamento equitativo e transparente o responsável pelo tratamento deve fornecer ao titular dos dados as seguintes informações:

a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
b) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como o direito de portabilidade dos dados;
c) Se o tratamento dos dados se basear no artigo 6.º, n.º 1 alínea a), ou o artigo 9.º, n.º 2, alínea a) a existência do direito de retirar o consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
d) O direito a apresentar uma reclamação a uma autoridade de controlo;
e) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer dados pessoais e as eventuais consequências de não fornecer esses dados;
f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n ^{os} 1 e 4 e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Quando o responsável pelo tratamento tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham

sido recolhidos, antes dessa operação de tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes.

O Regulamento preocupa-se também com as informações a facultar quando os dados pessoais não são recolhidos junto do titular de acordo com o artigo 14.º, quando esta situação se verifica, o responsável pelo tratamento fornece as seguintes informações:

a) A identidade e os contactos do responsável pelo tratamento, e se for caso disso, do seu representante;
b) Os contactos do encarregado de proteção de dados, se for caso disso;
c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
d) As categorias de dados em questão;
e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão adequada adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.º ou 47.º, ou no 49.º, n.º 1, segundo o parágrafo a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.

Para além destas informações, o responsável pelo tratamento fornece ao titular as seguintes informações, para garantir um tratamento equitativo e transparente:

a) O prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo;
b) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de terceiro;
c) A existência do direito de solicitar ao responsável pelo tratamento o acesso a dados pessoais que lhe digam respeito, e a retificação ou o apagamento, ou limitação do tratamento no que disser respeito ao titular dos dados, e do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;
d) Se o tratamento dos dados se basear no artigo 6.º, nº 1, alínea a), ou no artigo 9.º, n.º 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem

comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;

e) O direito de apresentar reclamação a uma autoridade de controlo;
f) A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público;
g) A existência de decisões automatizadas, incluindo a definição de perfis referida no artigo 22.º, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

O responsável pelo tratamento comunica as informações referidas num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês considerando as circunstâncias específicas em que estes sejam tratados. Se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados ou se estiver prevista a divulgação dos dados a outro destinatário, o mais tardar aquando da primeira divulgação dos mesmos. Além disso, obedecendo ao princípio da finalidade sempre que o responsável pelo tratamento tiver a intenção de proceder a um tratamento posterior dos dados pessoais para um fim distinto daquele pelo qual foram recolhidos, o responsável pelo tratamento antes desse tratamento deve fornecer ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes.

Estas obrigações de facultar informações ao titular dos dados não se verificam quando o titular dos dados já disponha das mesmas, sempre que se comprove a impossibilidade de disponibilizar a informação, ou que o esforço envolvido seja desproporcionado, quando o tratamento for para fins de arquivo de interesse público, para fins de investigação científica, histórica ou para fins estatísticos. Quando a obtenção de dados estiver prevista no direito da União ou do Estado-Membro ao qual o responsável pelo tratamento estiver sujeito ou quando os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada pelo direito da União ou de um Estado-Membro, incluindo uma obrigação de confidencialidade.

Direito de acesso

O direito de acesso encontra-se previsto no artigo 15.º "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". Assim, o ao titular dos dados é lhe conferido o direito a aceder aos seus dados pessoais e a determinadas informações tais como: as finalidades do tratamento; as categorias de dados pessoais em causa; os destinatários ou categorias de destinatários de a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais; se for possível o prazo previsto de conservação dos dados pessoais, ou se não for possível os critérios utilizados para a fixação desse prazo; a existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados e o direito de se opor a esse tratamento; o direito de apresentar reclamação à autoridade de controlo; se os dados não forem recolhidos junto do titular, as informações disponíveis sobre a origem desses dados; por fim, a existência de decisões automatizadas, incluindo a definição de perfis. Nestes casos, o responsável pelo tratamento deve fornecer as informações úteis relativas à logica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas nos termos do artigo 46.º.

Quando o titular dos dados exercer este direito o responsável pelo tratamento deve fornecer uma cópia dos dados pessoais que se encontrem em fase de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. Quando o pedido for apresentado por meios eletrónicos, salvo pedido em contrário do titular dos dados, a informação é fornecida em formato eletrónico.

Direito de retificação

O direito de retificação significa que o titular dos dados tem o direito de obter, sem demora justificada por parte do responsável pelo tratamento a verificação dos dados pessoais

inexatos que lhe digam respeito, tendo em consideração 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, de acordo com o artigo 16.º. [143]

Direito ao apagamento dos dados («direito a ser esquecido»)

De acordo com o artigo 17.º o titular dos dados 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 se aplique um dos seguintes motivos: os dados pessoais deixarem de ser necessários para a finalidade que motivou a sua recolha ou tratamento; o titular retire o seu consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a) ou do artigo 9.º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento; o titular opor-se ao tratamento nos termos do artigo 21.º, n.º 1, e não existirem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se nos temos do artigo 22.º, n.º 2; os dados pessoais forem tratados ilicitamente; os dados pessoais têm que ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável do tratamento está sujeito ou quando os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade de informação nos termos do artigo 8.º, n.º1. [144]

Se o responsável pelo tratamento tornar públicos os dados pessoais e for obrigado a apagá-los deve tomar medidas que forem razoáveis, incluindo de caráter técnico, tendo em conta a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como as cópias ou reproduções dos mesmos.

O direito ao apagamento dos dados («direito a ser esquecido») não se aplica quando o tratamento se demostre necessário para o exercício da liberdade de expressão e informação; no cumprimento de uma obrigação legal que exija o tratamento pelo direito da União ou de um Estado-Membro que o responsável pelo tratamento esteja sujeito, ao exercício de funções

[143] Nesse sentido, considerandos 39, 59, 65, 75 e 156 do Regulamento Geral sobre a Proteção de Dados.
[144] Nesse sentido, os considerandos 39, 59, 66, 68 e 73 do Regulamento Geral sobre a Proteção de Dados.

de interesse público ou exercício da autoridade pública de que esteja investido o responsável pelo tratamento; por motivos de interesse público no domínio de saúde pública, nos termos do artigo 9.º, n.º 2, alíneas h) e i), bem como do artigo 9.º, n.º 3; para fins de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1, na medida em que o direito de apagamento seja suscetível de tornar impossível ou prejudicar gravemente a obtenção desse tratamento ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial. [145]

Direito à limitação do tratamento

Segundo o artigo 18.º o titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento quando se verifique uma das seguintes situações: contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização; o responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial ou se tiver oposto ao tratamento nos termos do artigo 21.º, n.º 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre o titular dos dados.

Obrigação de notificação de retificação ou apagamento dos dados pessoais ou limitação do tratamento

De acordo com o artigo 19.º o responsável pelo tratamento comunica a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a que se tenha procedido em conformidade com o artigo 16.º; 17.º, n.º 1 e 18.º, a menos que a comunicação se revele impossível ou implique um esforço desproporcionado. Se o titular dos dados o solicitar, o responsável pelo tratamento fornece-lhe informações sobre os destinatários.

[145] Nesse sentido, considerando 156 do Regulamento Geral sobre a Proteção de Dados.

Direito à portabilidade dos dados

O titular dos dados tem o direito a 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, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se: o tratamento se basear no consentimento de dado nos termos do artigo 6.º, n.º1, alínea a) ou 9.º, n.º 2, alínea a) ou num contrato referido no artigo 6.º, n.º 1, alínea b) e se o tratamento for feito por meios automatizados.

O titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento sempre que seja tecnicamente possível. Este direito aplica-se sem prejuízo do direito ao apagamento dos dados («direito a ser esquecido»).

Os principais elementos da portabilidade dos dados são, designadamente um direito a receber dados, o direito à portabilidade dos dados é um direito do titular dos dados a receber um subconjunto dos dados pessoais tratados por um responsável pelo tratamento e que lhe digam respeito e armazenar os dados para um uso pessoal posterior. O tratamento pode ser realizado através de um dispositivo privado ou de uma nuvem privada, sem que haja necessariamente uma transmissão de dados para outro responsável pelo tratamento. Assim, a portabilidade complementa o direito de acesso. Outro elemento tem que ver com o direito de transmitir os dados pessoais de um responsável de tratamento para outro sem impedimentos, o considerando 68 estimula a utilização e desenvolvimento de formatos interoperáveis para facilitar o exercício destes direitos. Contudo, o RGPD não proíbe que os responsáveis pelo tratamento criem obstáculos à portabilidade. [146]

A portabilidade dos dados possibilita que os titulares reutilizem os seus dados, mas também os transmitam a outro prestador de serviços, inserido no mesmo sector empresarial ou num sector distinto. Este direito favorece a capacitação dos consumidores uma vez que evita a vinculação com o prestador, sendo que a expetativa criada em torno da portabilidade tem de ver como o facto de que esta promova oportunidades de inovação e de uma partilha segura de dados. outra possibilidade diz respeito a permissão, transmissão e reutilização dos

[146] Orientações sobre o direito à portabilidade dos dados, Grupo do Artigo 29.º para a Proteção de Dados, 16/PT, WP 242 rev. 01, p. 4-5.

dados pessoais relativos aos utilizadores entre os quais os vários serviços nos quais estejam interessados. [147]

A portabilidade assegura o controlo dos dados uma vez que garante o direito a receber os dados e de proceder ao seu tratamento consoante a vontade do titular. Contudo, salienta-se o facto de que o responsável pelo tratamento quando responde a um pedido de portabilidade não tem a obrigação específica de controlar e verificar a qualidade dos dados antes de o transmitirem, mas os dados devem estar naturalmente atualizados à luz do artigo 5.º. [148]

É importante evidenciar que o exercício do direito de portabilidade dos dados não prejudica qualquer outro direito, tal como sucede com qualquer outro direito no âmbito do Regulamento. O titular dos dados pode continuar a beneficiar dos serviços do responsável pelo tratamento após a portabilidade dos dados, a portabilidade não desencadeia automaticamente o apagamento dos dados. Assim como, se o titular dos dados exercer o direito ao apagamento dos dados, a portabilidade não pode ser utilizada pelo responsável pelo tratamento como forma de adiar ou recusar esse apagamento. [149]

A portabilidade aplica-se quando as operações de tratamento se baseiem no consentimento nos termos do artigo 6.º, n.º 1, alínea a) ou do artigo 9.º, n.º 2, alínea a) no que respeita às categorias especiais de dados pessoais ou num contrato no qual os titulares dos dados é parte nos termos do artigo 6.º, n.º 1 alínea b). A portabilidade deve incluir os dados que digam respeito ao titular dos dados e que tenham sido fornecidos pelo titular dos dados ao responsável pelo tratamento, isto é, os dados fornecidos pelo titular dos dados de forma ativa e consciente, como o nome de utilizador, morada, idade, entre outros e os dados observados fornecidos pelo titular dos dados em virtude da utilização do serviço ou do dispositivo, como o histórico das pesquisas, dados de tráfego, dados de localização, entre outros. No entanto esse direito não deve prejudicar a direitos e liberdade de terceiros nos termos do artigo 20.º, n.º 4. [150]

---

[147] Orientações sobre o direito à portabilidade dos dados, Grupo do Artigo 29.º para a Proteção de Dados, 16/PT, WP 242 rev. 01, p.5.
[148] *Idem,* p.7.
[149] Orientações sobre o direito à portabilidade dos dados, Grupo do Artigo 29.º para a Proteção de Dados, 16/PT, WP 242 rev. 01, p. 8-9.
[150] *Idem,* p. 9-16.

Relativamente ao prazo para responder a um pedido de portabilidade o artigo estipula o prazo de um mês sem demora injustificada, mas o prazo pode ser alargado até três meses nos casos mais complexos, com o conhecimento por parte do titular dos dados de quais os motivos da prorrogação. [151]

Direito de oposição

O direito de oposição tem que ver como o facto de o titular dos dados se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento de dados pessoas que lhe digam respeito com base no artigo 6.º, n.º 1, alínea e) ou f) ou no artigo 6.º, n.º 4, incluindo a definições de perfis com base nestas disposições. Quando o titular dos dados exerce este direito o responsável pelo tratamento cessa o tratamento de dados pessoais, a não ser que indique razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito processual judicial.

Relativamente aos dados que forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para efeitos da comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.

Assim como outros direitos consagrados no Regulamento deve ser exercido de forma fácil, acessível e gratuito. [152]

Decisões individuais automáticas, incluindo definições de perfis

O artigo 22.º dispõe que o titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete de uma forma significativa.

Esta disposição não se aplica se for necessária para a celebração ou execução de um contrato entre o titular dos dados e um responsável pelo tratamento, se for autorizada pelo

[151] Orientações sobre o direito à portabilidade dos dados, Grupo do Artigo 29.º para a Proteção de Dados, 16/PT, WP 242 rev. 01, p. 18.
[152] Nesse sentido, considerando 59 e 73, Regulamento Geral sobre a Proteção de Dados.

direito da União ou do Estado-Membro a que o responsável do tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas de salvaguarda dos direitos e liberdades e os legítimos interesses do titular dos dados, se for baseado no consentimento explícito do titular dos dados.

5. Obrigações gerais

Responsável pelo tratamento

O responsável pelo tratamento no que respeita a este Regulamento comporta muitas responsabilidades tendo em conta a natureza, âmbito, o contexto, as finalidades do tratamento dos dados, assim como os riscos para os direitos e liberdades das pessoas singulares, com probabilidade de erro variável, o responsável pelo tratamento deve tomar as medidas técnicas organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o Regulamento, sendo que as medidas devem ser revistas e atualizadas conforme as necessidades, de acordo como o artigo 24.º. As medidas incluem aplicação de políticas em matéria de proteção de dados para uma adequada aplicação do Regulamento. Para facilitar a aplicação e demonstração do cumprimento desta disposição legal, o responsável pelo tratamento poderá cumprir com códigos de conduta, nos termos do artigo 40.º ou através do cumprimento de processos de certificação conforme o artigo 42.º. Daqui depreende-se que o responsável pelo tratamento deve instituir mecanismos de cumprimento do Regulamento, mas também mecanismos que comprovem o esforço para cumprir este texto legal.

Proteção de dados desde a conceção e por defeito

O tratamento dos dados pessoais deve ser efetuado de uma forma adequada, as organizações devem adotar medidas técnicas e organizativas. Como já foi anteriormente referido, o responsável pelo tratamento terá de comprovar está em conformidade com as disposições do RGPD e para tal deve tomar determinadas medidas, que podem incluir a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais o mais cedo possível, a transparência no que toca às funções e ao tratamento de dados pessoais, a

possibilidade de o titular dos dados controlar o tratamento de dados e a possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança. [153]

No contexto do desenvolvimento, conceção, seleção e utilização de aplicações, serviços e produtos que se baseiam no tratamento de dados pessoais ou recorrem a este tratamento para executarem as suas funções. Haverá que incentivar os fabricantes dos produtos, serviços e aplicações a ter em conta o direito à proteção de dados quando do seu desenvolvimento e conceção e, no devido respeito pelas técnicas mais avançadas, a garantir que os responsáveis pelo tratamento e os subcontratantes estejam em condições de cumprir as suas obrigações em matéria de proteção de dados. Os princípios de proteção de dados desde a conceção e, por defeito, deverão também ser tomados em consideração no contexto dos contratos públicos.[154]

O responsável pelo tratamento aplica as medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento, obedecendo também ao princípio da minimização dos dados. Esta obrigação aplica-se à quantidade de dados recolhidos, à extensão do tratamento, ao prazo de conservação e à sua acessibilidade. Em especial, medidas que assegurem, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana de pessoas singulares. Pode ser utilizado este elemento para demonstrar o cumprimento destas obrigações um procedimento de certificação aprovado nos termos do artigo 42.º.

Responsáveis conjuntos pelo tratamento

Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis pelo tratamento. Determinam, por acordo entre si e de modo transparente as respetivas responsabilidades pelo cumprimento do Regulamento, nomeadamente no que respeita ao exercício dos direitos do titular dos dados aos respetivos deveres de fornecer as informações a facultar quando os dados são recolhidos junto do titular ou as informações a facultar quando os dados não são recolhidos junto do titular, a menos que e na medida em que as suas responsabilidades

[153] Nesse sentido, considerando 78 do Regulamento Geral sobre a Proteção de Dados.
[154] Nesse sentido, considerando 78 do Regulamento Geral sobre a Proteção de Dados.

respetivas sejam determinadas pelo direito da União ou do Estado-Membro a que estejam sujeitos. O acordo pode estabelecer um ponto de contacto para os titulares dos dados.

Representantes dos responsáveis pelo tratamento ou dos subcontratantes não estabelecidos na União

Se for aplicável o artigo 3.º, nº 2, isto é, se ocorrer o tratamento dos dados pessoais de titulares residentes no território da União for efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estão relacionadas com a oferta de bens ou serviços a esses titulares de dados na União, independente da exigência de os titulares dos dados procederem a um pagamento ou estiver relacionado com o controlo do seu comportamento, desde que esse comportamento tenha lugar na União, o responsável pelo tratamento designa por escrito um representante na União, segundo o artigo 27.º.

De fora deste artigo ficam as operações de tratamento que sejam ocasionais, não abranjam o tratamento em grande escala, de categorias especiais de dados a que se refere o artigo 9.º, n.º 1 ou o tratamento de dados pessoais relativos a condenações penais e infrações referido no artigo 10.º e não seja suscetível de implicar riscos para os direitos e liberdades das pessoas singulares, tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento e às autoridades ou organismos públicos.

O representante deve estar estabelecido num dos Estados-Membros onde se encontram os titulares dos dados cujos dados pessoais são objeto de tratamento no contexto da oferta que lhes é feita de bens ou serviços ou cujo comportamento é controlado. O representado é mandatado pelo responsável pelo tratamento ou pelo subcontratante para ser contactado em complemento ou em substituição do responsável pelo tratamento ou do subcontratante, em especial por autoridades de controlo e por titulares, relativamente a todas as questões relacionadas com o tratamento. A designação de um representante não prejudica as ações judiciais que podem vir a ser intentadas contra o próprio subcontratante.

Subcontratante

Quando o tratamento dos dados for efetuado por sua conta do subcontratante, o responsável pelo tratamento recorre a medidas técnicas e organizativas adequadas de uma

forma a que o tratamento transfronteiriço satisfaça os requisitos do RGPD e que assegure a defesa dos direitos do titular dos dados.

Assim, o subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado previamente e por escrito, autorização específica ou geral. Em caso de uma autorização geral por escrito, o subcontratante informa o responsável pelo tratamento de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratantes, dando assim ao responsável pelo tratamento a oportunidade de se opor a tais alterações. O objetivo desta disposição é elaborar uma cadeia de responsabilidades e mapear o fluxo dos dados do titular.

Nos termos do artigo 28.º, n. 3 o tratamento em subcontratação é regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros que vincule o subcontratante ao responsável pelo tratamento onde se estabeleça o objeto e a duração do tratamento, a natureza, a finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados e as obrigações e direitos do responsável pelo tratamento. Nesse contrato ou ato normativo estipula-se que o subcontratante:

a) Trata os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso o responsável pelo tratamento desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;
b) Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;
c) Adota todas as medidas exigidas nos termos do artigo 32.º;
d) Respeita as condições a que se referem os n.ºs 2 e 4 para contratar outro subcontratante;
e) Toma em conta a natureza do tratamento, e na medida do possível, presta assistência ao responsável pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos previstos no capítulo III;

f) Presta assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32.º a 36.º, tendo em conta a natureza do tratamento e a informação ao dispor do subcontratante;
g) Consoante a escolha do responsável pelo tratamento, apaga ou devolve-lhe todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros;
h) Disponibiliza ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no presente artigo e facilita e contribui para as auditorias, inclusive as inspeções, conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado.

No que diz respeito ao primeiro parágrafo, alínea h), o subcontratante informa imediatamente o responsável pelo tratamento se, no seu entender, alguma instrução violar o presente Regulamento ou outras disposições do direito da União ou dos Estados-Membros em matéria de proteção de dados.

Caso o subcontratante contratar outro subcontratante para realizar operações específicas de tratamento de dados por conta do responsável do tratamento, são impostas a esse outro subcontratante, por contrato ou outro ato normativo ao abrigo da União ou dos Estados-Membros, as mesmas obrigações em matéria de proteção de dados estabelecidas no contrato ou ato normativo entre o responsável pelo tratamento e o subcontratante, em particular as garantias suficientes de execução de medidas técnicas e organizativas adequadas de forma que o tratamento seja conforme com os requisitos do Regulamento. Se o outro subcontratante não cumprir com as suas obrigações em matéria de proteção de dados, o subcontratante inicial continua a ser plenamente responsável pelo tratamento, pelo cumprimento das obrigações desse subcontratante.

O subcontratante para demonstrar garantias suficientes pode cumprir o código de conduta do artigo 40.º ou através de um procedimento de certificação aprovado no artigo 42.º.

Tratamento sob a autoridade do responsável pelo tratamento ou subcontratante

O subcontratante ou qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou subcontratante tenha acesso a dados pessoais, não procede ao tratamento desses dados exceto por instrução do responsável pelo tratamento, salvo se a tal for obrigado por força do direito da União ou dos Estados-Membros.

Registos da atividade de tratamento

De acordo com o artigo 30.º, cada responsável pelo tratamento e, sendo caso disso, o seu representante conserva um registo de todas as atividades de tratamento sob a sua responsabilidade. Desse registo devem constar as seguintes informações:

a) O nome e os contactos do responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados;
b) As finalidades do tratamento dos dados;
c) A descrição das categorias de titulares de dados e das categorias de dados pessoais;
d) As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais;
e) Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49.o, n.º 1, segundo parágrafo, a documentação que comprove a existência das garantias adequadas;
f) Se possível, os prazos previstos para o apagamento das diferentes categorias de dados;
g) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.o, n.º 1.

Cada subcontratante e, sendo caso disso, o representante deste, conserva um registo de todas as categorias de atividades de tratamento realizadas em nome de um responsável pelo tratamento do qual constará:

a) O nome e contactos do subcontratante ou subcontratantes e de cada responsável pelo tratamento em nome do qual o subcontratante atua, bem como, sendo caso disso do representante do responsável pelo tratamento ou do subcontratante e do encarregado da proteção de dados;
b) As categorias de tratamentos de dados pessoais efetuados em nome de cada responsável pelo tratamento;
c) Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49.o, n.º 1, segundo parágrafo, a documentação que comprove a existência das garantias adequadas;
d) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.º, n.º 1. 3. Os registos a que se referem os n.ºs 1 e 2 são efetuados por escrito, incluindo em formato eletrónico. 4. O responsável pelo tratamento e, sendo caso disso, o subcontratante, o representante do responsável pelo tratamento ou do subcontratante, disponibilizam, a pedido, o registo à autoridade de controlo.

Cooperação com a autoridade de controlo

O responsável pelo tratamento e o subcontratante e, sendo caso disso, os seus representantes cooperam com a autoridade de controlo quando solicitados por esta, na prossecução das atribuições desta.

Avaliação de impacto sobre a proteção de dados

Com o intuito de promover o cumprimento do presente Regulamento nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para

determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco.[155]

A avaliação de impacto sobre a proteção de dados, doravante AIPD é um processo criado para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e auxiliar na gestão de riscos para os direitos e liberdades das pessoas singulares que resultam de uma operação de tratamento de dados pessoais, avaliando-os e determinando as medidas técnicas e organizativas para face a esses riscos. Constitui um instrumento importante em matéria de responsabilização uma vez que não só auxilia no cumprimento do Regulamento, mas também a demonstrar que foram tomadas todas as medidas adequadas para o cumprir. De acordo com o considerando 84 "os resultados da avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento está em conformidade com o presente regulamento". Assim, uma AIPD é um processo que visa estabelecer e demonstrar conformidade. [156]

Nos termos do RGPD a não conformidade com os requisitos de uma AIPD pode conduzir à imposição de coimas pela autoridade de controlo competente nos casos em que não se realize uma AIPD quando o tratamento está sujeito a uma nos termos do artigo 35.º, n.º 1 e nºs 3 e 4, realize-se uma AIPD incorreta, nos termos do artigo 35.º n.º 2 e n.ºs 7 a 9 ou não consultar uma autoridade de controlo competente quando necessária nos termos do artigo 36.º, nº 3 alínea e).[157]

Em consonância com a abordagem baseada no risco incorporada no Regulamento não é necessário realizar uma AIPD para todas as operações de tratamento, só existe a obrigação de realizar uma AIPD quando o tratamento for suscetível de implicar um elevado risco para os direitos liberdades das pessoas singulares, segundo o artigo 35.º, n.º 1. [158]

O RGPD impõe que os responsáveis pelo tratamento apliquem medidas para assegurar a sua conformidade, tendo em conta, entre outros, os riscos para os direitos liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, de

[155] Nesse sentido, considerando 84 do Regulamento Geral sobre a Proteção de Dados.
[156] Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Grupo de Artigo 29.º para a Proteção de Dados, 17/PT, WP 248, rev. 01, p. 4.
[157] *Idem,* p. 5.
[158] Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Grupo de Artigo 29.º para a Proteção de Dados, 17/PT, WP 248, rev. 01, p. 5.

acordo com o artigo 24.º. Assim, a obrigação de realização de uma AIPD recai sobre os responsáveis pelo tratamento em determinadas circunstâncias não deve ser entendida com no contexto de uma obrigação geral de fazer uma gestão adequada dos riscos do tratamento dos dados pessoais. Sendo que os riscos têm de ser identificados, analisados, estimados, avaliados, tratados e revistos regularmente. Os responsáveis pelo tratamento não podem fugir à responsabilidade, cobrindo os riscos com apólices de seguro. Um risco é um cenário que descreve um acontecimento e as respetivas consequências, estimando em termos de gravidade e probabilidade. A gestão do risco pode ser definida como as atividades coordenadas que visam direcionar e controlar uma organização no que toca ao risco. [159]

Relativamente à definição do que é suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, segundo o Grupo de Artigo 29.º diz respeito aos direitos de proteção de dados e privacidade, mas abrange outros direitos fundamentais como a liberdade de expressão, a liberdade pensamento, a liberdade de circulação, a proibição de discriminação, o direito à liberdade, consciência e religião. [160]

A AIPD pode dizer respeito a uma única de operação de tratamento de dados, no entanto, o artigo 35.º, n.º 1 esclarece que se um conjunto de operações de tratamento apresentar riscos elevados pode ser analisado numa única operação. O considerando 92 auxilia neste entendimento uma vez que dispõe que em certas circunstâncias pode ser razoável e económico alargar a avaliação de impacto sobre a proteção de dados para além de um projeto único, por exemplo se as autoridades ou organismos públicos pretendem criar uma aplicação ou uma plataforma de tratamento comum, ou se vários responsáveis pelo tratamento planearam criar uma aplicação ou ambiente de tratamento comum em todo setor ou segmento profissional, ou uma atividade horizontal amplamente utilizada. [161]

Desta forma, uma única AIPD pode ser utilizada para avaliar múltiplas operações de tratamento sejam semelhantes, em termos de âmbito, contexto, finalidades e riscos. As AIPD visam estudar sistematicamente as novas situações que possam ser suscetíveis de implicar

[159] Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Grupo de Artigo 29.º para a Proteção de Dados, 17/PT, WP 248, rev. 01, p. 7.
[160] *Ibidem.*
[161] Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Grupo de Artigo 29.º para a Proteção de Dados, 17/PT, WP 248, rev. 01, p. 8.

riscos elevados para os direitos e as liberdades das pessoas singulares, não existindo necessidade de realizar uma AIPD para casos já estudados. [162]

Nos casos em que a operação de tratamento envolve responsáveis pelo tratamento, este devem definir pormenorizadamente as obrigações. A AIPD deve definir qual das partes é responsável pelas várias medidas concebidas para dar resposta aos riscos e proteger os direitos e as liberdades dos titulares dos dados. Assim, cada responsável pelo tratamento deverá revelar quais as suas necessidades e partilhar informações úteis sem comprometer segredos ou revelar vulnerabilidades. [163]

A realização de uma AIPD é somente obrigatória quando o tratamento for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, segundo o artigo 35.º, n.º 1, artigo 35.º, n.º 3 e 4. Nos casos em que não é claro se se a realização de uma AIPD é necessária, o Grupo de Artigo 29.º recomenda que esta se realize uma vez que constitui um instrumento útil para auxiliar os responsáveis pelo tratamento a cumprir a legislação de proteção de dados. [164]

O artigo 35.º, n.º 3 prevê alguns exemplos de quando uma operação de tratamento é suscetível de implicar elevados riscos:

a) Avaliação sistemática e completa dos aspetos pessoais relacionados com as pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º;
c) Controlo sistemático de zonas acessíveis ao público em grande escala.

[162] Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Grupo de Artigo 29.º para a Proteção de Dados, 17/PT, WP 248, rev. 01, p p. 9.
[163] Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Grupo de Artigo 29.º para a Proteção de Dados, 17/PT, WP 248, rev. 01, p. 9.
[164] *Idem,* p. 9-10

A lista que consta neste artigo não é exaustiva podem existir operações de elevado risco que não estão incluídas nesta lista, mas que ainda assim impliquem riscos e, portanto, devem estar sujeitas a uma AIPD.[165]

O Grupo de Artigo 29.º com vista a fornecer um conjunto mais concreto de operações de tratamento que exija uma AIPD devido ao elevado risco inerente, considerando os elementos do artigo 35.º, n.º 1, nº 3, alíneas a) a c), a lista a considerar no artigo 35.º, nº 4 e os considerandos 71, 75 e 91 devem ser considerados nove critérios: [166]

1. Avaliação ou classificação, aqui inclui-se a definição de perfis e previsão, em especial "aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados".
2. Decisões automatizadas que produzam efeitos jurídicos que afetem significativamente de modo similar o tratamento destinado à tomada de decisões sobre os titulares dos dados e que introduza efeitos jurídicos relativamente à pessoa singular ou que a afetem de forma significativa de forma similar, de acordo com o artigo 35.º, n.º 3, alínea a).
3. Controlo sistemático, isto é, o tratamento utilizado para observar, monitorizar ou controlar os titulares dos dados, abrangendo os dados recolhidos através das redes, o um "controlo sistemático de zonas acessíveis ao público, segundo o artigo 35.º, n.º 3, alínea c). Este controlo é um critério porque os dados pessoais podem ser recolhidos em circunstâncias em que os titulares dos dados podem não estar cientes de quem está a recolher os dados e de que forma é que os seus dados estão a ser utilizados.
4. Dados sensíveis ou dados de natureza altamente pessoal, este critério inclui as categorias especiais de dados pessoais definidas no artigo 9.º, os dados pessoais relacionados com as condenações penais e infrações definidas no artigo 10.º.
5. Dados tratados em larga escala, o Regulamento não define grande escala, no entanto o considerando 91 auxilia o entendimento nesta matéria e o Grupo Artigo 29.º recomenda que determinados fatores sejam considerados, tais como: o número de titulares de dados envolvidos, quer em número específico quer através de uma percentagem da

[165] Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Grupo de Artigo 29.º para a Proteção de Dados, 17/PT, WP 248, rev. 01, p. 9-10.
[166] *Idem,* p. 10-14.

população pertinente; o volume de dados ou a sua diversidade de dados diferentes a tratar; a duração da atividade de tratamento de dados ou a sua pertinência e a dimensão geográfica da atividade de tratamento.

6. Estabelecer correspondências ou combinar conjuntos de dados, como a origem em duas ou mais operações de tratamento de dados realizadas com diferentes finalidades e/ou por diferentes responsáveis pelo tratamento de dados de tal forma a que excedam as expetativas razoáveis do titular dos dados.
7. Os dados relativos a titulares de dados vulneráveis, o tratamento deste tipo de dado constitui um critério devido ao acentuado desequilíbrio de poder entre os titulares dos dados e o responsável pelo tratamento dos dados, isto é, os indivíduos podem ser capazes de consentir, ou opor-se, facilmente ao tratamento dos seus dados ou de exercer os seus direitos. Os titulares de dados vulneráveis podem incluir crianças, que podem ser consideradas incapazes de consentir ou opor-se consciente e criteriosamente ao tratamento dos seus dados), empregados, segmentos mais vulneráveis da população que necessitem de proteção especial, tais como, pessoas com doenças mentais, requerentes de asilo, idosos, doentes, entre outros e todos os casos em que possa ser identificado um desequilíbrio na relação entre a posição do titular dos dados e o responsável pelo tratamento.
8. Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais, tais como combinar a utilização de impressão digital e do reconhecimento facial para melhorar o controlo de acesso físico, etc. O Regulamento esclarece no seu artigo 35.º, n.º 1 e nos considerandos 89 e 91 que a utilização de uma nova tecnologia definida em conformidade com os níveis de conhecimento tecnológicos alcançados pode desencadear a necessidade de uma AIPD. Essa necessidade porque a utilização de dados, possivelmente com elevado risco para os direitos e as liberdades dos indivíduos. As consequências pessoais da aplicação da implementação de uma nova tecnologia podem ser totalmente desconhecidas, como tal, a realização de uma AIPD auxiliará o responsável pelo tratamento de dados a compreender e dar resposta a esses riscos.
9. Quando o tratamento impede os titulares dos dados "de exercer um direito ou de utilizar um serviço ou um contrato", segundo o artigo 22.º e o considerando 91. Neste caso,

estão incluídas operações de tratamento destinadas a autorizar, alterar ou recusar o acesso dos titulares dos dados a um serviço ou que estes celebrem um contrato.

O responsável pelo tratamento de dados pode considerar que um tratamento que satisfaça dois critérios exige a realização de uma AIPD. O Grupo do Artigo 29.º considera que quanto mais critérios forem satisfeitos pelo tratamento maior é a probabilidade de este implicar um elevado risco para os direitos e as liberdades dos titulares dos dados e, portanto, verificar-se a necessidade de realização e uma AIPD. [167]

No caso de se verificar uma operação de tratamento conforme os casos mencionados e o responsável pelo tratamento considerar que a operação não é suscetível de implicar um elevado risco, o responsável pelo tratamento deve justificar e documentar as razões que o conduziram a não realizar uma AIPD e incluir ou registar os pontos de vista do encarregado de proteção de dados. [168]

As autoridades de controlo devem elaborar uma lista pública das operações de tratamento sujeitas a uma AIPD e devem comunicar a lista ao Comité Europeu da Proteção de Dados (CEPD), de acordo com o artigo 35.º, nº 4.

Relativamente aos casos em que o Grupo do Artigo 29.º não considera obrigatória uma AIPD são os seguintes:[169]

1. Quando o tratamento não for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, segundo o artigo 35.º, nº 1;
2. Quando a natureza, o âmbito, o contexto e as finalidades do tratamento forem muito semelhantes ao tratamento em relação ao qual tenha sido realizada uma AIPD. Nestes casos, podem ser utilizados os resultados da AIPD realizada para o tratamento semelhante, de acordo com o artigo 35.º, nº 1;

[167] Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Grupo de Artigo 29.º para a Proteção de Dados, 17/PT, WP 248, rev. 01, p. 14.
[168] Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Grupo de Artigo 29.º para a Proteção de Dados, 17/PT, WP 248, rev. 01, p. 14-15.
[169] *Idem.*

3. Quando as operações de tratamento tiverem sido previamente controladas por uma autoridade de controlo antes de maio de 2018 em condições específicas que não se tenham alterado, de acordo com o considerando 171;
4. Quando uma operação de tratamento, nos termos do artigo 6.º, nº 1, alíneas c) ou e), tiver um fundamento jurídico no direito da UE ou de um Estado-Membro, em que o direito regule as operações de tratamento específica e em que a AIPD já tenha sido realizada como parte da adoção desse fundamento jurídico, segundo o artigo 35.º, nº 10, salvo se o Estado-Membro considerar necessário proceder a essa avaliação antes das atividades de tratamento;
5. Quando o tratamento estiver incluído na lista operacional de tratamento, definida pela Autoridade de Controlo, para as quais não é obrigatória uma AIPD, nos termos do artigo 35.º, nº 5. A lista definida pelo Autoridade de Controlo pode conter atividades de tratamento que satisfazem as condições especificas por esta autoridade, em especial através de orientações, decisões ou autorizações específicas, regras de conformidade, entre outros. Nestes casos e sujeitos a uma reavaliação pela autoridade de controlo competente, não é obrigatório realizar uma AIPD, mas somente se o tratamento enquadrar estritamente no âmbito do procedimento pertinente mencionado na lista e continuar a estar totalmente em conformidade com todos os requisitos pertinentes do Regulamento.

Quanto às operações de tratamento existentes suscetíveis de implicar um elevado risco para direitos, liberdades e garantias das pessoas singulares em relação às quais não tenha havido alteração dos riscos, tendo em conta a natureza, o âmbito, contexto e as finalidades de tratamento existe a obrigação de realizar uma AIPD. No entanto, não existe necessidade de realizar uma AIPD para as operações de tratamento que tenham sido controladas por uma autoridade de controlo ou pelo encarregado da proteção de dados. Outra preocupação que se deve ter em relação à AIPD refere-se ao facto que uma vez realizada esta deve ser continuamente revista e regularmente avaliada. [170]

[170] Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, Grupo de Artigo 29.º para a Proteção de Dados, 17/PT, WP 248, rev. 01, p. 15-16.

6. Tratamento de dados pessoais de crianças

Uma criança deve usufruir de todos os direitos, incluindo o direito à proteção de dados. Contudo, a criança está em situação especial devendo ser considerada em duas perspetivas: a estática e a dinâmica.

Do ponto de vista estático, a criança é uma pessoa que ainda não alcançou a maturidade física e psicológica. Do ponto de vista dinâmico, encontra-se num processo de desenvolvimento físico e mental que a levará a tornar-se num adulto. Os direitos da criança e o exercício desses direitos devem ser expressos de forma a que reconheça ambas as perspetivas, incluindo o direito à proteção de dados.

No âmbito dos direitos da criança existem alguns princípios fundamentais que o Grupo do Artigo 29.º que se mostram relevantes. Os princípios fundamentais em geral são: [171]

a) O interesse superior da criança

O princípio jurídico essencial é o interesse superior da criança consagrado na Convenção das Nações Unidas sobre os Direitos da Criança no artigo 3.º e, mais tarde na Convenção 192 do Conselho da Europa no artigo 6.º e na Carta dos Direitos Fundamentais da União Europeia no artigo 4.º, n.º 2. A este princípio está subjacente a ideia de a pessoa ainda não atingiu a maturidade física e psicológica, portanto precisa de mais proteção que as restantes. Este princípio visa melhorar as condições das crianças e reforçar o direito ao desenvolvimento da personalidade, deve ser respeitado por todas as entidades privadas ou públicas que tomam decisões acerca das crianças. Nesse sentido, aplicam-se também aos pais e a outros representantes legais de crianças, quando os respetivos interesses estão em conflito ou quando a criança esteja a ser representada.

b) Proteção e cuidados necessários ao bem-estar da criança

O princípio do interesse superior requer que a posição da criança seja tida em devida conta, o que implica que se reconheça dois aspetos, o primeiro é a imaturidade das crianças torna-a vulnerável, o que deve ser compensado pela proteção e cuidados adequados. O segundo é o direito da criança ao desenvolvimento só pode ser devidamente exercido com a assistência ou a proteção de outras entidades ou pessoas. Essa proteção está a cargo da

[171] Parecer n. 2/2009 sobre a proteção dos dados pessoais das crianças (Orientações gerais e situações especiais das escolas), Grupo do Artigo 29.º para a Proteção dos Dados, 398/09/PT, WP 160, p. 4-7.

família, da sociedade e do Estado. No sentido de assegurar às crianças os seus dados pessoais devem ser amplamente tratados e por diversas partes. O tratamento amplo dos dados pessoais verifica-se em vários domínios relativos ao bem-estar como a educação, a segurança social, entre outros. Esta partilha pode afetar o princípio da finalidade e criar um risco de que os perfis sejam construídos sem respeitar o princípio da proporcionalidade.

c) Direito à privacidade

As crianças, como seres humanos tem direito ao respeito pela sua privacidade. Nenhuma criança pode ser sujeita a intromissões arbitrárias ou ilegais na sua vida privada, na sua família, na sua correspondência, nem ofensas ilegais à sua honra ou reputação, segundo o artigo 16.º da Convenção das Nações Unidas sobre os Direitos da Criança. O direito à privacidade da criança deve ser respeitado por todos, incluindo os responsáveis legais da criança.

d) Representação

As crianças para exercer a maioria dos seus direitos necessitam de representação jurídica. No entanto, o representante legal da criança não tem qualquer superioridade absoluta ou incondicional sobre a criança, uma vez que o interesse superior da criança pode conferir-lhe direitos relativos à proteção dos dados que se podem sobrepor aos desejos dos pais ou dos representantes legais. Outro aspeto que deve ser tido em conta é que apesar da necessidade de representação jurídica também não implica que a partir de determinada idade, as crianças possam ser consultadas quanto a questões que lhes digam respeito.

Se o consentimento de uma criança for prestado pelo seu representante legal, a criança pode quando atingir a maioridade, revogar o consentimento, mas se desejar que o tratamento continue, o titular dos dados pode dar o seu consentimento explícito, sempre que este seja necessário. O direito à proteção de dados pertence à criança e não aos seus representantes legais que apenas os exercem em nome destas.

e) Interesses concorrentes: a privacidade e o interesse superior da criança

O interesse superior da criança pode ter uma dupla função, nomeadamente exigir que a privacidade das crianças seja o melhor possível protegida possível para que o direito de proteção de dados seja o mais efetivo possível. No entanto, podem ocorrer situações em que o interesse superior da criança e o seu direito da privacidade estejam em conflito. Nos casos

em que esses dois interesses concorram entre si, o direito de proteção de dados deve ceder em relação ao princípio do interesse superior.

f) Adaptação ao grau de maturidade da criança

Uma criança ainda não atingiu a maturidade necessária, está em fase de desenvolvimento, nomeadamente no exercício dos seus direitos, inclusive os direitos da proteção de dados devendo adaptar-se ao seu nível de desenvolvimento físico e psicológico. As crianças encontram-se em desenvolvimento e tem direito ao mesmo e a forma como este desenvolvimento é gerido difere de Estado para Estado, mas as crianças devem ser tratadas de acordo com o seu nível de maturidade.

g) Direito à participação

As crianças à medida que vão crescendo tornam-se gradualmente capazes de contribuir para as decisões tomadas sobre a sua vida e como tal, à medida que crescem deve participar com regularidade no exercício de direitos, incluindo o direito à proteção de dados.

O primeiro grau ou nível do direito à participação é o direito a ser consultado. Este direito consiste em ter em consideração a opinião, mas não se fica vinculado à mesma. À medida que as crianças vão crescendo a participação tende a aumentar, sendo que a decisão pode ser tomada em conjunto ou de forma autónoma. Na proteção de dados esse direito pode estar presente em assuntos como a geolocalização ou na utilização de imagens. [172]

A Diretiva 95/45/CE e a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) não fazem uma menção explícita do direito da privacidade dos menores, ao contrário do que acontece com o RGPD. [173]

O Grupo de Artigo 29.º no seu parecer sobre a proteção dos dados pessoais das crianças refere os dados pessoais das crianças no contexto escolar. As escolas ou instituições equivalentes possuem ficheiros dos alunos que contêm inúmeras informações sobre os mesmos, a relação com instituições de ensino normalmente inicia-se com o preenchimento de formulários, onde o Grupo de Artigo 29.º recomendava no parecer de 2009 que os

[172] Parecer n. 2/2009 sobre a proteção dos dados pessoais das crianças (Orientações gerais e situações especiais das escolas), Grupo do Artigo 29.º para a Proteção dos Dados, 398/09/PT, WP 160, p. 11.
[173] *Idem.*

interessados deveriam ser informados de que os seus dados pessoais são recolhidos e tratados, qual o objetivo, quem são os responsáveis pelo tratamento dos dados e como podem exercer os direitos de acesso e retificação. Se os dados fossem divulgados a terceiros deveriam informar os titulares dos mesmos. Aqui, fica bastante latente o dever de informação que o responsável pelo tratamento tem em relação a titular dos dados, tal e plasmado no RGPD. [174]

O Grupo Artigo 29.º advertia que nos ficheiros dos alunos só poderá incluir informações necessárias para os objetivos legítimos prosseguidos pelas escolas e não devem ser utilizados de forma incompatível com esses objetivos. Os dados exigidos não devem ser excessivos como graus académicos dos pais, profissão ou situação laboral. Neste ponto, fica plasmado os princípios da finalidade e da proporcionalidade que se o RGPD também adota. [175]

Os dados pessoais recolhidos não devem colocar em causa discriminações tais como dados relativos, à raça, estatuto de emigrante ou certas incapacidades. [176]

Os dados recolhidos devem atender ao princípio da finalidade, isto é, não devem ser utilizados para fins de *marketing*. [177]

Os dados contidos nos ficheiros dos alunos devem estar sujeitos a uma rigorosa confidencialidade, onde fica plasmado a necessidade de restringir o acesso aos dados. Os dados de natureza especial devem estar sujeitos a requisitos de segurança, tais como os dados referentes a: processos disciplinares; registos de casos de violência; tratamentos médicos na escola; orientação escolar; ensino especial para pessoas com deficiência e alunos pobres. [178]

Os dados só devem ser mantidos durante o tempo estritamente necessários ao objetivo para que foram recolhidos. No contexto educacional deve-se avaliar cuidadosamente quais os dados dos ficheiros escolares que devem ser suprimidos, nomeadamente os dados a que se referem os processos ou sanções profissionais. [179]

No âmbito escolar e educacional as questões de proteção de dados podem colocar-se em algumas dimensões, nomeadamente quantos as escolas socorrem-se de sistemas de

---

[174] Parecer n. 2/2009 sobre a proteção dos dados pessoais das crianças (Orientações gerais e situações especiais das escolas), Grupo do Artigo 29.º para a Proteção dos Dados, 398/09/PT, WP 160, p. 12.
[175] *Idem,* p. 13.
[176] *Ibidem.*
[177] *Idem,* p. 14.
[178] Parecer n. 2/2009 sobre a proteção dos dados pessoais das crianças (Orientações gerais e situações especiais das escolas), Grupo do Artigo 29.º para a Proteção dos Dados, 398/09/PT, WP 160, p. 15.
[179] *Idem,* p. 16.

televisão em circuito fechado por motivos de segurança. As instituições de ensino quando utilizam estes sistemas de vigilância que afetam as liberdades individuais tem que atender a certos cuidados no momento da instalação o que significa que as instituições só devem recorrer a estes métodos quando sejam necessários e quando não estejam disponíveis outros meios menos invasivos e que possibilitem alcançar o mesmo objetivo. [180]

Os dados de saúde dos alunos são dados sensíveis e os dados médicos só devem ser tratados por médicos ou por quem diretamente responsável por cuidar dos alunos, os professores e outro pessoal escolar vinculado pelo sigilo profissional. [181]

Relativamente às fotografias das crianças em âmbito escola é cada vez mais frequente a publicação de fotografias dos alunos na internet. Nestes casos, deve-se proceder a uma avaliação sobre o tipo de fotografias, a importância e objetivo da publicação. Sempre que uma fotografia seja publicada as crianças e os representantes legais devem ser informados. Quando as fotografias são individuais deve se obter o consentimento prévio dos legais da criança ou da criança dependendo da sua maturidade. [182]

O tratamento de dados pessoais é altamente considerado pelo Regulamento considerando que são um grupo que merecem proteção especial quanto ao tratamento dos seus dados considerando que podem estar menos cientes dos riscos, consequências e garantias em questão e dos direitos relacionados com o tratamento dos dados pessoais. Esta proteção deverá aplicar-se à utilização de dados pessoais de crianças para efeitos de comercialização ou criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança. Relativamente, ao princípio de transparência do tratamento as crianças merecem proteção específica, logo sempre que o tratamento lhes seja dirigido qualquer informação e comunicação deverá ser redigida numa linguagem clara e simples, em conformidade com o disposto no artigo 12.º. [183]

---

[180] Parecer n. 2/2009 sobre a proteção dos dados pessoais das crianças (Orientações gerais e situações especiais das escolas), Grupo do Artigo 29.º para a Proteção dos Dados, 398/09/PT, WP 160, p. 16.
[181] *Idem,* p. 18.
[182] *Ibidem.*
[183] Nesse sentido, considerando 38 do Regulamento Geral sobre a Proteção dos Dados.

O artigo 8.º prevê as condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade de informação, ou seja, quando se aplique o consentimento como forma de tratamento lícito dos dados pessoais e este seja recolhido no âmbito de uma oferta direta dos serviços da sociedade de informação, os dados pessoais só poderão ser objeto de tratamento quando estas tenham pelo menos 16 anos. Caso contrário, o tratamento só será lícito quando o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança. Os Estados-Membros podem dispor do direito uma idade inferior para os efeitos referidos, desde que esta não seja inferior aos 13 anos. O responsável pelo tratamento empenha todos os esforços adequados para verificar que o consentimento foi dado pelo titular das responsabilidades parentais da criança, tendo em consideração a tecnologia disponível.

7. Encarregado da Proteção de Dados

A figura do Encarregado de Proteção de Dados (EPD) era defendida pelo Grupo Artigo 29.º antes da adoção do Regulamento Geral sobre a Proteção de Dados. O RGPD determina que determinados responsáveis pelo tratamento e subcontratantes devem obrigatoriamente designar um Encarregado de Proteção de Dados. Essa obrigatoriedade aplica-se a todas as autoridades e organismos públicos, independentemente dos dados que tratam e de outras organizações cuja atividade principal consista no controlo de pessoas de forma sistemática e em grande escala, ou que tratam categorias especiais de dados em larga escala [184]

O EPD tem como principais funções serem intermediários entre as partes interessadas quer sejam as autoridades de controlo, os titulares de dados e as unidades empresarias dentro da organização. Contudo, o EPD não é pessoalmente responsável pelo incumprimento do Regulamento Geral sobre a Proteção de Dados, o artigo 24.º, n. 1 explicita claramente que compete ao responsável pelo tratamento ou ao subcontratante assegurar e comprovar que o tratamento dos dados é realizado de forma lícita. O EPD tem um papel importante no novo sistema de governação de dados exposto pelo RGPD, que estabelece as condições de aplicação, nomeação, posição e atribuição.

[184] Orientações para sobre os encarregados da proteção dos dados (EPD), Grupo do Artigo 29.º para a Proteção de Dados, 16/PT, WP 243 rev. 01, p. 5.

Assim, a designação do EPD é obrigatória em três situações, de acordo com o artigo 37.º, n.º 1:

a) Sempre que o tratamento seja efetuado por uma autoridade ou um organismo público;
b) Sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou
c) Sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados (conforme o artigo 9.º) ou de dados pessoais relacionados com condenações penais e infrações (conforme o artigo 10.º).

Nas situações em que a organização nomeie um EDP e que legalmente não o seja obrigada a fazê-lo, isto é, quando a nomeação é feita a título voluntário, os requisitos impostos no âmbito da nomeação que se encontram plasmados nos artigos 37.º a 38.º são aplicáveis à sua nomeação, posição e atribuições aplicam-se como se a nomeação fosse obrigatória.

O entendimento de "autoridade e organismo público" tem muito que ver com a legislação nacional de cada Estado-Membro. No entanto, pode-se incluir neste conceito as autoridades nacionais, regionais, e locais, mas o seu conceito, por norma abrange um conjunto de outros organismos de direito público. O desempenho de funções de serviço público e o exercício de autoridade pública podem pertencer as pessoas singulares ou coletivas de direito público ou privado, nomeadamente em setores como os transportes públicos, o abastecimento de água ou energia, infraestruturas rodoviárias, a radiodifusão de serviço público, a habitação pública ou órgãos disciplinares de profissões regulamentadas, consoante a legislação de cada Estado-Membro. [185]

Já no que refere ao significado de "atividades principais" tem que ver como as operações essenciais para alcançar objetivos do responsável pelo tratamento ou do subcontratante, onde se insere as atividades de tratamento de dados possuiu uma parte

[185] Orientações para sobre os encarregados da proteção dos dados (EPD), Grupo do Artigo 29.º para a Proteção de Dados, 16/PT, WP 243 rev. 01, p. 7.

indissociável das atividades do responsável pelo tratamento ou do subcontratante, esta interpretação é realizada em consonância com o artigo 37.º, n.º 1 alíneas b) e c). [186]

O conceito de grande escala deve ter em consideração um conjunto de fatores, designadamente o número de titulares de dados afetados; o volume de dados e/ou alcance dos diferentes elementos de dados objetos de tratamento; a duração, pertinência da atividade de tratamento de dados; o âmbito geográfico da atividade de tratamento. [187]

No caso do "controlo regular e sistemático" inclui todas as formas de seguimento e de definição de perfis na internet para fins de publicidade comportamental, mas este conceito não se limita ao ambiente em linha. O Grupo Artigo 29.º entende que "regular" significa que o tratamento inclui as seguintes caraterísticas: o tratamento é contínuo ou que ocorre em intervalos específicos num determinado período, o tratamento é recorrente ou repetido em horários estipulados ou constante ou periódico. Já que no que refere à interpretação de sistemático o tratamento deve conter as seguintes caraterísticas: o tratamento de ocorre de acordo com um determinado sistema, deve ser predefinido, organizado ou metódico, realizado no âmbito de um plano geral de recolha de dados e efetuado no âmbito de uma estratégia. [188]

Quanto à designação de um EPD, um grupo empresarial pode designar um único EPD desde que este seja de fácil acesso a partir de cada estabelecimento. A acessibilidade tem que ver com o facto de este estabelecer facilmente contacto com o titular dos dados e à autoridade de controlo. A acessibilidade tem de se verificar caso o EPD nomeado seja interno ou externo à organização, acessibilidade de comunicação tem que cumprir o requisito da língua, isto é, as comunicações devem ser realizadas na língua ou nas línguas utilizadas pela autoridade de controlo e pelos titulares dos dados em causa. O EPD deve possuir um canal de comunicação direto para que este esteja sempre disponível para possíveis contactos dos titulares dos dados. [189]

Quanto à localização o EPD deve estar dentro da União Europeia, independentemente de o responsável pelo tratamento ou o subcontratante estar ou não estabelecido na União

[186]Orientações para sobre os encarregados da proteção dos dados (EPD), Grupo do Artigo 29.º para a Proteção de Dados, 16/PT, WP 243 rev. 01, p. 23.
[187]*Idem,* p. 24.
[188]Orientações para sobre os encarregados da proteção dos dados (EPD), Grupo do Artigo 29.º para a Proteção de Dados, 16/PT, WP 243 rev. 01, p. 24-25.
[189]*Idem,* p. 25.

Europeia para que possa exercer as suas funções de um modo mais eficaz. No entanto, este pode exercer a suas funções fora do espaço da União Europeia. [190]

O EPD pode ser um elemento interno da entidade responsável pelo tratamento ou do subcontratante, nesses casos, trata-se de um EPD interno, ou pode exercer as suas funções no âmbito de um contrato de prestação de serviços, isto é, ser um EPD externo. Caso, seja externo, por motivos de clareza jurídica e com intuito de prevenir conflitos de interesses o contrato de prestação de serviços deve incluir uma clara repartição de tarefas no seio da equipa do EPD externo e a designação de uma única pessoa como contacto principal e da pessoa responsável do cliente. [191]

Relativamente às qualidades profissionais do EPD, o Grupo Artigo 29.º refere que este deve possuir conhecimentos especializados no domínio das normas e práticas de proteção de dados que serão determinados tendo em consideração as operações de tratamento de dados realizadas e a proteção exigida para os dados pessoais em causa nessa operação de tratamento. As competências e conhecimentos especializados dizem respeito às competências de domínio das normas e práticas de proteção de dados nacionais e europeias, incluindo um bom conhecimento do RGP; conhecimento das operações de tratamento efetuadas; conhecimento das tecnologias de informação e da segurança dos dados; conhecimento do setor empresarial e da organização e capacidade para promover uma cultura de proteção de dados no seio da organização. [192]

O EPD para exercer devidamente as suas funções necessita de recursos que devem ser adequados à natureza das operações de tratamento, das atividades de tratamento e dimensão da organização. Os recursos disponíveis deverão ser um apoio ativo às funções do EPD por parte dos quadros de gestão superiores; tempo suficiente para que os EPD desempenhem as suas tarefas; apoio adequado em termos de recursos financeiros, infraestruturas (locais, instalações, equipamento) e pessoal, sempre que necessário; comunicação oficial da nomeação do EPD a todo o pessoal; acesso a outros serviços no seio

[190] Orientações para sobre os encarregados da proteção dos dados (EPD), Grupo do Artigo 29.º para a Proteção de Dados, 16/PT, WP 243 rev. 01, p. 25.
[191] *Idem,* p. 26.
[192] *Ibidem.*

da organização, para que os EPD possam receber apoio, contributos ou informações essenciais por parte desses serviços e formação contínua. [193]

O Encarregado de Proteção de Dados para que possa atuar de forma independente necessita de várias salvaguardas, desde logo, os responsáveis pelo tratamento e os subcontratantes não transmitem instruções relativas ao exercício das suas funções de encarregado de proteção de dados, o responsável pelo tratamento não pode destruir nem penalizar o EPD pelo exercício das suas funções e não é possível um conflito de interesses com outras possíveis atribuições[194].

8. Segurança do Tratamento

O artigo 32.º do Regulamento Geral sobre a Proteção de dados dispõe que tendo em conta as técnicas mais avançadas, os custos, de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado: a) a pseudonimização e cifragem dos dados pessoais; b) a capacidade de assegurar a confidencialidade, integridade e disponibilidade e resiliência permanentes dos sistema dos serviços de tratamento; c) a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de incidente físico ou técnico; d) um processo para testar, apreciara e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento. As questões da segurança serão avaliadas e analisadas no próximo capítulo.

[193] Orientações para sobre os encarregados da proteção dos dados (EPD), Grupo do Artigo 29.º para a Proteção de Dados, 16/PT, WP 243 rev. 01, p. 27.
[194] *Idem.*

Capítulo III – Segurança da Informação

9. Segurança da Informação

Os sistemas de informação encontram-se disseminados nas várias esferas sociais e têm um enorme impacto na vida das pessoas e das organizações, sendo de realçar que a computação ubíqua inflama este cenário. Neste contexto, os aspetos relacionados com a segurança informática desempenham um papel vital nos sistemas de informação sendo necessário que estes sistemas sejam mais seguros para resistir ao elevado número de potenciais ataques. Por conseguinte, as organizações têm dedicado cada vez mais recursos de modo a dar a devida atenção às questões relacionadas com a gestão dos sistemas de informação inclusivamente na sua segurança[195].

No contexto do Regulamento Geral sobre a Proteção de Dados o conceito de sistemas de informação revela-se muito relevante uma vez que as organizações detêm enormes quantidades de dados. A gestão e a segurança desses dados são absolutamente necessárias para cumprir o RGPD. Realce-se que os sistemas de informação constituem-se como um conceito muito debatido, mas ainda carece de uma definição harmonizada e consensual. No entanto, pode ser descrito, *grosso modo*, como um sistema, automatizado ou manual, que compreende pessoas, máquinas e/ou métodos organizados para recolher, processar, transmitir e disseminar dados que representam informações do utilizador[196].

A informação pode ser considerada enquanto um significado transmitido por símbolos. Deste modo, os símbolos podem ser, nomeadamente o alfabeto (carateres, números, pontuações), as sequências genéticas (físicas ou lógicas, como por exemplo, livro ou um computador) e pode ser mensurável, utilizando a teoria da informação desenvolvida por Claude Shannon em 1940. [197] Ainda a este respeito, a definição de informação inclui tipicamente termos como o de precisão, oportuna, conveniente, contextualizada, relevante e intencional pois especifica, consegue ser organizada e valiosa uma vez que pode ser monetizada. Através da informação é possível aumentar a compreensão, diminuir a incerteza, afetar decisões e resultados de comportamento.[198]

---

[195] Nicolas MAYER, *Model-based Management of Information System Security Risk*, 2009, p. 1. Disponível em: https://tel.archives-ouvertes.fr/tel-00402996/document Consultado em: 07-07-2018.
[196] Nicolas MAYER, *Model-based Management of Information System Security Risk*, 2009, p. 2. Disponível em: https://tel.archives-ouvertes.fr/tel-00402996/document Consultado em: 07-07-2018.
[197] Disponível em: https://pure.mpg.de/rest/items/item_2383164/component/file_2383163/content . Consultado em: 05-06-2018.
[198] Disponível em https://pure.mpg.de/rest/items/item_2383164/component/file_2383163/content:. Consultado em: 05-06-2018.

A ISO 27 001 é uma norma internacional que fornece um modelo para estabelecer, implementar, operar, monitorar, rever, manter e melhorar um Sistema de Gestão de Segurança de Informação (SGSI). Desta forma, uma organização necessita de identificar e gerir várias atividades em simultâneo para conseguir funcionar eficazmente. A aplicação de um sistema de processos dentro de uma organização, acompanhada da identificação e interações desses processos e da sua gestão, pode ser chamada de "abordagem de processo". [199]

A abordagem de processo para gestão de segurança da informação apresentada na ISSO 27 001 encoraja os seus utilizadores a enfatizar a importância de:[200]

a) entender os requisitos de segurança da informação de uma organização e a necessidade de estabelecer políticas e objetivos para a segurança da informação;
b) implementar e operar controlos para gestão dos riscos de segurança da informação de uma organização no contexto dos riscos gerais;
c) monitorizar e rever o desempenho e a eficácia do SGSI;
d) melhoria contínua das infraestruturas que suportam o sistema de informação.

A norma ISO 27 001 adota o modelo "Plan-Do-Check-Act" (PDCA) que é aplicado com o objetivo de estruturar todos os processos do SGSI. A Figura 1 ilustra como um SGSI considera os requisitos e expectativas de segurança das informações das partes interessadas e, por meio das ações e processos necessários, produz resultados de segurança da informação que atendem a esses requisitos e expectativas. [201]

[199] International Standard – ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements, 2005, p. 1.
[200] *Idem.*
[201] *Ibidem.*

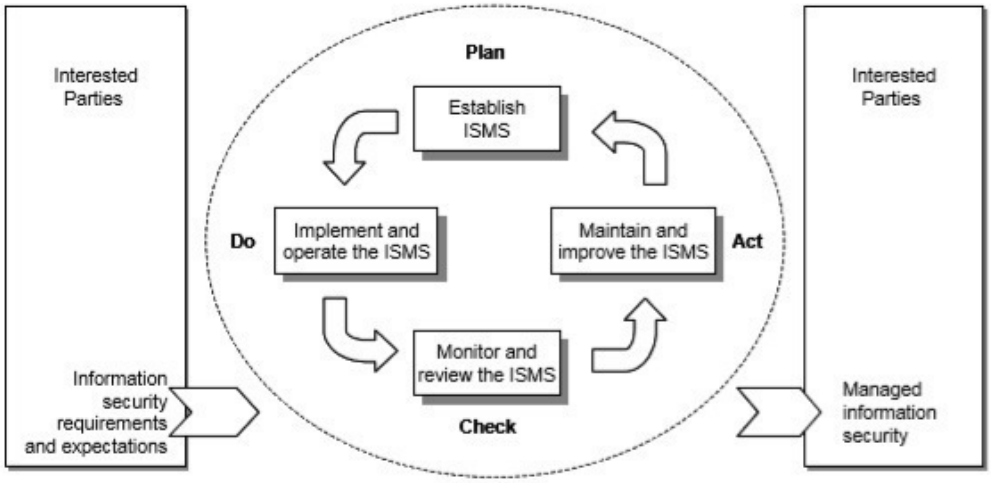

Figura 1- Modelo PDCA aplicado aos SGSI

A segurança da informação pode ser definida como uma prática que visa a defesa das informações contra o acesso não autorizado, uso, divulgação, interrupção, modificação, inspeção, gravação ou destruição dos dados. Apresenta-se como uma definição genérica que pode ser utilizada independentemente da forma como se armazenam os dados, quer seja em formato físico ou digital. Vulgarmente, utiliza-se a segurança de informação nos contextos dos computadores e cenários virtuais e encontra-se fortemente associada ao termo segurança cibernética. A ISO 31 000 é uma norma internacional que fornece a definição de gestão do risco (*risk management*). Nesta norma, o risco é definido como uma combinação da probabilidade de um evento e a sua consequência. Através dessa norma define-se a gestão do risco como um conjunto de atividades coordenadas para dirigir e controlar uma organização em relação ao risco. Os riscos podem estar relacionados com a gestão da organização, por exemplo, doença de uma pessoa chave em relação ao negócio; as finanças, a título de exemplo, relacionadas com investimentos; o meio ambiente como a poluição ou à segurança[202].

A cibernética pode ser encarada como uma disciplina que se baseia na computação que envolve tecnologias, pessoas, informações e processos para permitir operações de uma organização. Esta disciplina envolve a criação, a análise e o teste de sistemas de

[202] Nicolas MAYER, *Model-based Management of Information System Security Risk*, 2009, p. 10. Disponível em: https://tel.archives-ouvertes.fr/tel-00402996/document Consultado em: 07-07-2018.

computadores, bem como agrega áreas relacionadas com o direito, a política, os fatores humanos e a gestão de riscos cimentando-se como uma atividade interdisciplinar. [203] [204]

Tríade CIA – Confidentiality, Integrity e Availability.

O modelo clássico para descrever os principais conceitos da segurança da informação é a chamada tríade CIA – *Confidentiality* (Confidencialidade), *Integrity* (Integridade) e *Availability* (Disponibilidade), que é exibido num diagrama clássico, conforme a imagem *infra*. [205] [206] [207]

Figura 2- CIA Triad

Assim, a segurança visa proteger a confidencialidade, integridade e disponibilidade de informações e/ou processos numa organização. A confidencialidade é a propriedade que garante que as informações não são disponibilizadas ou divulgadas aos indivíduos, entidades ou processos que não estejam autorizados. A integridade é a responsável pela salvaguarda da exatidão e da integridade dos ativos. A integridade é a responsável pela salvaguarda da exatidão e da integridade do sistema podendo ser ameaçada pelas atualizações/alterações (não autorizadas ou adulteradas) e/ou pela exclusão. Por fim, a disponibilidade é a propriedade acessível e utilizável, sob pedido, por uma entidade autorizada. A

[203] Disponível em: https://www.swinburne.edu.au/study/courses/units/Computer-and-Logic-Essentials-COS10003/local.Consultado em: 05-06-2018.
[204] Disponível em: https://www.csec2017.org/. Consultado em:10-07-2018.
[205] Disponível em: https://www.techrepublic.com/blog/it-security/the-cia-triad/ Consultado em: 05-06-2018.
[206] Disponível em: http://panmore.com/the-cia-triad-confidentiality-integrity-availability Consultado em: 15-06-2018.

estas propriedades podem associar-se os conceitos de não-repúdio, autenticidade e de responsabilidade. [208]

Modelo RMIAS – Reference Model of Information Assurance and Security

O modelo RMIAS – *Reference Model Information Assurance and Security*, isto é, modelo de referência de garantia de informação e segurança, é um modelo proposto em 2013 que combina vários pontos de vista e expande o modelo de tríade CIA, exposto anteriormente. Este afigura-se como um modelo que amplia as perspetivas da segurança da informação e considera diferentes aspetos.

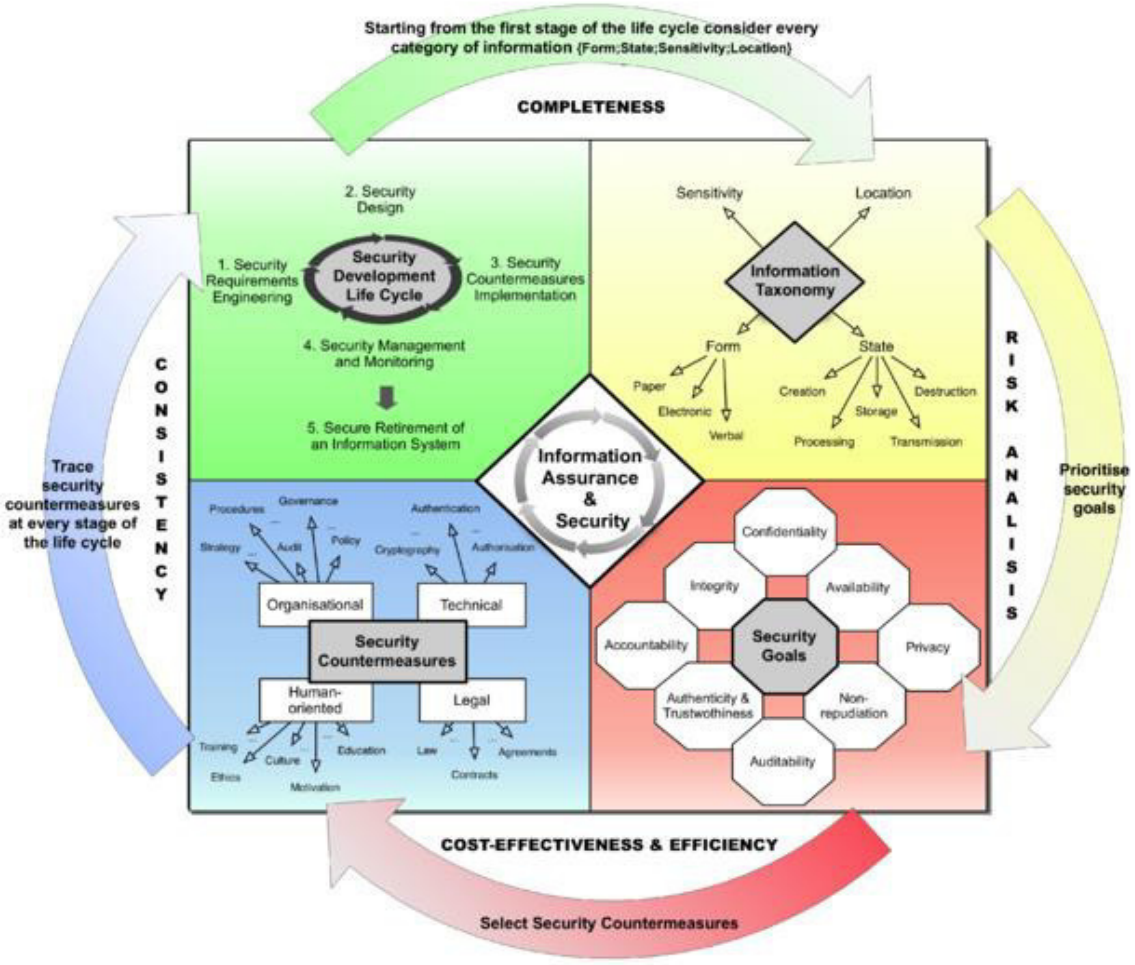

Figura 3 - Reference Model Information Assurance and Security (RMIAS)[1]

[208] Nicolas MAYER, *Model-based Management of Information System Security Risk*, 2009, p. 10-11. Disponível em: https://tel.archives-ouvertes.fr/tel-00402996/document Consultado em: 07-07-2018.

O modelo incorpora quatro dimensões, Ciclo de Vida da Segurança do Sistema de Informação, Taxonomia da Informação, Objetivos de Segurança e Contramedidas de Segurança. Para além disso, incorpora ainda um conhecimento metodológico e auxilia no desenvolvimento e revisão de um documento de política de segurança da informação. [209]

A taxonomia da informação auxilia na compreensão, na interpretação e na identificação da forma em que a informação se encontra, isto é, se está em formato de papel, verbal ou eletrónico. O estado da informação varia ao longo do tempo, desde a sua criação até à sua destruição, e, portanto, a classificação a informação é feita nos seguintes moldes: normal, oficial, secreta ou ultrassecreta. Realce-se que todos estes parâmetros variam de acordo com o contexto em que se encontram inseridos.

No meio do quadrante pode encontra-se o IAS, *Information Assurance & Security* que significa garantia de segurança e de informação. Os objetivos de segurança estipulam quais os parâmetros a que o sistema tem que corresponder para que seja possível alcançar um nível de segurança considerável e ajustado. Assim, o sistema deve possuir caraterísticas como a auditabilidade, que corresponde à capacidade de monitorizar as ações das máquinas e das pessoas. O não-repúdio que tem que ver com a capacidade do sistema de provar a ocorrência ou não de um evento, por exemplo, o envio de um e-mail. A autenticidade e fidedignidade do sistema que se assiste quando este é capaz de verificar a identidade e estabelecer a confiança numa terceira parte, assim como nas informações e serviços prestados. A privacidade onde um sistema deve obedecer à legislação sobre essa matéria e que habilita os utilizadores a controlar e a saber onde é viável colocar a sua informação pessoal. Assim como a capacidade do sistema de se mostrar capaz de possuir as caraterísticas de autenticidade, integridade e disponibilidade e também de responsabilidade que é a capacidade do sistema em que os utilizadores se responsabilizam pelas suas ações. [210]

As contramedidas de segurança encontram-se divididas em quatro áreas principais, a organizacional, a técnica, a legal e as pessoas. Relativamente, às questões técnicas, como a criptografia na proteção os dados no armazenamento ou na transmissão, proteção do perímetro da organização por meio de *firewalls* e dispositivos de deteção e intrusão, controlo de acesso para que apenas os utilizadores autorizados possam aceder à organização. Outra

[209] Disponível em: http://users.cs.cf.ac.uk/Y.V.Cherdantseva/RMIAS.pdf Consultado a 10-01-2018.
[210] Disponível em: http://users.cs.cf.ac.uk/Y.V.Cherdantseva/RMIAS.pdf Consultado a 10-01-2018.

área dentro das contramedidas de segurança são as legais que dizem respeito a um conjunto de leis distintas de vários países em que as organizações atuam e devem ter em consideração nos contratos ou acordos com entidades terceiras. O terceiro aspeto a ter em consideração nas organizações são as pessoas habitualmente referidas como a partes mais vulneráveis na cadeia de segurança. Os primeiros aspetos a serem considerados nas pessoas tem que a ver com a consciencialização, o treino e a educação que podem contribuir para uma cultura de segurança e incutir motivação e desenvolvimento de um quadro ético. Por fim, tem-se a componente organizacional que diz respeito a um conjunto de atividades, estratégias ou procedimentos de gestão, como a definição de políticas, processos, procedimentos e a determinação de conformidade através de auditorias. No centro desses processos encontram-se as pessoas que trabalham dentro de elementos técnicos, legais e organizacionais no seu local de trabalho para alcançar os requisitos do negócio. [211]

[211] Disponível em: http://users.cs.cf.ac.uk/Y.V.Cherdantseva/RMIAS.pdf Consultado a 10-01-2018.

Capítulo IV – Caso de Estudo

10. Caso de estudo

O caso de estudo na dissertação refere-se a uma Instituição Particular de Solidariedade Social que trata dados pessoais sobretudo de crianças, mas também dos respetivos agregados familiares e dos trabalhadores.

Caracterização

As Instituições Particulares de Solidariedade Social estão definidas no Decreto-Lei n.º 119/83 de 25 de fevereiro que aprova o Estatuto das Instituições Particulares de Solidariedade Social, no artigo 1.º "são instituições particulares de solidariedade social, as constituídas por iniciativa de particulares, sem finalidade lucrativa, com o propósito de dar expressão organizada ao dever moral de solidariedade e de justiça entre os indivíduos, que não sejam administradas pelo Estado ou por um corpo autárquico, para prosseguir, entre outros, os seguintes objetivos: a) Apoio a crianças e jovens; b) Apoio à família; c) Proteção dos cidadãos na velhice e invalidez e em todas as situações de falta ou diminuição de meios de subsistência ou de capacidade para o trabalho; d) Promoção e proteção da saúde, nomeadamente através da prestação de cuidados de medicina preventiva, curativa e de reabilitação; e) Educação e formação profissional dos cidadãos e f) Resolução dos problemas habitacionais das populações".

A IPSS em questão é de pequena/média dimensão com cerca de setecentos e vinte e sete (727) utentes e cento e sessenta e seis (166) funcionários.

Descrição do Processo

O plano de intervenção dividiu-se em três momentos: diagnóstico, planificação de medidas de conformidade e na implementação das referidas medidas.

Diagnóstico

O diagnóstico foi realizado a partir de visitas às instalações da Instituição Particulares de Solidariedade Social (doravante IPSS), com questionários aos serviços administrativos e

financeiros de forma a perceber o modo de funcionamento da mesma, no estudo dos documentos de funcionamento da IPSS e da legislação que regula o funcionamento da mesma.

O primeiro passo foi fundamentalmente conhecer a IPSS através de visitas e de questionários, onde foi facultada um conjunto de informação como o regulamento interno, formulários, entre outros. Num segundo momento, constitui-se necessário estudar esses documentos que auxiliavam e regulavam o funcionamento da IPSS, com destaque para o Regulamento Interno e para os formulários de inscrição onde se solicitavam um conjunto de dados.

O segundo passo do plano de intervenção da IPSS teve que ver com o estudo da legislação que regula os institutos particulares de solidariedade social e a legislação que regula especificamente o sector. o estudo da forma e da metodologia de funcionamento da IPSS, designadamente como está organizada. Qual a informação partilhada nos diversos sectores da creche e com que finalidades.

Os dados solicitados dividiam-se por dados das crianças, dos pais e responsáveis legais e agregado familiar e estariam armazenados nas salas ou na secretaria. Os documentos solicitados para a sala são: três fotografias tipo passe, boletim de vacinas, boletim de saúde infantil, cartão de utente da criança, declaração médica comprovando a situação clínica da criança, relatórios médicos, BI's / CC's das pessoas a quem as crianças podem ser entregues e os BI's e CC's do agregado familiar ou responsáveis legais. Os documentos solicitados e que ficam na secretaria, são: os BI's do agregado familiar e responsáveis legais, NIF (Número de Identificação Fiscal) da criança, visto ou autorização de residência, NISS (Número de Identificação de Segurança Social), recibos de vencimento dos familiares (dois últimos meses), Declaração de IRS (Imposto sobre o Rendimento de Pessoas Singulares), despesas com saúde (doenças crónicas), despesas com habitação (renda/empréstimo bancário) e despesas com transporte público (passe) (cf. Anexo 1). Assim, os dados solicitados têm que ver não só com a criança, mas os seus responsáveis legais e com a composição do seu agregado familiar.

Os dados dos funcionários da IPSS solicitados são, designadamente nome, número de identificação civil, NIF, NISS, estado civil, IBAN e dados biométricos para controlo de assiduidade e controlo das entradas na creche.

A IPSS recolhe também dados dos seus associados nomeadamente o nome, morada, NIF e contacto telefónico.

A IPSS possui ainda controlo biométrico para duas pessoas autorizadas a ir buscar as crianças, assim como um sistema de videovigilância.

Admissão de trabalhadores é realizada por divulgação da vaga. A IPSS pode, eventualmente, rececionar currículos na receção das instalações ou através do único e-mail institucional que possui.

Este passo tem como objetivo a realização de um mapeamento de todos os dados que a IPPS possui, para desta forma compreender se os dados solicitados são legítimos, durante quanto tempo devem ser conservados e com quem são partilhados. Assim, a IPPS troca dados com as seguintes entidades: Segurança Social, Autoridade Tributária, Seguradora para o contrato de seguro dos funcionários e das crianças, com a empresa de higiene e segurança no trabalho e advogado. Importa agora compreender a que legislação a IPSS está sujeita e o modo de funcionamento da mesma junto dos funcionários que auxiliam na gestão da IPSS.

A IPSS encontra-se sujeita a toda a legislação que tenha que ver com o funcionamento das Instituições Particulares de Solidariedade Social, nomeadamente o Decreto-Lei n.º 119/83 de 25 de fevereiro que aprova o Estatuto das Instituições Particulares de Solidariedade Social, Portaria n.º 196-A/2015 de 1 de julho, Portaria n.º 262/2011 de 31 de agosto.

Nesta fase, foram também realizadas várias conversas exploratórias no sentido de conhecer melhor a IPSS e as suas dimensões. Para tal, foi elaborado um questionário que foi posteriormente aplicado a um funcionário com uma função crucial na administração da Creche, respetivamente dos Serviços Administrativos e Financeiros. A estrutura e as respostas dadas pela pessoa ao mesmo constam no Anexo 2, ressalvando que nem todas as questões colocadas foram respondidas pois a pessoa entrevistada não tinha conhecimento sobre as mesmas.

Além disso, foi elaborada uma tabela para auxiliar na análise, como todos os dados solicitados, o tipo de dados (se se referiam a dados relativos à saúde, dados biométricos, etc.), quando se tratava de um documento único que dados tinham os documentos, qual a base legal para a sua recolha, quando a base legal para a recolha era o consentimento se o tinha obtido, duração da conservação dos dados, onde estavam armazenados e em que formato (papel, digital ou ambos) (cf. Anexo 10).

Plano de Intervenção

Após a análise de todo o panorama da IPSS definiu-se um conjunto de sugestões para serem discutidas com os funcionários dos Serviços Administrativos e Financeiros e com a Direção da IPSS para saber se as sugestões seriam viáveis do ponto de vista logístico e financeiro.

As sugestões tiveram que ver com a eliminação de dados solicitados na Ficha de Inscrição dos utentes, por razões de inutilidade dos dados, quer por falta de fundamentação jurídica para a solicitação dos mesmos. A Portaria n.º 262/2011 de 31 de agosto, no artigo 15.º define que a creche deve organizar um processo individual de cada criança, do qual constem, designadamente: a) Ficha de inscrição; b) Critérios de admissão aplicados; c) Exemplar do contrato de prestação de serviços; d) Exemplar da apólice de seguro escolar; e) Horário habitual de permanência da criança na creche; f) Identificação, endereço e telefone da pessoa a contactar em caso de necessidade; g) Autorização, devidamente assinada pelos pais ou por quem exerça as responsabilidades parentais, com identificação da(s) pessoa(s) a quem a criança pode ser entregue; h) Identificação e contacto do médico assistente; i) Declaração médica comprovativa do estado de saúde da criança e outras informações tais como dieta, medicação, alergias; j) Comprovação da situação das vacinas e grupo sanguíneo; l) Informação sobre a situação sociofamiliar; m) Registo de períodos de ausência, bem como de ocorrência de situações anómalas e outros considerados necessários. O número dois do artigo dispõe que o processo individual é de acesso restrito e deve ser permanentemente atualizado, assegurando a creche o seu arquivo em conformidade com a legislação vigente, estando em consonância com o princípio da atualização dos dados.

A Portaria n.º 196-A/2015 de 1 de julho define no artigo 19.º define a comparticipação familiar e o anexo do regulamento das comparticipações familiares devidas pela utilização dos serviços e equipamentos sociais a informação necessária para aferir se a família tem ou não direito à comparticipação familiar. Para tal, a IPSS precisa de ter acesso à seguinte informação: os rendimentos do agregado familiar, as despesas fixas do agregado familiar (o valor das taxas e impostos necessários à formação do rendimento líquido; renda de casa ou prestação devida pela aquisição de habitação própria e permanente; despesas com transportes até ao valor máximo da tarifa de transporte da zona de residência; despesas com saúde e a

aquisição de medicamentos de uso continuado em caso de doença crónica) e o número de elementos do agregado familiar.

Com base na análise, as medidas propostas foram:

1. Rever os contratos de subcontratação da IPSS, designadamente a empresa de seguros, higiene e segurança do trabalho, a empresa que fornece o equipamento de controlo biométrico e avença com o advogado.
2. Encontrar alternativas à fotocópia ao cartão de cidadão quer no momento da inscrição, quer para as fotocópias que estão na sala, relativas às pessoas que estão autorizadas a ir buscar as crianças. Uma vez que a fotocópia do cartão de cidadão não é permitida sem o consentimento dos titulares de acordo com a Lei n.º 7/2007 de 5 de fevereiro alterada pela Lei n.º 91/2015 de 2 de agosto de acordo com o artigo 5.º, nº 2 "é igualmente interdita a reprodução do cartão de cidadão em fotocópia ou qualquer outro meio sem consentimento do titular". As soluções podem ser: a utilização de um *software* de leitura do cartão de cidadão para aferir a identidade dos cidadãos no momento da inscrição. Relativamente, às pessoas que estão autorizadas a entrar na Creche, a solução seria a instalação de um programa de leitura do cartão de cidadão que permitisse a entrada e saída das pessoas autorizadas. Outra solução seria eliminação da fotocópia do cartão de cidadão uma vez que apresentação do mesmo deve ser suficiente para atestar a identidade do indivíduo. Outra solução poderá ser a solicitação do consentimento para a fotocópia do cartão de cidadão sendo que depois essa informação deverá ser armazenada em sítio seguro de preferência com recurso a cadeado;
3. Na Ficha de inscrição sugere-se: a eliminação de um conjunto de dados, nomeadamente dados dos pais, como a data de nascimento, profissão, habilitações académicas, de acordo com o princípio da limitação dos dados; apresentar a base legal para os dados que são solicitados; elaborar o consentimento para a solicitação dos dados biométricos dos encarregados de educação e para o cartão de cidadão, caso se decida manter a fotocópia dos mesmos.
4. Reforçar as medidas de segurança do único e-mail utilizado pela IPSS com revisão das práticas de utilização do e-mail, do antivírus e alteração cíclica das passwords.

5. Dados que se encontram na sala tais como, as fotocópias das pessoas a quem a criança pode ser entregue, os dados das tomas dos medicamentos podem manter-se na sala uma vez que por razões logísticas verifica-se estas necessidade. No entanto, toda a informação que possa não ser necessária deve ser entregue aos serviços administrativos e financeiros, tal como dispõe o artigo 15.º da Portaria 262/2011 de 31 de agosto.
6. Informação das crianças encontra-se dispersa por vários departamentos da IPSS, nomeadamente salas, serviços administrativos e financeiros e cantina. Essa informação está relacionada com o facto de algumas crianças terem doenças crónicas, alergias, intolerâncias alimentares entre outros. Esses tipos de informações podem estar dispersa por razões de segurança do próprio utente e por razões de logística. No entanto, essa informação está protegida uma vez que os trabalhadores da IPSS, estes estão obrigados pela cláusula de confidencialidade.
7. Apesar do dever de confidencialidade dos trabalhadores consagrado no Código de Trabalhado do artigo 22.º, para tal, sugeriu-se que se inserisse cláusulas no contrato de trabalho, no sentido de o harmonizar com o RGPD.
8. Proporcionar ações de formação junto dos trabalhadores para que estes se consciencializem acerca destas temáticas.
9. Encontrar um mecanismo apropriado para a receção de currículos quer por abertura de vagas, quer por candidaturas espontâneas rececionadas no e-mail e nas instalações, uma vez que os titulares dos dados possuem o direito da privacidade de informação.
10. Questões importantes a definir:
    a. Estabelecer uma pessoa responsável pelas questões de proteção de dados.
    b. Criar uma espécie de *template*/modelo para comunicar à autoridade de controlo e ao titular dos dados sempre que existir a imposição legal de comunicar. [212]
    c. Criar um mecanismo que permita dar resposta aos pedidos dos titulares dos dados, tais como, o acesso, atualização, esquecimento.
    d. Criar um documento em que se informe o titular dos dados sobre quais os direitos que possui.
    e. Estabelecer uma política de segurança da informação.
11. Criação de uma política de privacidade.

[212] Nota: Definido antes da CNPD disponibilizar o formulário *online.*

Medidas Implementadas

Relativamente, às opções sugeridas no caso dos cartões de cidadão optou-se por se eliminar a fotocópia e fazer a verificação da identidade no momento da inscrição. Relativamente, às pessoas autorizadas a ir buscar as crianças eliminou-se a fotocópia dos cartões de cidadão e optou-se por fazer uma lista das pessoas autorizadas que no momento da entrega da criança atestam a sua identidade com a mostra do cartão de cidadão.

A ficha de inscrição sofreu diversas alterações com a eliminação de um conjunto de dados, nomeadamente dados da filiação e solicitou-se aos pais o consentimento para a recolha dos dados biométricos (cf. Anexo 3). A decisão de solicitar o consentimento aos encarregados de educação teve em consideração diversos aspetos: o facto de o dado pessoal solicitado ser um dado sensível e o facto de que o programa utilizado para a leitura da impressão digital armazena numa base de dados as impressões digitais dos encarregados de educação. Inicialmente, colocou-se a hipótese de não solicitar pois achávamos que o programa utilizado era apenas de leitura e não com recurso a uma base de dados. Depois de contactar a empresa percebeu-se que era utilizada uma base de dados e optou-se pela base legal do consentimento.

Na tabela abaixo podemos observar os dados que eram anteriormente solicitados e os que são solicitados após a intervenção.

Tabela 1- Dados recolhidos na ficha de inscrição: pré e pós implementação do RGPD

	Dados	Antes da implementação	Depois da implementação
Dados de identificação da criança	Nome	X	X
	Data de nascimento/idade	X	X
	Morada/Código Postal/Localidade	X	X
Filiação Mãe	Nome	X	X
	Data de nascimento	X	
	Profissão	X	
	Habilitações literárias	X	
	Local de emprego	X	
	Telefone	X	X
	Morada	X	X
	E-mail	X	X
Filiação Pai	Nome	X	X
	Habilitações literárias	X	
	Local de emprego	X	
	Telefone	X	X

	Morada	X	X
	E-mail	X	X
Informações complementares	Se a criança tem irmãos a frequentar a creche	X	
	Se a criança é familiar de um bombeiro voluntário	X	
	Se a criança necessita de algum apoio especial e qual	X	
Caracterização do Agregado Familiar	Composição do agregado familiar	X	X
	Cópia de encargos com habitação	X	X
	Cópia de dedução do IRS e respetivo comprovativo de liquidação	X	X
	Cópia dos BI's/CC's dos pais	X	
	Se o agregado é beneficiário do RSI	X	
Outros encargos	Tipo de habitação	X	
	Propriedade	X	
	Encargos com habitação	X	X
	Encargos com saúde	X	X
	Outros encargos	X	

Quanto à revisão dos contratos de subcontratação enviou-se uma carta no sentido de consciencializar as empresas com quem a IPSS troca dados da necessidade de cumprir o Regulamento e no sentido de compreender se as empresas estavam sensibilizadas e preparadas para estas questões (cf. Anexo 4)

Relativamente à comunicação de violação de proteção de dados à CNPD esta será efetuada através do formulário online.[213] No entanto, antes da criação do formulário online criou-se um modelo para auxiliar caso isso ocorra (cf. Anexo 5). Quanto à comunicação de violação dos dados ao titular dos dados criou-se um documento modelo (cf. Anexo 6). Criou-se um modelo de exercício de direitos no âmbito do Regulamento Geral sobre Proteção de Dados, caso o titular dos dados o queira utilizar para exercer os seus direitos e de forma a facilitar o procedimento, quer para a IPSS quer para o titular dos dados (cf. Anexo 7).

Quanto à revisão do contrato de trabalho foi sugerida uma adenda ao contrato de trabalho tendo em consideração as alterações do RGPD com as seguintes cláusulas:

[213] Disponível em: https://www.cnpd.pt/DataBreach/?AspxAutoDetectCookieSupport=1

1. A entidade empregadora poderá recolher e tratar dados pessoais dos trabalhadores e dos documentos em que os mesmos se encontrem:
   a. Dados de identificação pessoal (número de identificação civil, número de identificação fiscal, número de identificação da segurança social, contacto telefónico e móvel, morada e endereço de correio eletrónico);
   b. Situação familiar (número de membros do agregado familiar, número de membros dependentes, estado civil, informação sobre situação profissional do cônjuge ou pessoa em condições análogas);
   c. Dados relativos a formação académica ou profissional;
   d. Dados relativos a retribuições (IBAN e identificação do banco junto do qual detém conta bancária);
   e. Fotografias de caráter profissional;
   f. Dados biométricos;
   g. Imagens de videovigilância.
2. Os dados pessoais do trabalhador poderão ser recolhidos e tratados pela entidade empregadora para as seguintes finalidades:
   a. Gestão administrativa, planeamento e organização do trabalho, de igualdade e diversidade no trabalho, saúde e segurança no trabalho, registos disciplinares, registos de antiguidade, prémios de produtividade e outros, publicitação de elementos da empresa em *site,* redes sociais e qualquer outro meio de divulgação da empresa e, outros assuntos relacionados com a gestão pessoal e cumprimento de obrigações conexas com a regulação laboral;
   b. Cálculo e pagamento de retribuições, prestações, abonos e subsídios;
   c. Cálculo e retenção na fonte relativos a descontos nas retribuições e demais atribuições patrimoniais;
   d. Execução de decisão ou sentença judicial, bem como o tratamento de pedidos formados pelos trabalhadores;
   e. Comunicações com o trabalhador;
   f. Tratamento dos assuntos relativos a retribuições, prestações, abonos ou subsídios;
   g. Cumprimento de obrigações previstas por lei e por instrumentos de regulamentação coletiva de trabalho;

h. Para efeitos de exercício e gozo, individual, coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho;
i. Controlo de assiduidade e pontualidade;
j. Segurança de pessoas e bens;
k. Formação profissional.

3. Relativamente aos períodos de retenção e conservação dos dados *supra* referidos estes serão conservados para os seguintes efeitos:
   a. Para a finalidade de gestão administrativa de trabalhadores os dados podem ser retidos por um período de 10 anos após a cessação do contrato de trabalho;
   b. Para efeitos de retribuições, prestações e regalias de trabalhadores, os dados podem ser conservados por um período de 10 anos após a cessação da relação do contrato de trabalho;
   c. Para efeitos de pensões, previdência ou pagamento de prestações complementares devidas em momento posterior à cessação da relação de trabalho, tempo de serviço e evolução da remuneração poderão ser conservados até 10 anos após a cessação da relação de trabalho;
   d. O prazo dos respetivos dados poderá ser prolongado por motivos de ação judicial, até seis meses após a transferência dos dados às instituições judiciárias ou em trânsito em julgado da sentença;
   e. Sem prejuízo do *supra* exposto, os dados pessoais proporcionados serão conservados pelo prazo que for determinado conforme os seguintes critérios: obrigação legal de conservação, duração da relação contratual e terá em consideração quaisquer responsabilidades derivadas dessa relação e, solicitação de supressão por parte do interessado, nos casos aplicáveis.
4. Os destinatários dos dados pessoais serão as seguintes entidades:
   a. Entidades a quem os dados devam ser comunicados por força de disposição legal ou a pedido do titular dos dados;
   b. A empresa responsável pelo processamento de vencimentos, para tal efeito e para o cumprimento das demais obrigações conexas;

c. As instituições financeiras que gerem as contas da entidade destinadas ao pagamento da retribuição dos trabalhadores;
d. As entidades gestoras de Fundos e Pensões, do Regime de Previdência ou dos Fundos de compensação do trabalho e garantia do trabalho;
e. As companhias de seguros com quem é celebrado o contrato de seguro de acidentes de trabalho ou de acidentes pessoais;
f. Empresas formadoras no âmbito da formação profissional;
g. Empresa que fornece os serviços de higiene e segurança no trabalho;
h. Empresa que fornece os serviços de informática que tendo em conta a especificidade da prestação do serviço acedem a um conjunto de informações pessoais dos trabalhadores;
i. Empresa que fornece o equipamento de controlo biométrico;
j. Empresa de informática.

No caso do controlo biométrico dos trabalhadores não foi solicitado o consentimento uma vez que o consentimento poderia não ser considerado livre tendo em conta a diferença de poderes entre o trabalhador e o colaborador. Para além disso, a utilização do controlo biométrico já se encontra regulado pelo Código de Trabalho, designadamente no artigo 18.º, n.º 1 onde dispõe que o empregador só pode tratar os dados biométricos do trabalhador após a notificação à Comissão Nacional de Proteção de Dados, o que a IPSS já tinha feito anteriormente, dispondo dessa autorização para tratar dados biométricos. A IPSS possui um sistema de videovigilância anterior ao Regulamento e também possui a autorização da Comissão Nacional de Proteção de Dados. Caso, a IPSS não tivesse a autorização da CNPD teria que realizar uma AIPD, isto é, uma avaliação de impacto. No entanto, a IPSS foi alertada para o facto de a CNPD estar a elaborar uma lista de tratamentos que deverão ser sujeitas a uma avaliação de impacto. [214] [215]

Relativamente, à receção de currículos quer por abertura de uma vaga de emprego, quer por candidatura espontânea optamos por solicitar o consentimento do titular dos dados, considerando sobretudo que o ónus da prova do cumprimento do Regulamento recai sobre o

[214] Conforme o site da CNPD: https://www.cnpd.pt/bin/consultapublica/consultapublica.htm Consultado em: 31-07-2018.
[215] Conforme o site da CNPD: https://www.cnpd.pt/bin/consultapublica/Projeto_regulamento_1-2018.pdf Consultado em 31-07-2018.

responsável pelo tratamento, isto é, sob a IPSS. O currículo constitui um dado pessoal tendo em conta todos os dados que contêm esse documento, tais como, nome completo, estado civil, contacto telefónico, e-mail e são objeto de tratamento dos dados pessoais, independentemente do modo como foram rececionados. Assim, o titular dos dados tem o direito de ser informado de acordo com o artigo 12.º ou 13.º do RGPD quer o currículo tenha sido rececionado junto do titular dos dados ou quer não tenha sido rececionado junto do titular dos dados.

Outra questão que se levanta em relação aos currículos é de qual será a base legal para o seu tratamento. A legitimidade para o seu tratamento pode ser efetuada com base no artigo 6.º, n.º 2 alínea b) para diligências pré-contratuais, como o é a recolha de currículos na abertura de uma vaga de emprego ou com fundamento do artigo 6.º, nº 2, alínea f) na prossecução de interesses legítimos por parte do empregador, mas não podem deixar de ser aferidos os limites impostos pelo artigo 16.º reserva da intimidade da vida privada e 17.º dados pessoais, ambos do Código do Trabalho. Adverte-se para o facto de que esses dados apenas podem ser tratados para fins de recrutamento e não para outras finalidades, como por exemplo, marketing.

Assim, num primeiro momento poderá se iniciar uma diligencia pré-contratual (quando existe a abertura de uma vaga) ou na prossecução de interesses legítimos do empregador, devidamente justificados e observados os limites do RGPD, aquando da justificação para o interesse legítimo.

O ideal será elaborar um procedimento para a gestão de currículos, onde se contemple o processo de informar os titulares dos dados da forma como os dados irão ser tratados, em especial quais as finalidades dos respetivos dados, o prazo pelo qual os dados serão conservados, de modo a que o fundamento jurídico para o tratamento dos dados seja o consentimento e para se possa sustentar que esse consentimento foi informado.

Relativamente à licitude no tratamento de dados dos currículos não solicitados ou para fins de entrevistas o consentimento, artigo 6.º, nº 2, alínea a) parece ser o mais adequado, pois coloca o ónus das responsabilidades dos dados pessoais em quem fornece os dados pessoais. Desta forma, o titular dos dados deve ser informado que os seus dados pessoais serão objeto de tratamento aquando da sua aquisição. Perante o tratamento de dados pessoais constitui-se necessário observar os princípios para os mesmos e os direitos dos titulares dos

dados pessoais, desde logo, o princípio da limitação do armazenamento e da minimização dos dados. Assim, para efeitos de prova o consentimento será a melhor opção para o tratamento dos currículos. Nesse seguimento, elaborou-se um documento para auxiliar este procedimento, quer quando rececionadas por e-mail quer quando rececionados nas instalações (cf. Anexo 8).

Por fim, foi elaborada a política de privacidade, onde se tentou condensar todos os tratamentos de dados elaborados pela IPSS. A política e privacidade será um documento público à disposição dos pais, responsáveis legais ou funcionários para que possam ter a informação de como a IPSS se preocupa com a temática do RGPD (cf. Anexo 9).

Conclusão

A presente dissertação de mestrado permitiu concluir que a implementação do Regulamento Geral de Proteção de Dados deu origem a várias alterações na organização de uma instituição. Em particular, no caso de estudo, a organização estava imbuída numa lógica de funcionamento instituída há já vários anos, antes de toda a evolução tecnológica. Considerando esta situação, verificou-se que não existia praticamente nenhum questionamento ou sensibilidades acerca da temática da privacidade e da proteção de dados nos seus funcionários e na própria direção.

A implementação do Regulamento deparou-se com algumas dificuldades, desde logo financeiras, uma vez que, existem para compra, mecanismos que podem auxiliar a melhorar a eficiência do trabalho e a da segurança, mas ainda são produtos onerosos para algumas organizações com um orçamento mais limitado. Outra dificuldade teve que ver com a falta de instrumentos e orientações para alguns aspetos da implementação do Regulamento, nomeadamente, de como se elabora uma Avaliação de Impacto sobre a Proteção de Dados. O facto de Portugal não possuir uma legislação nacional nesta matéria dificulta a implementação e a consciencialização das organizações para o cumprimento da disposição legal que é o Regulamento.

Findado o trabalho de implementação técnica do Regulamento na organização em estudo, nunca é de mais realçar que a implementação do Regulamento Geral da Proteção de Dados não se esgota na presente dissertação. A implementação é um exercício diário de consciencialização e de adoção de boas práticas de funcionamento organizacional, dos trabalhadores e das organizações como um todo.

Bibliografia

CANOTILHO, J.J. Gomes e MOREIRA, Vital, *Constituição da República Portuguesa: anotada,* 4.ª Edição, Coimbra, Coimbra Editora, 2007.

CORDEIRO, A. Barreto Menezes, *Dados Pessoais: Conceito, Extensão e Limites.* Disponível em: https://blook.pt/publications/publication/e38a9928dbce/

CUNHA, Paulo de Pitta, *Direito Europeu Instituições e Políticas da União,* Coimbra, Almedina, 2006.

Data Protection Certification, Recommendations on European Data Protection Certification, Version 1.0, European Union Agency For Network and Information Security (ENISA), 2017. Disponível em: https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification

Deliberação n.º 7680/2014, aplicável aos tratamentos de dados pessoais decorrentes de tecnologias de geolocalização em contexto laboral, Comissão Nacional de Proteção de Dados. Disponível em: https://www.cnpd.pt/bin/orientacoes/DEL_7680-2014_GEO_LABORAL.pdf

DUNTONE, Ted e YAGER Neil, *Biometric System and Data Analysis: Design, Evaluation, and Data Mining,* Eveleigh, NSW, Australia, Springer, 2009.

FREITAS, Pedro Miguel, MOREIRA, Teresa Coelho, ANDRADE Francisco – *Data Protection and Biometric Data: European Union Legislation.* **Biometric Security and Privacy, in.,** Switzerland: Springer, 2016.

FUSTER, Glória González, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Vrije Universiteit Brussel (VUB), Bruxelas, Springer, 2014.

GONÇALVES, Maria Eduarda, *O regulamento europeu sobre proteção de dados pessoais e o desafio do Big Data.* Disponível em: http://boletim.oa.pt/oa-02/opiniao_maria-eduarda-goncalves

Guidance Paper - Articles 14-16 of the new Regulation 45/2001: Transparency rights and obligations EDPS Guidance on Articles 14 - 16 of the proposal for a Regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, European Data

Protection Supervision, 2017. Disponível em: https://edps.europa.eu/data-protection/our-work/publications/other-documents/articles-14-16-new-regulation-452001_en

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251), Adopted on 3 October of 2017. Disponível em: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Guidelines on Consent under Regulation 2016/679, (WP 259), Adopted on 28 November 2017. Disponível em: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Guidelines on Personal data breach notification under Regulation 2016/679 (WP 250), adopted on 3 October of 2017. Disponível em: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679 (WP253), adopted on 3 October 2017. Disponível em: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

HAMOUND, R.I; ABIDI, B.R. e ABIDI M.A. (Eds.) *Face Biometrics for Personal Identification: Multi-Sensory Multi-Modal Systems,* The University of Tennessee, USA, Springer, 2007.

International Standard ISO/IEC 27001 – *Information technology – Secutrity techniques – Information security management systems – Requirements.*

KLITOU, Demetrius, *Privacy-Invading Technologies and Privacy by Design – Safeguarding Privacy, Liberty and Security in the 21 st Century,* Leiden University, Holanda, Springer, 2014.

LIU, Nancy Yue, *Bio-privacy: privacy regulations and the challenge of biometrics*, Abingdon: Routledge, 2013.

MAGALHÃES, Filipa, *Formação Regulamento Geral sobre a Proteção de Dados,* Ordem dos Contabilistas, 2018.

Manual da Legislação Europeia de Proteção de Dados, Agência dos Direitos Fundamentais da União Europeia, Conselho da Europa, 2014. Disponível em https://www.coe.int/en/web/data-protection/home

MASSENO, David, *O novo Regulamento Geral sobre a proteção de dados da União Europeia,* Recife, Brasil, 2016. Disponível em: http://manueldavidmasseno.academia.edu/research#talks

MAYER, Nicolas, *Model-based Management of Information System Risk* - Doctoral thesis for the degree of Doctor of Science Computer Science Department, University of Namur, 2009.

Opinion 15/2011 on the definition of consent, Article 29 Data Protection Working Party, (WP187), adopted on 13 July 2011. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento «é suscetível de resultar num elevado risco» para efeitos do Regulamento (EU) 2016/679 (WP 248 rev.01), adotadas em abril de 2017. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf

Orientações sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do subcontratante (WP 244 rev.01), adotadas em 13 de dezembro de 2016. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp244rev01_pt.pdf

Orientações sobre o direito à portabilidade dos dados (WP 242 rev.01), adotadas em 13 de dezembro de 2016. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp242rev01_pt.pdf

Orientações sobre os encarregados da proteção de dados (EPD), (WP243 ver.01), adotadas em 13 de dezembro de 2016. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp243rev01_pt.pdf

Parecer n.º 4/2007 sobre o conceito de dados pessoais (WP136), adotado em 20 de junho. Disponível em: https://www.gpdp.gov.mo/uploadfile/2014/0505/20140505062209480.pdf

Parecer n.º 2/2009 sobre a proteção dos dados pessoais das crianças (Orientações gerais e a situação especial das escolas), (WP 160), adotado em 11 de fevereiro de 2009. Disponível em: https://www.gpdp.gov.mo/uploadfile/2014/0505/20140505062209480.pdf

Parecer n.º 20/2018, Processo n.º 6275/2018, Comissão Nacional de Proteção de Dados, 2018. Disponível em:

http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a5763765130394e4c7a464451554e45544563765247396a6457316c626e527663306c7561574e7059585270646d464462323170633334e686279396a5a57593359544d794f4330325a44526c4c54526c4e546b74596a41304e4331694e54426d4f5449314d6a64684d7a45756347526d&fich=cef7a328-6d4e-4e59-b044-b50f92527a31.pdf&Inline=true

PFLEEGER, Charles P., PFLEEGER, Shari Lawarence, MARGULIS, *Security in Computing,* Fifth Edition, Prantice Hall.

Princípios sobre a Privacidade no local de trabalho – o tratamento de dados em centrais eletrónicas, o controlo do e-mail e do acesso à Internet, Comissão Nacional de Proteção de Dados, 2002. Disponível em: https://www.cnpd.pt/bin/orientacoes/PRINCIPIOS-controloE-mails-telefones-Internet.pdf

RATHA, Nalini K. e GOVINDARAJU, *Advances in Biometrics: Sensors, Algorithms and System,* New York, USA, Springer, 2008.

SHONIREGUN, Charles A. e CROSIER, Stephen, *Securing Biometrics Applications,* University of East London, London, UK, Springer, 2008.

SILVEIRA, Alessandra, *Princípios de Direito da União Europeia,* 2ª edição, Lisboa, Quid Iuris, 2011.

VIELHAUER, Claus *Biometric Use Authetication for IT Security: From Fundamentals*, Universitdt Magdeburg, Magdeburg, Germany, Springer, 2006.

ZARZA, Ángeles Guitérrez, *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe,* The Hargue, Holanda, Springer, 2015.

Anexos

- Fichas de inscrição pré e pós implementação
- Documentos de auxílio à implementação e cumprimento do Regulamento

11. Anexo 1 – Ficha de inscrição antes da implementação

FICHA DE INSCRIÇÃO

Instituição Particular de Solidariedade Social

A. A PREENCHER PARA INSCRIÇÃO DA CRIANÇA NA RESPOSTA SOCIAL

1. VALÊNCIA A QUE SE CANDIDATA

SEDE ☐ PALMEIRA ☐

2. RESPOSTA SOCIAL

CRECHE ☐ PRÉ- ESCOLAR ☐ CATL ☐ LAR DE APOIO ☐

3. DADOS DE IDENTIFICAÇÃO DA CRIANÇA

Nome:

Nome pelo qual é tratado:

Data de nascimento: Idade: Anos/Meses

Morada:

Fotografia

Código postal: Localidade: Telefone:

4. FILIAÇÃO

Nome da Mãe:

Data nascimento: Habilitações literárias:

Profissão: Local de emprego: Telefone:

Morada:

Código postal: Localidade:

Telefone: Telemóvel: Mail:

Nome do Pai:

Data nascimento: Habilitações literárias:

Profissão: Local de emprego: Telefone:

Morada:

Código postal: Localidade:

Telefone: Telemóvel: Mail:

Página 1 de 3

FICHA DE INSCRIÇÃO

Instituição Particular de Solidariedade Social

5. INFORMAÇÕES COMPLEMENTARES

Irmãos a frequentar o estabelecimento?

Sim ☐ Se sim, qual o nome e a resposta social que frequenta?

Não ☐

Criança familiar de Bombeiro Voluntário?

Sim ☐

Não ☐

Criança necessita de algum apoio especial?

Sim ☐ Se sim, especifique?

Não ☐

6. OUTRAS NFORMAÇÕES (Aplicável ao CATL)

Escola que pretende frequentar:

Regime:

☐ Pontas com almoço

☐ Pontas sem almoço

7. CARACTERIZAÇÃO DO AGREGADO FAMILIAR

Composição do agregado familiar
Identificação das pessoas que residem com a criança habitualmente

Nome	Parentesco	Idade	Profissão	Rendimento Mensal Líquido *Aplicável a estabelecimentos da rede solidária e da rede pública*
			Sub-total	
			Outros rendimentos	
			Total	

Anexar cópia dos seguintes documentos:

- Encargos com a habitação
- Declaração de IRS e respectivo comprovativo de liquidação
- Recibo de vencimento dos familiares
- BI dos pais
- NISS/ NIF da criança

FICHA DE INSCRIÇÃO

Instituição Particular de Solidariedade Social

Local de residência do Agregado Familiar (morada):

Agregado Familiar Beneficiário de RSI?
(Aplicável a estabelecimentos da rede solidária e da rede pública)

Sim ☐

Não ☐

Dados do Agregado Familiar
(Aplicável a estabelecimentos da rede solidária e da rede pública)

Tipo de habitação	**Propriedade**
☐ Vivenda	☐ Própria
☐ Andar	☐ Alugada
☐ Parte da casa	
☐ Quarto	

Encargos: (mensais ou anuais)	
Habitação:	
Saúde:	
Outros:	
Total:	

5. ASSINATURAS	
Família:	Data:
Organização:	Data:

12. Anexo 2 – Questionários

Grupo I - Quanto à organização da [redacted]

1. Poderia facultar-nos um documento com a hierarquia da organização? (documento que descreve a empresa; uma representação concisa dos aspetos organização)? **Sem resposta.**
2. O número de funcionários da Creche: **166**

- **Dos 166 funcionários, a informação recolhida aquando do contrato é a mesma para todos?**
- **Qual o procedimento efetuado quando há rescisão de contrato de funcionários**?

3. Já foram alvo de uma inspeção da Segurança Social? S**im.**
4. Já foram alvo de uma inspeção da Autoridade Tributária? **Não.**

Grupo II - Quanto aos apoios da Segurança Social

1. A segurança social atribui subsídios/apoios tendo em conta os rendimentos de cada agregado familiar ou por cada criança? **Por cada criança.**

Grupo III - Dados solicitados aos pais

1. Porque são solicitadas as habilitações literárias dos pais? **Sem resposta.**
2. Os dados económicos são solicitados devido ao facto de que se tem em conta a situação económica de cada utente no pagamento da mensalidade? **Sim.**
3. Os dados de saúde solicitados são genéricos ou específicos? **Genéricos.**
4. Que dados são solicitados aos pais para que possam usufruir do horário alargado da Creche? **Não são pedidos dados aos pais no início do ano há um documento para os pais que necessitam do horário alargado assinado.**

Grupo IV - Dados

1. Os dados que constam na secretaria são armazenados em papel, em digital ou ambos? **Ambos.**
2. Que dados dos utentes se encontram nas salas? Encontram-se armazenados em papel, em digital ou ambos? Quem tem acesso aos mesmos? **Na sala os dados estão em**

papel: cc dos responsáveis pela criança e de quem os pode vir buscar. os funcionários da sala têm acesso aos documentos.

3. Existe controlo de acesso dos funcionários a sistemas e aplicações? **Não**
4. Todos os funcionários podem aceder aos sistemas e aplicações? **Não, só os funcionários dos serviços administrativos e financeiros.**
5. Possui uma política de segurança da informação? Se sim, por favor, envie em anexo. **Não, no entanto, não damos o acesso a qualquer pessoa nos serviços.**
6. Já sofreram algum ataque informático? **Sim, em 2015 foi corrompido um ficheiro de salários.**

Grupo V – Dados biométricos

1. O controlo a partir de dados biométricos só é feito em relação aos funcionários? **Funcionários e pais.**

Grupo VI – Acesso à Creche por parte dos pais ou outros

1. Como é feito o controlo de acesso à Creche por parte dos pais ou de outros estranhos aos serviços? **Através do sistema biométrico dos pais.**
2. Que serviços e qual o critério para deixarem entrar uma pessoa estranha na creche? **Os estranhos aos serviços tocam à campainha e a funcionária encaminha para o serviço.**

Grupo VII – Outras informações

1. São guardados de forma estruturada (em formulário eletrónico ou em papel) alguns dos seguintes dados:
   a. A informação sobre quem efetuou os pagamentos das prestações (e quando)? **Papel.**
   b. Detalhes dos períodos de suspensão de prestação de serviços? **Papel.**
   c. Notificações aos Encarregados de Educação, nomeadamente, notificações por desrespeito pelo regulamento (pagamentos, higiene, etc.)? **Papel.**
   d. Quem notifica os pais em caso de falta de pagamento de prestação de serviços? **Sem resposta.**

e. Informações sobre participação em atividades extracurriculares (e respetivas avaliações se aplicável)? **Papel.**
f. Registo dos incidentes de doença familiar e necessidades de tratamento médico da criança? **Papel.**

2. Haverá informação, que possa ser associada a um utente ou respetiva família, que seja partilhada com outras entidades, nomeadamente para:
   a. Fornecimento de atividades extracurriculares? **Os pais preenchem diretamente na ficha da escola das atividades extracurriculares os dados.**
   b. Contratação de seguros? **Os nomes das crianças vão nas listas mensais que temos de enviar para o seguro.**
3. Como é que a informação sai da Creche para os seguros, com a lista do nome das crianças? Por mail, por carta ou por outra forma de envio? **Lista enviada por email.**
4. Para além dos contratos de seguro, a Creche realiza e com quem troca informação de dados pessoais? Por exemplo, serviços de transporte utentes, serviços de refeição e de lavagem de roupa ou outros? **Com mais ninguém, utilizam a plataforma da SS para enviar o NISS das crianças.**
5. Quem é que tem acesso todos os serviços. Quem tem acesso à secretaria? Quem tem acesso à tesouraria? **Pessoal que trabalha nos serviços administrativos e financeiros.**
6. Quando as crianças sofrem de doenças crónicas, quem tem acesso à informação? Onde é armazenada a informação? **Na secretaria, na sala e na cozinha. A informação é armazenada na sala.**
7. Quem notifica os representantes legais quando existe uma falha de pagamento? Como é feita essa notificação, por mail, carta ou outra forma? Quem tem acesso a essa informação? **Por carta, a tesouraria notifica, tem acesso o pessoal dos serviços administrativos e financeiros.**
8. Existe algum tipo de avaliação das crianças? Quem tem acesso? Onde está armazenada? **Sim, a PDI, a educadora e está armazenada na sala.**
9. Os registos de incidentes de doença familiar e os dados de necessidade de tratamento? Quem tem acesso? Como a informação é recolhida? É fornecida pelos pais ou é feita por um atestado médico? **É necessário saber o que acontece a todos os dados de**

saúde da criança. Só é necessário saber se a criança tem alguma doença crónica é perguntado aos pais, armazenado na sala.

10. A informação recolhida aquando do contrato é a mesma para todos os funcionários? **Sim.**
11. Todos os funcionários podem aceder aos sistemas e aplicações? Ou o acesso a limitado a um departamento dos serviços? Se sim, qual? **Não, só os serviços financeiros e administrativos.**
12. Quando o ficheiro de salários foi corrompido, quem teve conhecimento? Qual foi a gravidade? O que foi feito para reparar o dano? Isso está documentado? **A direção e os serviços administrativos e financeiros; foram chamados os técnicos de informática e não conseguiram recuperar o ficheiro.**
13. Qual o critério para deixarem entrar uma pessoa estranha na creche? **Uma pessoa estranha não pode entrar.**
14. Os documentos que se encontram armazenados em papel estão seguros de alguma maneira? Isto é utilizam por exemplo cadeados? E sabem quem é que acede a esses documentos, está limitado a determinados funcionários? **Os documentos encontram-se no arquivo e as únicas pessoas que têm acesso são as que trabalham nos serviços administrativos e financeiros.**

13. Anexo 3 – Ficha de inscrição pós implementação do RGPD

Instituição Particular de Solidariedade Social

FICHA DE INSCRIÇÃO

A presente ficha de inscrição, está de acordo com o novo REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (de 25 de maio de 2018) - Regulamento europeu nº 2016/679.

- Os dados que constam na Ficha de inscrição da Associação da Creche de Braga- Instituição Particular de Solidariedade Social- serão tratados conforme a legislação em vigor.

1. VALÊNCIA A QUE SE CANDIDATA

SEDE ☐ PALMEIRA ☐

2. RESPOSTA SOCIAL

CRECHE ☐ PRÉ-ESCOLAR ☐ ATL ☐

3. DADOS DE IDENTIFICAÇÃO DA CRIANÇA (de acordo com o disposto no art.º 14º da Portaria 262/2011)

Nome completo:

Nome pelo qual é tratado:

Idade (à data da inscrição):

NISS: NIF:

Morada: Código postal: _____ - _____

LOCALIDADE: TELEFONE:

4. FILIAÇÃO (de acordo com o disposto no art.º 14º da Portaria 262/2011)

Nome da Mãe:

Telefone: Telemóvel:

Morada: Código postal: _____ - _____

Localidade: Correio eletrónico:

Nome do Pai:

Telefone: Telemóvel:

Morada: Código postal: _____ - _____

Localidade: Correio eletrónico:

Sede

1

Instituição Particular de Solidariedade Social

5. INFORMAÇÕES COMPLEMENTARES

Tem irmãos a frequentar a Instituição:

Sim ☐ **Não** ☐

Se sim, qual o nome e a resposta social que frequenta?

Nome:_____

Resposta Social:_____

6. OUTRAS INFORMAÇÕES (Aplicável ao CATL)

Escola que pretende frequentar:

Regime:

Pontas com almoço: ☐ Pontas sem almoço: ☐

7. CARACTERIZAÇÃO DO AGREGADO FAMILIAR:
(Identificação das pessoas que habitualmente residem com a criança)

Nome	**Parentesco**	**Rendimento mensal Líquido** (de acordo com o disposto no nº4 do anexo do art.º 19 da Portaria 196-A-2015) *Aplicável a estabelecimentos da rede solidária e da rede pública*
	Sub- total	
	Outros rendimentos	
	Total	

2

Sede

8. ENCARGOS (mensais ou anuais) (conforme a Portaria nº 196-A/2015 de 1 de julho- anexo ao art.º 19, nºs 4 e 5)	
Habitação:	
Saúde:	
Outros:	
Total:	

Devem entregar na Secretaria da Instituição, os seguintes documentos:
(conforme a Portaria nº 196-A/2015 de 01 de julho)

- Declaração de IRS e respetivo comprovativo de liquidação (nº4);
- Despesas com o transporte (nº 5.1 alínea c);
- Despesas com a habitação (n º 5.1 alínea b);
- Despesas com a saúde (doenças crónicas) (n º 5.1 alínea d);

3

Autorizo que os dados pessoais que constem na Ficha de Inscrição da *Associação da Creche de Braga,* sejam tratados para o fim para os quais são recolhidos, com a certeza que a Instituição os tratará de acordo com os pressupostos de proporcionalidade e de finalidade:

Assinatura do encarregado de educação:_____

Data:____/____/_____

(A preencher pelos serviços)

Recebido por: _____	Data: ___/ ___/ _____

14. Anexo 4 – Carta de consciencialização para o cumprimento do RGPD

De: [redacted]

Para: [redacted]

Assunto: Acordo sobre o Tratamento de Dados pessoais

Exmos Senhores,

A [redacted] demonstra preocupação com o tratamento de dados pessoais dos seus trabalhadores, considerando a aplicação do Regulamento sobre a Proteção de Dados, doravante RGPD. A presente carta tem como intuito percecionar se os dados pessoais fornecidos pela [redacted], no âmbito da prestação de serviços se encontram a ser tratados e processados de acordo com a legislação em vigor.

Nos termos do RGPD a [redacted] assume o papel de responsável pelo tratamento e a [redacted] o papel de subcontratante. A [redacted] necessita perceber se no âmbito da prestação de serviços realizados pode assumir que a [redacted] cumpre os seguintes pontos:

a) O tratamento dos dados pessoais obedecerá às instruções documentadas do responsável pelo tratamento, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, exceto se for obrigado a fazê-lo elo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso o responsável pelo tratamento desse requisito, antes de proceder a essa transferência, salvo se tal informação for proibida por motivos de interesse público;

b) Garante que as pessoas autorizadas a tratar dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;

c) Adota todas as medidas de segurança do tratamento, designadamente:

   i) a pseudonomização e a cifragem de dados pessoais;

   ii) a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;

   iii) capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada em caso de incidente físico ou técnico;

   iv) têm um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

d) O Subcontratante tem implementado todas as medidas técnicas e organizativas para dar respostas aos pedidos os titulares dos dados para o exercício de direitos, nomeadamente do direito de acesso, retificação, apagamento, limitação do tratamento, portabilidade dos dados e oposição ao tratamento;

e) Apenas contratará outro subcontratante se o Responsável pelo Tratamento o autorizar ou, em caso de autorização prévia, comunicará ao Responsável pelo Tratamento a contratação de um subcontratante que deverá respeitar todas as obrigações de tratamento decorrentes do RGPD;

f) Caso ocorra uma violação dos dados fornecidos pelo Responsável pelo tratamento no âmbito do presente contrato, o Subcontratante comunicará a violação de dados ao Responsável pelo tratamento no prazo máximo de 36 horas a contar a partir do momento em que tiver conhecimento da mesma;

g) Em caso de violação dos dados, o Subcontratante adotará todas as medidas técnicas para sanar e diminuir o impacto da violação dos dados, assumindo todos os custos resultantes dessa ação. Garante que implementou um plano de ação e uma equipa de gestão desses incidentes;

h) O Subcontratante comunicará ao Responsável pelo tratamento a nomeação de um Encarregado de Proteção de Dados ou de um ponto de contato nessas temáticas, para facilitar a comunicação nesses domínios;

i) Caso estas disposições não sejam cumpridas o Responsável pelo tratamento pode pedir que o Subcontratante o indemnize nos termos gerais de direito dos prejuízos causados.

Solicita-se que a [redacted] responda à presente carta garantindo que os dados pessoais fornecidos e gerados através do contrato de prestação de serviços que estabelece com a [redacted] se encontram de acordo com os preceitos supramencionados, isto é, de acordo com o Regulamento Geral sobre a Proteção de dados.

Entende-se como aceitação dos termos e garantia de conformidade com o RGPD a cópia da preste carta, assinada e com a indicação do responsável pela matéria de proteção de dados ou o Encarregado de Proteção de Dados e os respetivos contatos.

Na [redacted] o contato nestas matérias pode ser feito através do seguinte e-mail "[redacted]@[redacted].com" com o assunto: "RGPD – [redacted]"

Sem mais assunto, apresentamos os nossos melhores cumprimentos.

Braga,

_____

15. Anexo 5 – Modelo para comunicação de violação de dados à CNPD

Notificação de Violação de Dados Pessoais

Tipo de notificação: Completa ☐ Preliminar ☐ Complementar ☐

Data da notificação: ____/____/_____

Notificação/Incidente número: _____

Avaliação do incidente: Insignificante: ☐ Reduzido: ☐ Significativo: ☐ Crítico: ☐

Dados sobre a organização

Nome da organização: _____

Morada: _____ Código Postal: _____

Telefone: _____ E-mail: _____

Responsável pelo Tratamento de Dados: _____

Encarregado da Proteção de dados: _____

Nome da pessoa que identificou a violação de dados: _____

Pessoa para contacto (para obtenção de informação sobre a violação de dados)

Nome: _____

Função na organização: _____

Morada: _____ Código Postal: _____

Telefone: _____ E-mail: _____

Linha cronológica

Data da violação: _____ Data de fim da violação: _____

Data de início da violação: _____ Data de conhecimento da violação: _____

Razões que levaram ao conhecimento da violação: _____

_____

_____

Informações sobre a violação de dados

Natureza da violação: Confidencialidade ☐ Integridade ☐ Disponibilidade ☐

- ☐ Dispositivo perdido/roubado
- ☐ Negação do Serviço (Denial of service)
- ☐ Espionagem cibernética
- ☐ Crime cibernético
  - Malware
  - Phising
  - Spam
- ☐ Documentos em papel perdidos/roubados
- ☐ Perda de e-mail ou roubo

Outra: _____

Página **1** de **3**

Causa da violação de dados:

- ○ Negligência interna (erro humano)
- ○ Violação interna intencional
- ○ Fonte externa não maliciosa
- ○ Fonte externa maliciosa
- ○ Acidental (falha no sistema)

Outra: _____

Informações sobre os dados

Nº de dados pessoais envolvidos na violação de dados: _____

Dados violados:

- ○ Dados de identificação (nome, data de nascimento, morada, etc…)
- ○ Dados económicos e/ou financeiros
- ○ Dados que revelam opiniões políticas, convicções religiosas ou filosóficas
- ○ Dados que revelam a filiação sindical
- ○ Dados sobre condenações penais e infrações
- ○ Dados genéticos
- ○ Dados biométricos
- ○ Dados sobre opiniões políticas
- ○ Dados que revelam origem racial ou étnica
- ○ Dados médicos
- ○ Dados sobre a vida sexual
- ○ Dados sobre a atividade profissional
- ○ Ainda desconhecidos

Titulares dos Dados

Titulares dos dados:

- ○ Funcionários
- ○ Clientes
- ○ Menores de idade
- ○ Utilizadores
- ○ Pacientes
- ○ Subscritores

Outro(s):

Descrição detalhada dos titulares de dados envolvidos na violação: _____

_____

_____

_____

Nº de pessoas envolvidas preocupadas com a violação: _____

Consequências

Violação da disponibilidade:

- ○ Perda da capacidade de fornecer um serviço aos titulares de dados envolvidos na violação
- ○ Alteração da capacidade de fornecer um serviço aos titulares de dados envolvidos na violação
- ○ Outro: _____

_____

Natureza do potencial impacto para o titular dos dados:

- ☐ Perda de controlo sobre os dados
- ☐ Limitação dos seus direitos
- ☐ Discriminação
- ☐ Usurpação ou roubo de identidade
- ☐ Fraude
- ☐ Perda financeira
- ☐ Dano reputacional
- ☐ Outra: _____

_____

Severidade do potencial impacto: Insignificante ☐ Reduzido ☐ Significativo ☐ Crítico ☐

Medidas tomadas

Os titulares dos dados foram informados:

- ☐ Sim
- ☐ Não, mas serão informados
- ☐ Não serão informados
- ☐ Ainda não definido

Medidas adotadas pelo responsável pelo tratamento de dados e/ou subcontratante para mitigar as consequências da violação:

Medidas propostas pelo responsável pelo tratamento de dados e/ou subcontratante para mitigar as consequências da violação:

16. Anexo 6 – Notificação de uma violação de dados pessoais ao titular dos dados

Exmo (a) Senhor(a), _____

Vimos por este meio comunicar-lhe que devido a fatores que infelizmente não conseguimos controlar os seus dados pessoais fornecidos à [redacted] foram comprometidos através de uma violação dos dados pessoais que poderá ter como consequências:

□ Perda de controlo sobre os dados
□ Limitação dos seus direitos
□ Discriminação
□ Usurpação ou roubo de identidade
□ Fraude
□ Perda financeira
□ Dano reputacional
□ Outra: _____

A [redacted] para reparar a violação de dados pessoais tomou as seguintes medidas:

Para mais informações contacte: contacto de e-mail

17. Anexo 7 – Exercício de direitos do RGPD

Na sequência dos meus dados pessoais cedidos à [redacted] para efeitos de tratamento dos mesmos, venho por este meio, pelos poderes que detenho nos termos dos arts. 12.º e seguintes do RGPD, exercer o seguinte direito (marcar com X o direito que pretendo exercer):

- O direito a ser informado___
- O direito de acesso aos seus dados___
- O direito à retificação dos seus dados____
- O direito ao esquecimento/apagamento____
- O direito à restrição de processamento____
- O direito à portabilidade dos dados_____
- O direito de oposição____
- Direitos de oposição a decisões individuais automatizadas, incluindo a definição de perfis____

Pretendo que o direito seja exercido da seguinte forma:

_____

_____

_____

_____

Para dar cumprimento ao direito por mim exercido dou expressamente consentimento para utilização do meu e-mail_____ para posteriores notificações.

18. Anexo 8 – Receção dos currículos

- **Receção de currículos por e-mail:**

Quando os currículos são rececionados por e-mail deve enviar a seguinte resposta:

Devido à alteração da legislação no âmbito da legislação de proteção de dados para que se possa proceder ao tratamento do seu currículo para efeitos de recrutamento necessitamos do seu consentimento. Para tal, basta enviar um e-mail de resposta, assinado com a seguinte frase:

Aceito que os dados pessoais sejam tratados para fins de recrutamento.

Caso, não responda a este e-mail com a frase referida teremos que não considerar os seu e-mail e os seus dados não serão utilizados para recrutamento.

Os titulares de dados no âmbito do regulamento geral de proteção de dados possuem um conjunto de direitos e podem exercê-los a qualquer momento. Os direitos dos titulares de dados são, designadamente o direito de informação, acesso, retificação, limitação ou oposição a tratamento, e eliminação dos seus dados pessoais. Se desejar dispor de algum destes direitos deve contactar para o efeito a [redacted] com o assunto "Exercício de direitos dos titulares dos dados" para os seguintes contactos:

Morada: _____

E-mail: _____

- **Receção de currículos nas instalações da empresa:**

Os currículos devem após a receção devem ser guardados em envelope fechado e transportado para as instalações da administração/ recursos humanos no final do expediente.

Nota: se o consentimento não for facultado não se pode rececionar os currículos.

Consentimento pode ser facultado de uma das seguintes formas:

1. Devido à alteração da legislação no âmbito da legislação de proteção de dados para que se possa proceder ao tratamento do seu currículo para efeitos de recrutamento necessitamos do seu consentimento. Para tal, todas as folhas do currículo devem estar rubricadas pelo titular dos dados e na última folha do currículo deve constar a seguinte

frase: **Aceito que os dados pessoais sejam tratados pela [redacted] para fins de recrutamento.**

Os direitos podem ser enviados por e-mail ou impressos.

Caso, não aceite dar o seu consentimento não podemos aceitar o sei currículo. Os titulares de dados no âmbito do regulamento geral de proteção de dados possuem um conjunto de direitos e podem exercê-los a qualquer momento. Os direitos dos titulares de dados são, designadamente o direito de informação, acesso, retificação, limitação ou oposição a tratamento, e eliminação dos seus dados pessoais. Se desejar dispor de algum destes direitos deve contactar para o efeito a [redacted] com o assunto "Exercício de direitos dos titulares dos dados" para os seguintes contactos:

Morada: _____

E-mail: _____

2. Devido à alteração da legislação no âmbito da legislação de proteção de dados para que se possa proceder ao tratamento do seu currículo para efeitos de recrutamento necessitamos do seu consentimento:

☐ Aceito que os meus dados sejam tratados pela [redacted] para fins de recrutamento.

☐ Não aceito que os meus dados sejam tratados pela [redacted] para fins de recrutamento.

Caso, não aceite dar o seu consentimento não podemos aceitar o sei currículo. Os titulares de dados no âmbito do regulamento geral de proteção de dados possuem um conjunto de direitos e podem exercê-los a qualquer momento. Os direitos dos titulares de dados são, designadamente o direito de informação, acesso, retificação, limitação ou oposição a tratamento, e eliminação dos seus dados pessoais. Se desejar dispor de algum destes direitos deve contactar para o efeito a [redacted] com o assunto "Exercício de direitos dos titulares dos dados" para os seguintes contactos:

Morada: _____

E-mail: _____

19. Anexo 9 – Política de privacidade

I. A [redacted] é uma Instituição particular de solidariedade social e utilidade pública devidamente registada na Direção-Geral da Segurança Social no livro das Associações de Solidariedade Social, que desenvolve a sua atividade nos seguintes estabelecimentos e com as seguintes respostas sociais: [redacted]

II. Sede: [redacted]

III. O presente Regulamento Interno de Política de Proteção de Dados e Privacidade aplica-se a todos os indivíduos que no âmbito da sua relação contratual com a IPSS fornecem dados pessoais. Os dados pessoais segundo a legislação em vigor caraterizam-se como a informação relativa a uma pessoa singular identificada ou identificável, 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 da pessoa singular.

IV. Informação recolhida:

1. Dos utentes: Cartão de Cidadão ou Bilhete de Identidade (Nome, Filiação, Número de Identificação civil, NIF, NISS, Número de utente e fotografia), fotografias boletim de vacinas, boletim de saúde infantil, declaração médica comprovando a situação clínica da criança, relatórios médicos.
2. Dos responsáveis legais/agregado familiar: Cartão de Cidadão ou Bilhete de Identidade (Nome, Filiação, Número de Identificação Civil, NIF, NISS, Número de utente e fotografia) com justificação legal, na Portaria 262/2011, de 31 de agosto, artigo 14.º, nº1, alínea a). Relativamente, às informações do agregado familiar, nomeadamente, encontram-se reguladas na Portaria nº 196-A/2015, de 1 de julho, no Anexo (a que se refere o Artigo 19.º) Regulamento das comparticipações familiares devidas pela utilização dos serviços e equipamentos sociais, a declaração de IRS e respetivo comprovativo de liquidação, ponto 4, as despesas com transporte, ponto 5.1., alínea c), despesas com habitação, ponto 5.1., alínea c), despesas com habitação, ponto 5.1. alínea b) e despesas com a saúde, ponto 5.1., alínea d).

3. Dos funcionários: nome, número de identificação civil, número de identificação fiscal, número da segurança social, IBAN e dados biométricos.
4. Dos associados: nome, morada, número de identificação fiscal e contacto telefónico.
5. Dados sensíveis: recolha de impressão digital.
6. A recolha de fotografias dos utentes realizada pela IPSS prende-se com razões de identificação dos utentes.
7. A recolha de dados efetuada constitui-se necessária para a correta prestação de serviços a que a IPSS se dedica.
8. Assim, tendo em conta a importância dos dados recolhidos os utentes e funcionários devem manter atualizar as informações recolhidas, para que os dados se encontrem atualizados uma vez que são imprescindíveis ao bom funcionamento da IPSS, bem como à qualidade dos serviços prestados pela mesma.
9. A IPSS assegura que os dados pessoais fornecidos pelos utentes são devidamente protegidos.

V. Finalidades para os quais a informação é recolhida:

1. Obrigações para com entidades do Estado, designadamente:
    i. Segurança Social
    ii. Autoridade Tributária
    iii. Para o cumprimento das obrigações/ legislação estatal.
2. Para que seja possível contactar os interessados em casos de em casos de falta de pagamento, em caso de doença ou indisposição dos utentes, para informar os responsáveis legais assuntos relacionados com os utentes, alterações de preçário, entre outros assuntos relacionados com a prestação de serviços.
3. Para fins estatísticos, no sentido de melhorar o funcionamento e consequente prestação de serviços da IPSS.
4. Para aumentar o nível de personalização dos serviços da IPSS.
5. Os dados pessoais sensíveis serão recolhidos para os seguintes fins:
    i. Os dados biométricos dos trabalhadores serão utilizados apenas para controlo de assiduidade dos trabalhadores;
    ii. Os dados biométricos dos responsáveis parentais e das pessoas a quem os utentes podem ser entregues.

6. Os dados biométricos quando recolhidos têm que ser acompanhados do consentimento.

VI. Comunicação/Divulgação dos dados pessoais:

1. A Comunicação/divulgação dos dados pessoais só será realizada dentro dos termos da lei permite e obriga. Caso, contrário será solicitado o consentimento ao titular dos dados para a comunicação/divulgação dos dados pessoais.
2. A IPSS no âmbito da sua atividade realiza contratos de subcontratação com as seguintes entidades:
    i. Seguros
    ii. Higiene e Segurança no Trabalho
    iii. Advogado
    iv. Empresa que fornece o serviço para controlo biométrico
3. A IPSS realiza contratos de subcontratação, tendo em conta o âmbito e natureza da prestação de serviços com quem partilha dados pessoais que asseguram cumprir a regulamentação europeia e nacional no que respeita a este domínio.
4. As comunicações dos dados pessoais só serão efetuadas mediante autorização e conhecimento dos titulares dos mesmos ou dos responsáveis legais. Quando os dados pessoais recolhidos dizem respeito a crianças a comunicação/divulgação dos dados pessoais só serão efetuados aos pais ou as responsáveis legais das mesmas.

VII. Tempo de armazenamento dos dados

1. Os dados que dizem respeito a obrigações estatais
    i. Os dados que respeitam à Segurança Social e Autoridade Tributária, isto é, os livros, registos contabilísticos e os respetivos documentos de suporte devem ser armazenados durante o prazo de 12 anos, segundo o artigo 123.º, nº 4 do CIRC.
    ii. Os dados dos utentes são armazenados durante 20 anos.

VIII. Procedimentos da segurança dos dados

1. Os dados que se encontram armazenados em formato papel, localizados nos Serviços Administrativos e Financeiros e nas Salas
    i. Só as pessoas autorizadas poderão ter acesso a estes locais;
    ii. Encontram-se protegidos por um cadeado.

2. Os dados que se encontram armazenados em formato digital
    i. Controlo e registo de acesso, para a criação e eliminação.
    ii. Encriptação de e-mails.
    iii. Alteração cíclica das passwords.
3. A IPSS toma todas as precauções necessárias e legalmente existentes para garantir a proteção dos dados recolhidos.

IX. Responsabilidade/Contato em matéria de proteção de dados

1. Sempre que o titular dos dados quiser contactar a Associação no âmbito destas questões poderá fazê-lo nas instalações ou através do seguinte e-mail: _____
2. Se ao titular dos dados pessoais suscitar alguma dúvida de como dos procedimentos adotados em matéria de proteção de dados proteção dos dados deverá contatar o responsável XX, através dos seguintes mecanismos: email, morada, contato telefónico, fax

X. Direitos dos titulares dos dados

1. Em consonância com legislação vigente os titulares dos dados têm com conjunto de direitos que serão respeitados pela organização XX, designadamente:
    i. O direito de acesso
    ii. O direito de retificação
    iii. O direito de acesso
    iv. O direito de retificação
    v. O direito ao apagamento dos dados («direito ao esquecimento»)
    vi. O direito à limitação do tratamento
    vii. O direito à portabilidade dos dados
2. A organização [redacted] tem um responsável pelo tratamento dos dados que tem a obrigação comunicar a cada titular dos dados pessoais que tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento dos mesmos.
3. Relativamente ao direito ao esquecimento e portabilidade existem dados que pela sua natureza e tendo em conta a natureza do serviço não podem ser apagados ou não podem ser apagados em determinados períodos de tempo, sendo necessário aferir

caso a caso. Note-se que estes direitos não são absolutos, portanto, tem que ser aferidos tendo em conta o contexto.

XI. Disposições finais:

1. O presente documento aplica-se a todos os indivíduos sobre os quais a IPSS possua dados pessoais sobre os mesmos, quer sejam recolhidas junto dos titulares dos dados ou quando não é recolhida junto do titular dos dados. A IPSS reserva-se do direito de alterar a Política de Proteção dos Dados e de Privacidade a qualquer momento, não deixando de respeitar os direitos do titular dos dados de acordo com a legislação em vigor.
2. A IPSS tem o direito a alterar o Regulamento sempre que entender, a qualquer momento, por qualquer motivo, sem aviso prévio.
3. A organização pode mandar lembretes por e-mail, carta, notificações com as alterações das condições materiais, mas deve consultar com frequência as condições nestas matérias.

20. Anexo 10 – Tabela de auxílio na implementação do Regulamento

	Tipos de dados	Dados dos docs	Base Legal	Consent.	Dados do menor	Finalidade	Duração	Armazenamento	Formato
Fotografias					x	Prestação serviço	indeterminado	Sala	papel
Boletim de Vacinas	Relativos à saúde	Nome, data de nascimento, sexo, nº de utente, filiação, naturalidade, freguesia, concelho, distrito	Art. 15.º, al. j) Portaria 262/2011		x	Prestação serviço	até a criança permanecer + tempo logístico para os eliminar	Sala	papel
Boletim de saúde	Relativos à saúde				x	Prestação serviço	até a criança permanecer + tempo logístico para os eliminar	Sala	papel
Cartão de utente da criança	Pessoal	Número identificação			x	Prestação serviço	até a criança permanecer + tempo logístico para os eliminar	Sala	papel
Declaração médica comprovando a situação clínica	Relativos à saúde		Art. 15.º, al. h) Portaria 262/2011		x	Prestação serviço	até a criança permanecer + tempo logístico para os eliminar	Sala	papel
Relatório médico	Relativos à saúde					Prestação serviço	até a criança permanecer + tempo logístico para os eliminar	Sala	papel

BI's das pessoas a quem a criança pode ser entregue	Identificação pessoal	Nome, Sexo, Altura, Data de nascimento, Nacionalidade, Nº Identificação Civil, Fotografia, Filiação, NIF, NISS, Nº de utente de saúde	Art. 14.º, Portaria 262/2011			Prestação serviço	até a criança permanecer + tempo logístico para os eliminar	Sala	papel
BI's do agregado familiar/responsáveis legais	Identificação pessoal	Nome, Sexo, Altura, Data de nascimento, Nacionalidade, Nº Identificação Civil, Fotografia, Filiação, NIF, NISS, Nº de utente de saúde	Art. 14.º, Portaria 262/2011			Prestação serviço	indeterminado	Sala	papel
NIF da criança	Identificação pessoal	Nº	Art. 14, Portaria 262/2011		x	Prestação serviço	indeterminado	Secretaria	papel+digital
Visto de autorização de residência						Prestação serviço	indeterminado	Secretaria	papel+digital
Boletim de Nascimento/BI/CC da criança	Pessoal		Art. 14.º, Portaria 262/2011		x	Prestação serviço	indeterminado	Secretaria	papel+digital
NISS do agregado familiar/responsáveis legais	Pessoal	Nº	Art. 14.º, Portaria 262/2011		x	Prestação serviço	8 anos + tempo logístico para eliminar	Secretaria	papel+digital
Recibo de vencimento dos familiares	Pessoal/económico	Entidade empregadora, nome completo, número de	Art. 14.º, Portaria 262/2011			Prestação serviço	8 anos + tempo logístico para eliminar	Secretaria	papel +digital

		identificação na empresa (caso o possua), IBAN e banco, NIF e função ou categoria profissional, data do recibo, subsídio de alimentação, descontos, Regime de tributação							
Morada da criança	Localização		Art. 14.º, Portaria 262/2011			Prestação serviço	8 anos + tempo logístico para eliminar	Secretaria	papel+digital
Profissão dos pais (2)	Profissional					Prestação serviço	até a criança permanecer na creche + tempo logístico para o eliminar	Secretaria	papel+digital
Mail (2)	Identificação					Prestação serviço	até a criança permanecer na creche + tempo logístico para o eliminar	Secretaria	papel+digital
Morada (2)	Localização					Prestação serviço	até a criança permanecer na creche + tempo logístico para o eliminar	Secretaria	papel+digital
Telefone e telemóvel (2)	Pessoal/económico					Prestação serviço	até a criança permanecer na creche + tempo logístico para o eliminar	Secretaria	papel+digital

Local de Emprego	Profissional					Prestação serviço	até a criança permanecer na creche + tempo logístico para o eliminar	Secretaria	papel+digital
Habilitações Literárias	Profissional/escolar		Sem fundamento legal			Prestação serviço	até a criança permanecer na creche + tempo logístico para o eliminar	Secretaria	papel+digital
Se tem irmãos a frequentar o estabelecimento			Funcionamento da Creche			Prestação serviço	até a criança permanecer na creche + tempo logístico para o eliminar	Secretaria	papel+digital
Se é filho de BV			Funcionamento da Creche			Prestação serviço	até a criança permanecer na creche + tempo logístico para o eliminar	Secretaria	papel+digital
Se necessita de apoio especial						Prestação serviço	até a criança permanecer na creche + tempo logístico para o eliminar	Secretaria	papel+digital
Caraterização do Agregado Familiar	Económico	Nome, idade, parentesco, profissão e rendimento mensal líquido	Art. 4.º, Portaria 196-A/2015			Prestação serviço	8 anos + tempo logístico para eliminar	Secretaria	papel+digital
		Encargos com habitação				Prestação serviço	8 anos + tempo logístico para eliminar		

		Declaração de IRS e comprovativo de liquidação				Prestação serviço	8 anos + tempo logístico para eliminar		
		Recibo de vencimento dos familiares				Prestação serviço	8 anos + tempo logístico para eliminar		
		BI dos pais; NISS/NIF da criança				Prestação serviço	8 anos + tempo logístico para eliminar		
Se beneficia do RSI	Económico		Art. 4.º, Portaria 196-A/2015			Prestação serviço	8 anos + tempo logístico para eliminar	Secretaria	papel+digital
Tipo de habitação do AG e a propriedade do mesmo	Económico		Art. 5,1, al. b) Portaria 196-A/2015			Prestação serviço	8 anos + tempo logístico para eliminar	Secretaria	papel+digital
Encargos	Económico	Habitação, saúde e outros	Saúde: Portaria 196-A/2015, Art. 5.1, al. d); Transporte: Portaria 196-A/2015, Art. 5.1, al. c)			Prestação serviço	8 anos + tempo logístico para eliminar	Secretaria	papel+digital
Impressão digital	Biométrico			x		Proteção de crianças e instalações	1 ano	Programa	digital
Nome dos trabalhadores	Identificação pessoal					Execução do contrato		Secretaria	papel+digital
NIF dos trabalhadores	Identificação pessoal					Execução do contrato		Secretaria	papel+digital

NISS dos trabalhadores	Identificação pessoal					Execução do contrato		Secretaria	papel+digital
NIB/IBAN	Económico					Proteção de crianças, instalações e controlo de assiduidade		Secretaria	papel+digital
Impressão digital dos trabalhadores	Biométrico		Art. 18.º do Código de Trabalho				1 ano	Programa	digital