UNIVERSIDADE D
COIMBRA

Ana Sofia Medeiros Melo

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

UM NOVO PARADIGMA REGULATÓRIO

Dissertação no âmbito do Mestrado em Ciências Jurídico-Forenses, orientada pelo Professor Doutor Pedro António Pimenta Costa Gonçalves e apresentada à Faculdade de Direito da Universidade de Coimbra.

Janeiro de 2019

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

Um Novo Paradigma Regulatório

Ana Sofia Medeiros Melo

Dissertação no âmbito do Mestrado em Ciências Jurídico-Forenses, orientada pelo Professor Doutor Pedro António Pimenta Costa Gonçalves e apresentada à Faculdade de Direito da Universidade de Coimbra.

Janeiro de 2019

UNIVERSIDADE D
COIMBRA

Aos meus pais,

que me obrigam a não desistir de lutar

"Fazer tudo da nossa parte
como se Deus não pudesse fazer nada e, depois,
pôr toda a nossa esperança em Deus como se,
da nossa parte, não tivéssemos feito nada."

(Inácio de Loyola)

AGRADECIMENTOS

Aqui chegados cumpre dizer obrigada a todos os que mudaram a minha vida para melhor, ao que de bom, muito bom, a vida me traz e ao resto, porque tem me feito correr atrás dos meus sonhos, ao que tenho e ao que sou, aos que me deram a mão, aos que acrescentaram luz aos dias e aos que me fizeram perceber a pessoa que quero ser.

Em primeiro lugar, ao Senhor Professor Doutor Pedro António Pimenta Costa Gonçalves, que aceitou orientar a presente dissertação, pela sua sempre rápida e afável resposta a todas as minhas comunicações, bem como pela sua cuidadosa observação ao meu trabalho. Permite-se afirmar que num mundo em que é difícil fazer escolhas, esta era uma das escolhas que não me podia faltar fazer.

Aos meus pais, Helena e José, a quem devo a pessoa que me tornei, fruto de uma conjugação de valores e ideias tanto maternos como paternos. A eles, que em todos os momentos tanto do percurso académico como ao longo da vida, revelaram-se um pilar responsável por toda a carga que a minha estrutura emocional acarreta. Pais, que sempre me indicaram o rumo, quando eu (tantas vezes) achei-me perdida. A eles que dão sentido a cada coisa da minha vida, que para além de conhecerem o caminho, percorreram-no até ao fim de mãos dadas comigo. Eles, mais do que eu, acreditaram e continuam a acreditar no meu potencial.

Aos meus irmãos e aos meus cunhados, que sempre me indicaram que o sentido é em frente e que, apesar de tudo, tal como os nossos pais os transmitiram a fé é o que sempre temos a nosso favor. Um "*não te preocupes que eu estou sempre aqui*" nos dias certos, uma palavra de alento, um gesto de amor, uma frase de coragem. Obrigado à mão cheia de esperança que depositaram em mim, e por tantas vezes aliviarem a força do aperto no coração.

Aos meus sobrinhos, que na ingenuidade dos seus olhos encontro o verdadeiro significado de felicidade, e que ganham o estatuto de pessoas-luz de toda esta caminhada. A presença deles enche-me os dias de amor, e é com este Amor que goza de maior pureza, que me sinto feliz.

À restante família, pelo apoio incondicional e por me ajudar a perceber que sou tão feliz com o "pouco" que tenho. Por fazerem me sentir fenomenal e que, sem saber, fazem magia com a sua alegria.

Ao Doutor Ricardo do Nascimento Cabral um sentido obrigado por ter lançado a primeira pedra nesta obra, por me ter impulsionado na pesquisa e investigação na área da proteção de dados. E, por desde o início, ter incentivado a frequência neste Mestrado. Não posso nunca deixar de agradecer aos restantes colegas de trabalho, sem distinções, pelas condições proporcionadas e pelo apoio prestado.

Às amigas que Coimbra me deu, pela inabalável força dada ao longo dos últimos 6 anos, e aos restantes amigos, amigos de A grande que sabem (*sempre*) como me reconfortar.

Ao que o Direito e a ilha juntaram, diga-se ao Bruno, à Carolina, à Matilde, à Joana e à Rita, por acreditarem, por nunca me deixaram tirar da cabeça o que levo no coração. Quando eu queria muito que desse certo, eles acreditaram, sempre, que daria certo! São uma luz que se soma à minha força.

Estes 6 anos chegaram para perceber que o que importa de verdade é lutar para alcançar os nossos sonhos, é saber quem são os que caminham ao nosso lado, sem filtros. É ter a coragem de não desistirmos de nós. É saber levantar e dar sempre a volta por cima. É decidir que não importa onde (em Coimbra ou na ilha), não importa quando, não importa como, o plano é um só: *nem tudo vale tanto, e quase nada vale tanto*.

Neste e noutros desafios da minha vida, *obrigada, muito obrigada*, será por vezes a mais reconhecida homenagem, num mundo em que *só não somos nada*.

RESUMO

A presente dissertação, encetada numa época em que o desenvolvimento tecnológico desafia os direitos fundamentais, pretende enquadrar e analisar o novo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (Regulamento Geral de Proteção de Dados Pessoais).

Para tanto foi levado a cabo a divisão em duas partes do presente trabalho. A montante, a proteção de dados enquanto direito fundamental e alvo de uma evolução legislativa concisa, por força da qual surgiu o RGPD.

De facto, foi com base na CEDH e na Convenção 108, no contexto do Conselho da Europa, que a União Europeia e os países da Europa desenvolveram o *direito à proteção de dados*. No caso de Portugal, consagrando inclusive constitucionalmente (através do artigo 35.º da CRP), e no âmbito da Direito da União Europeia através da Diretiva 95/46/CE, a base para o atual panorama do direito da proteção de dados.

Essa diretiva, embora inovatória, não conseguiu atingir a harmonização pretendida. A solução foi o Parlamento Europeu e o Conselho socorrem-se da base legal do art. 16.º do TFUE e aprovarem o Regulamento Geral de Proteção de Dados, diretamente aplicável nos Estados-Membros, que teve como objetivo primário a centralização normativa de modo a fomentar a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Daí que num segundo momento são apresentadas as inovações que o RGPD trouxe e que afetam todos os agentes económicos.

O RGPD incorpora muito daquilo que já eram os direitos e obrigações consagrados na anterior diretiva. As diferenças essenciais encontram-se no modelo sancionatório (20 milhões de euros ou 4% da faturação anual) e a autorresponsabilização, que obrigaram muitas empresas a preocuparem-se com o tema pela primeira vez.

Assim, o RGPD o que exige é uma mudança de atitude por parte de todos os agentes económicos: *Cidadãos, Organizações e Estado*, para que se consiga promover a

sensibilização e a compreensão da existência de um verdadeiro direito à proteção de dados pessoais.

Palavras-Chave: Proteção de Dados, Regulamento Geral de Proteção de Dados, Direito da União Europeia, Convenção 108, Diretiva 95/46/CE, Direito à Privacidade, Dados Pessoais.

ABSTRACT

This dissertation, made in an era when the technological development poses a challenge to fundamental rights, intends to frame and analyze the new Regulation (EU) 2016/679, from the European Parliament and the Council of 27th April 2016 (General Data Protection Regulation).

For that purpose, the work was split in two parts. Upstream, data protection as a fundamental right, the target of a concise legislative evolution, from which GDPR was born.

In fact, it was based on the ECHR and the Convention 108, amidst the Council of Europe, that the European Union and the European countries developed the *right to data protection*. In the Portuguese case, it was even constitutionally elevated (through article 35 of the Portuguese constitution), and in the European Union law through the Directive 95/46/CE, the basis of the current outlook of the data protection law.

That directive, although with new solutions, was unable to achieve the harmonization that was wished for. The solution was for the European Parliament and Council to use article 16 TFEU to approve the General Data Protection Regulation, directly applicable in the Member-states, which had the main purpose of centralizing the rules insofar as to promote the protection of individual persons as to their personal data processing and free movement of those data.

Hence, in a second moment the innovations brought by GDPR, which affect all the economic agents, are presented.

GDPR encompasses much of what were already the rights and obligations enshrined in the former directive. The essential differences are found in the sanctions framework (20 Million euros or 4% of turnover) and accountability, which forced many companies to worry about the topic for the first time.

Therefore, what GDPR demands is an attitude shift of all economic agents: *Citizens, Organizations and State*, in order to promote the awareness of a true right to personal data protection.

Keywords: Data Protection, General Data Protection Regulation, European Union Law, Convention 108, Directive 95/46/CE, Right to Privacy, Personal Data.

SIGLAS E ABREVIATURAS

AC. - Acórdão

ACS. - Acórdãos

AEPD - Autoridade Europeia para a Proteção de Dados

AIPD - Avaliação de Impacto sobre a Proteção de Dados

AL. – Alínea

ALS. - Alíneas

ART. – Artigo

ARTS. - Artigos

CC - Código Civil

CCTV – Closed-circuit television (circuito fechado de televisão)

CDFUE - Carta dos Direitos Fundamentais da União Europeia

CE - Conselho Europeu

CEE – Comunidade Económica Europeia

CEDH - Convenção Europeia dos Direitos do Homem

CF. - Confira

CNPD - Comissão Nacional de Proteção de Dados

CP - Código Penal

CRP - Constituição da República Portuguesa

DPO - Data Protection Officer

ECHR – European Court of Human Rights

EPD - Encarregado de Proteção de Dados

EPE – Entidade Pública Empresarial

EU – European Union

GDPR – General Data Protection Regulation

GTA29 - Grupo de Trabalho do Artigo 29

IT – Informação tecnológica

N.º - Número

N.ºs - Números

P. - Página

P. EX. - Por exemplo

PROC. - Processo

RGCO - Regime Geral das Contra-Ordenações

RGPD - Regulamento Geral de Proteção de Dados

SS - Seguintes

TC - Tribunal Constitucional

TEDH – Tribunal Europeu dos Direitos do Homem

TFEU – Treaty on the Functioning of the European Union

TFUE - Tratado sobre o Funcionamento da União Europeia

TJUE - Tribunal de Justiça da União Europeia

UE - União Europeia

V. – *Versus*

VOL. – Volume

ÍNDICE

INTRODUÇÃO

A presente dissertação de Mestrado, do Curso de Mestrado em Ciências Jurídico-Forenses, da Faculdade de Direito da Universidade de Coimbra, tem como principal objetivo abordar a temática do Regulamento Geral de Proteção de Dados, Regulamento n.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, no que concerne às principais implicações e mudanças que se assistem na União Europeia. Mudanças estas que levam a que as organizações caminhem para a implementação de uma solução de *compliance*.

A principal razão que nos impulsionou para a escolha do tema foi as repercussões em termos de exequibilidade prática do mesmo, até porque tendo em conta a dimensão de tal ato legislativo não é de prever que o este se fique pela mera discussão teórica e abstrata. Dada à consabida complexidade e as consequências práticas que deste Regulamento podem decorrer fomos assomados pela certeza quanto à importância do tema que nos propusemos investigar. Não se esconde ainda que a recente experiência profissional foi determinante nesta opção, seja pela perceção da crescente relevância da matéria, seja pelas oportunidades que tal experiência tem criado.

Este é um tema que a todos atinge, e que de uma maneira ou outra se encontra presente diariamente na vida de cada um de nós. Veja-se que dada a velocidade que a tecnologia mudou, vivemos todos num mundo conectado, no entanto isto não nos permite afirmar que devemos arredar da privacidade devida. Até como Alan Westin[1] afirmou *"(...) cada indivíduo está continuamente empenhado num processo de ajuste pessoal em que mantém um equilíbrio entre o desejo de privacidade com o desejo de divulgação e comunicação (...)."*

Volvidos mais de vinte anos desde a Diretiva 95/46/CE, a União Europeia, entendeu ser tempo de alargar horizontes e empreender uma viagem em busca de abordagens atuais, reforçando assim a matéria de proteção de dados pessoais, adotando o RGPD que tem como objetivo principal contribuir para a realização de um espaço de liberdade, segurança, justiça e de uma união económica, para o progresso económico e social, consolidação e a

[1] WESTIN, Alan, *Privacy and Freedom*, 1967.

convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.

A presente dissertação encontra-se dividida em duas partes, respetivamente, a Parte I (enquadramento) e a Parte II (o Regulamento Geral de Proteção de Dados), cada uma delas integrada por capítulos e alguns destes por secções.

Outra não poderia ser a ordem de exposição das matérias. Na parte I iniciaremos a abordagem, em termos genéricos, através do capítulo I, da temática da proteção de dados enquanto direito fundamental tanto no ordenamento jurídico português, como no quadro legal europeu, passando à evolução legislativa sentida na presente matéria, no capítulo II.

Enquadramento este necessário para, que na parte II se possa tratar e expor as principais inovações do Regulamento, e dos problemas que a sua aplicação suscita e continuará a suscitar.

No âmbito da dissertação, de forma cuidada, selecionámos jurisprudência pertinente, embora os Acórdãos citados tenham por base a diretiva já revogada, as interpretações feitas continuam a ser válidas para a interpretação e aplicação do RGPD.

O momento em que se avança com a dissertação não nos permite assentar cegamente nas soluções neles consagradas, em face do caráter aberto de algumas delas. A opção passou antes pela apresentação dos traços gerais do regime, dos princípios ali refletidos, do conjunto de direitos dos titulares firmados, e ainda das responsabilidades do responsável pelo tratamento e do subcontratante. Depois de compreendidos estes elementos avançou-se para a matéria que, em muito, tem controvertido, a das sanções. E, por último, os mecanismos de tutela judicial e de acionamento da responsabilidade.

§ PARTE I §

ENQUADRAMENTO

CAPÍTULO I: CONTEXTUALIZAÇÃO DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS

1. Consagração na Constituição da República Portuguesa

Portugal foi o primeiro e um dos raros países a conferir dignidade constitucional à proteção de dados pessoais. Logo na CRP aprovada em 2 de abril de 1976, que foi sucessivamente atualizada, ampliada e reforçada pelas leis de revisão de 1982 e 1989, e por fim, na revisão constitucional de 1997 dedicou um artigo à matéria da proteção de dados pessoais, nomeadamente o seu art. 35.º[2].

Conclui-se que a matéria de proteção de dados em Portugal não é um tema desconhecido[3], no entanto não goza da preocupação devida, quando comparado a outras países europeus, nomeadamente a Alemanha.

Verdade é que, em Portugal, as preocupações relativas à proteção de dados pessoais passaram a estar em maior evidência, só com a entrada em vigor do RGPD.

2. Presença em diplomas europeus

A proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais, é um direito que se encontra plasmado tanto no art. 8.º, n. º1, da CDFUE[4] como no art. 8.º da CEDH[5].

Este direito coloca em prática um sistema de ponderação de modo a salvaguardar os indivíduos sempre que os seus dados pessoais são tratados, por isso não é um direito absoluto

[2] Cf. Anexo 1.
[3] O direito à reserva da intimidade da vida privada foi consagrado pela primeira vez em Portugal no CC de 1966.
[4] Carta dos Direitos Fundamentais da União Europeia, adotada em 7/12/2000.
[5] Convenção Europeia dos Direitos do Homem, adotada pelo Conselho da Europa, em 4/11/1950.

mas deve ser considerado em relação à sua função, veja-se neste sentido PAULO MOTA PINTO, quando afirma que a *"tutela da privacy é caracterizada por uma fundamental contraposição: de um lado, o interesse do indivíduo na sua privacidade, isto é, em subtrair-se à atenção dos outros, em impedir o acesso a si próprio ou em obstar à tomada de conhecimento ou à divulgação de informação pessoal (...), de outro lado, fundamentalmente o interesse em conhecer e em divulgar a informação conhecida (...)"*[6].

Para além disso, o regime europeu de proteção de dados pessoais, veio a ser consideravelmente reforçado com a consagração do art. 16.º do TFUE[7] em que o seu n.º 1 nos enuncia que *"todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito".* Este artigo estabeleceu, assim, pela primeira vez uma base jurídica expressamente aplicável aos tratamentos de dados pessoais pelos Estados-Membros.[8]

[6] PINTO, Paulo Mota, *O Direito à Reserva sobre a Intimidade da Vida Privada*, Boletim da Faculdade de Direito - Universidade de Coimbra LXIX, 1993, p. 508 e 509.
[7] Tratado de Funcionamento da União Europeia.
[8] Cf. GALVÃO, Luís Neto, *Comentário ao artigo 16.º do TFUE in* PORTO, Manuel Lopes e ANASTÁCIO, Gonçalo (coordenadores), *Tratado de Lisboa Anotado e Comentado*, 2012, p. 252.

CAPÍTULO II: EVOLUÇÃO LEGISLATIVA

1. Convenção para a proteção das pessoas singulares relativamente ao tratamento automatizado dos dados de carácter pessoal

Com o surgimento da tecnologia da informação na década de 1960, disparou a necessidade de regras capazes de proteger os indivíduos e em consequência os seus dados pessoais.

Assim, em meados da década de 1970, o Comité de Ministros do Conselho da Europa adotou várias resoluções sobre proteção de dados pessoais, referindo-se ao art. 8.º da CEDH. A 28 de janeiro de 1981, a Convenção para a proteção das pessoas relativamente ao tratamento automático de dados pessoais (Convenção 108) foi assinada. A Convenção 108 aplica-se a todos os tratamentos de dados pessoais efetuados pelo sector público ou privado, incluindo o tratamento realizado pelas autoridades policiais ou judiciárias, e visa proteger os cidadãos contra os abusos que possam surgir a recolha e tratamento de dados pessoais.

A esta Convenção foi adotado um Protocolo Adicional, em 2001, que introduziu disposições relativas aos fluxos de dados transfronteiras para países terceiros, e ao estabelecimento obrigatório de autoridades nacionais de supervisão da proteção de dados.

2. Diretiva 95/46/CE

De 1995 a maio de 2018, o principal instrumento jurídico da UE em matéria de proteção de dados foi a 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. A Diretiva de Proteção de Dados foi inicialmente baseada na base legal do mercado interno e na necessidade de aproximar as leis nacionais para que a livre circulação de dados dentro da UE não fosse inibida[9], tomando sempre como base o já disposto na Convenção 108.

[9] Ainda não constava dos tratados da CEE qualquer norma de natureza semelhante ao art. 16.º do TFUE.

Contudo, com a adoção da Diretiva, a harmonização que se pretendia não foi alcançada. Ora, as diretivas carecem de transposição interna pelos Estados-Membros. Deste modo, os Estados-Membros ficaram dotados de margem de discricionariedade na sua transposição, o que originou uma transposição heterogénea nos diferentes Estados-Membros.

A desarmonização sentida na UE e as mudanças significativas na tecnologia da informação levaram a que se repensasse a legislação em vigor, o que motivou a reforma e a adoção do Regulamento Geral de Proteção de Dados, em Abril de 2016, que visa criar um espaço legislativo uniforme e harmonizado.

§ PARTE II §

O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

CAPÍTULO I: NOTA INTRODUTÓRIA

1. O processo de adoção

O fundamento legal para a adoção do RGPD encontra-se plasmado no n.º 2, do art. 16.º do TFUE, nos seguintes termos:

"(...) 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 atos.*** *(...)".*[10]

A negociação do RGPD demonstrou uma grande complexidade de mobilização de meios[11], até porque se trata de uma matéria com projeção social, cultural e financeira de grande dimensão.

Após anos de acesa discussão[12], a ratificação formal do acordo previamente obtido pelo Conselho deu-se a 12 de fevereiro de 2016, e a aprovação definitiva pelo Plenário do Parlamento Europeu deu-se a 14 de abril de 2016, com um período de *"vacatio legis"* de dois anos, tornando-se plenamente aplicável em 25 de maio de 2018, quando a Diretiva 95/46/CE foi revogada.

[10] Negrito nosso.
[11] Neste sentido veja-se MAÑAS, José Luís Piñar, *Antecedentes e processo de reforma sobre protección de datos personales en la Unión Europea in Regulamento General de Protección de Datos. Hacia un nuevo modelo europeo de protección de datos*, 2016, p. 49.
[12] Os debates tiveram início em 2009, contudo a proposta de Regulamento só foi publicada pela Comissão em janeiro de 2012, dando início a um longo processo legislativo de negociações entre o Parlamento Europeu e o Conselho da UE.

2. Um Regulamento, porquê?

Nos termos do disposto no 2.º parágrafo do art. 288.º do TFUE, e como, aliás, consta do Regulamento, este *"(…) é **obrigatório** em todos os seus elementos e diretamente aplicável em todos os Estados membros".*[13]

Trata-se, portanto, de um ato legislativo da UE, que, pela sua natureza, é parte integrante do direito interno e produz efeito direto simultaneamente nas relações verticais e horizontais, sem necessidade de qualquer mecanismo de receção[14] .

No entanto, mesmo que o RGPD seja diretamente aplicável, espera-se que os Estados Membros atualizem as leis nacionais de proteção de dados existentes para que se alinhem plenamente com o Regulamento, o que reflete alguma margem de discricionariedade para disposições específicas[15], neste sentido importa sublinhar ALEXANDRE SOUSA PINHEIRO *"(...) não pensamos que o RGPD possa ser considerado como um texto paradigmaticamente unificador da matéria da proteção de dados no domínio da União Europeia. Esta conclusão é extraída pela abertura legislativa fornecida aos Estados-Membros, não pela atuação das autoridades de controlo cuja ação está sujeita ao procedimento do controlo da coerência*."[16]

3. Objeto e objetivos

O RGPD prevê um conjunto único de regras consistentes de proteção de dados em toda a UE, estabelecendo um ambiente de segurança jurídica do qual os operadores económicos e os titulares dos dados podem beneficiar, o que contribuiu para a modernização da legislação da UE, tornando-a adequada para proteger os direitos fundamentais no contexto dos desafios económicos e sociais da era digital. Verifica-se, portanto, a harmonização da legislação, coerência do tratamento de dados pessoas e segurança jurídica.

[13] Negrito nosso.
[14] Cf., por todos, MACHADO, Jónatas E. M., *Direito da União Europeia*, 2010, p. 199-201, e HENRIQUES, Miguel Gorjão, *Direito da União Europeia*, 2014, p. 296.
[15] Muitas delas de extrema relevância, p. ex. os Estados-Membros podem introduzir limitações às obrigações e direitos previstos no RGPD (considerando 85 a 91 e art. 23.º).
[16] PINHEIRO, Alexandre Sousa, *Comentário ao Regulamento Geral de Proteção de Dados*, 2018, p. 21.

As novas regras e obrigações impostas às organizações, farão com que a matéria de proteção de dados passe a ser levada em conta na sua gestão.

4. Âmbito de aplicação

4.1.Material

Segundo o art. 2.º n.º 1, o RGPD aplica-se ao tratamento[17] de dados pessoais[18] realizados por meios total ou parcialmente automatizados, ou por meios não automatizados, desde que contidos em ficheiros ou a eles destinados.

Em conjugação ainda com o n.º 2 importa delimitar negativamente o seu âmbito. Assim, encontram-se excluídos do âmbito de aplicação do Regulamento:

a. O tratamento de dados efetuado no exercício de atividades não sujeitas à aplicação do direito da UE[19];
b. O tratamento de dados efetuado pelos Estados-Membros no exercício de atividades relativas à política externa e de segurança comum;
c. O tratamento efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública;
d. Os "dados anonimizados", ou seja, os dados relativos a uma pessoa identificada ou identificável que não pode, razoavelmente, voltar a ser identificada ou identificável[20];
e. Os dados das pessoas coletivas;

[17] Definição constante do art. 4.º n.º 2.
[18] Cf. art. 4.º n.º 1, saliente-se que o legislador optou por uma definição do conceito de dados pessoais bastante ampla que abrange qualquer informação, de qualquer natureza e independentemente do suporte.
[19] P. ex. no âmbito de medidas de segurança nacional.
[20] A informação pessoal identificável é irreversivelmente alterada, de tal forma que a informação pessoal identificável principal não pode mais ser identificada direta ou indiretamente, quer pelo responsável pelo tratamento, quer por terceiros.

f. O tratamento de dados efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas[21], ou seja, sem ligação a uma atividade profissional ou comercial[22].

Em relação a este último ponto, importa apresentar o sentido da jurisprudência proveniente do TJUE, que nos permite clarificar que situações se enquadram no âmbito de aplicação material. O Ac. de 6 de novembro de 2003, Lindqvist[23], sustenta que " *a operação que consiste na referência, feita numa página da Internet, a várias pessoas e a sua identificação pelo nome ou por outros meios, por exemplo, o número de telefone ou informações relativas às suas condições de trabalho e aos seus passatempos, constitui um «tratamento de dados pessoais por meios total ou parcialmente automatizados» na aceção do artigo 3.°, n.º 1, da Diretiva (...)".*

Ou, sublinhe-se o Ac. de 11 de Dezembro de 2014, Ryneš, em que Ryneš captou a imagem de dois indivíduos que quebraram as janelas da sua casa através do sistema de vigilância CCTV doméstico que havia instalado. A gravação foi entregue à polícia e usada durante o processo criminal. Para o TJUE os tratamentos em causa não se integravam na "*household exemption*", "*uma videovigilância (...) ainda que parcialmente, ao espaço público e, por esse motivo, se dirige para fora da esfera privada da pessoa que procede do tratamento de dados por esse meio, não pode ser considerada uma atividade exclusivamente «pessoal ou doméstica» (...).*"

Daí que a decisão tenha sido no sentido de que "*(...)a exploração de um sistema de câmara que dá lugar a uma gravação vídeo de pessoas, guardada num dispositivo de gravação contínua, como um disco rígido, sistema esse instalado por uma pessoa singular na sua casa de família para proteger os bens, a saúde e a vida dos proprietários dessa casa e que vigia igualmente o espaço público,* ***não constitui um tratamento de dados efetuado no exercício de atividades exclusivamente pessoais ou domésticas, na aceção desta disposição."*** [24]

[21] A compreensão desta disposição obriga à avaliação de doutrina do GTA29 e do considerando 18 do RGPD (acompanhado pela recomendação do AEPD em adenda ao Parecer n.º 3/2015).
[22] P. ex. operações realizadas na lista de contactos do telemóvel pessoal.
[23] Merece igualmente destaque o Ac. TJUE, de 16 de Dezembro de 2008, proc. C-73/07, Satamedia.
[24] Negrito nosso.

4.2.Territorial

O âmbito de aplicação territorial do RGPD está relacionado com a localização do estabelecimento do responsável pelo tratamento ou do subcontratante, assim aplica-se a empresas estabelecidas na UE e aplica-se também a responsáveis pelo tratamento e a subcontratantes não estabelecidos na UE que oferecem bens ou serviços[25] a titulares de dados residentes na UE ou que procedam ao controlo do seu comportamento, e por último a um responsável pelo tratamento estabelecido não na UE, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público.

Tal opção legislativa justifica-se porque várias empresas de tecnologia estrangeiras têm uma participação chave no mercado europeu, assim sujeitar estas organizações às regras de proteção de dados da UE é importante para garantir a proteção dos indivíduos, bem como para garantir condições equitativas. Ora, o seu âmbito de aplicação territorial acarreta **consequências a nível global.**

[25] O mero facto de estar disponível um sítio web do responsável pelo tratamento ou subcontratante, um endereço eletrónico ou outro tipo de contactos, não é suficiente para determinar a intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da UE. Contudo existem indicadores determinantes, p. ex. a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros.

CAPÍTULO II: PRINCÍPIOS

O art. 5.º n.º 1 do RGPD estabelece um conjunto de princípios, de respeito obrigatório, que regem o tratamento de dados pessoais.

Conforme dispõe o art. 5.º n.º 2 o responsável pelo tratamento é o centro de imputação de obrigações e de responsabilidades, ou seja, para além de cumprir os princípios constantes do RGPD terá de o comprovar- *accountability*[26].

Esta disposição legal é a bússola que deverá nortear todo o comportamento dos responsáveis pelo tratamento de dados pessoais, até porque opera como uma "*Constituição do RGPD*"[27]. De seguida, analisaremos cada um destes princípios:

1. Licitude, lealdade e transparência

É a base de todo o sistema consagrado no Regulamento. De acordo com o princípio da "*licitude, lealdade, transparência*" constante da al. a) do n.º 1 do art. 5.º os dados pessoais devem ser *"objeto de um tratamento lícito, leal e transparente".*

Diga-se, ***"****os dados tratados deverão ser associados ao respetivo fundamento jurídico do tratamento, mantendo-se disponíveis as evidências de legitimidade (...). Deverão, ainda, ser disponibilizadas aos titulares dos dados pessoais as informações previstas nos arts. 13.º e 14.º*[28]*(...). Para efetivação destes princípios, o responsável pelo tratamento poderá ceder certo controlo, a todo o tempo, aos titulares dos dados que sobre os mesmos estejam tratados, e com a possibilidade de prestação e retirada do consentimento, ou de oposição ao tratamento; assegurando, contudo que cada titular apenas terá acesso aos seus próprios dados."*[29]

[26] No mesmo sentido, cf. GRUPO DE TRABALHO DO ARTIGO 29 "Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»", (WP 169), adotado em 16/02/2010, p. 4 e 11.
[27] Expressão utilizada *in* PINHEIRO, Alexandre Sousa e GONÇALVES, Carlos Jorge, *Comentário ao Regulamento Geral de Proteção de Dados,* 2018, p. 205.
[28] Vide art. 13.º n.º 3 e art. 14.º n.º 4 do RGPD.
[29] PINHEIRO, Alexandre Sousa (coordenação) [et al.], *op. cit,* p. 401 e 402.

Em seguida, iremos discorrer sobre cada um dos conceitos constante do princípio suprarreferido:

1.1.Transparência[30]

A **transparência** exige que *"as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples (...) informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados."* [31]

Ou seja, as informações acerca dos direitos enquanto titular dos dados e as relacionadas com o tratamento de dados pessoais devem ser de **fácil compreensão e acesso**. Deverá, portanto, ser claro para as pessoas singulares que os dados pessoais que lhes digam respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados.

1.2.Licitude

A **licitude** está associada não só ao cumprimento da legalidade na prossecução dos tratamentos de dados, como também na aplicação do art. 52.º da CDFUE, assim exige-se que os dados pessoais sejam processados de forma lícita, para tanto o art. 6.º n.º 1 do RGPD inclui seis fundamentos para o tratamento lícito de dados pessoas[32]. Para tanto os titulares dos dados devem ser avisados dos riscos, regras, garantias e direitos associados ao tratamento, e ainda alertados para os meios que dispõem para exercer esses direitos.

[30] Cf. Considerando 58, 60, 61 e 62.
[31] Considerando 39.
[32] Matéria alvo de desenvolvimento no capítulo IV.

1.3.Lealdade

*"A **lealdade** está essencialmente relacionada com o desenvolvimento dos tratamentos de dados pessoais com respeito por uma relação de equilíbrio entre responsáveis e subcontratantes e titulares dos dados pessoais. Pode manifestar-se de uma forma mais evidente em tratamentos de dados realizados por entidades públicas ou por empregadores."*[33]

Quer isto dizer que os responsáveis pelo tratamento devem tomar as medidas adequadas para manter os titulares dos dados informados do modo com os seus dados são tratados, devendo ainda ser capazes de demonstrar a conformidade das operações de tratamento com o RGPD.

2. Limitação dos tratamentos às finalidades[34]

Segundo o art. 5.º n.º 1 al. b) os dados pessoais são recolhidos para finalidades **determinadas, explícitas e legítimas** que foram estabelecidas no momento da recolha, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades.

ALEXANDRE SOUSA PINHEIRO[35] afirma que *"o espaço do princípio da finalidade no direito a proteção de dados pessoais é crucial, na medida em que funciona como a primeira justificação para a realização de um tratamento de dados, impondo-se até ao consentimento. A realização de recolha de informação pessoal – ou qualquer outra operação de tratamento – deve estar respaldada numa razão-finalidade para, em função dela, se determinar a natureza necessária e não excessiva da informação pessoal recolhida. A imposição do princípio da finalidade ao consentimento assenta na necessidade de proteger situações em que o primeiro esteja por natureza limitado."*

Aceita-se o tratamento de dados para finalidades não apenas determinantes da recolha, mas também *não com estas incompatíveis*, no entanto é entendimento doutrinário

[33] PINHEIRO, Alexandre Sousa (coordenação) [et al.], *op. cit.*, p. 207.
[34] Cf. considerando 50
[35] PINHEIRO, Alexandre Sousa, *Privacy Proteção de Dados Pessoais (...)*, 2015, p. 826.

que não podem ser armazenados dados pessoais para "*finalidades futuras que ainda não estão previstas no momento da recolha*".[36]

Vejamos que a al. b) do n.º 1 do art. 5.º, tendo por base as finalidades do n.º 1 do art. 89.º, determina que os tratamentos *"para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos"* não são considerados incompatíveis com as finalidades iniciais.

Para avaliar se o tratamento posterior é compatível (ou não) com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, o responsável pelo seu tratamento, após ter cumprido todos os requisitos para a licitude do tratamento inicial, deverá ter em atenção os seguintes fatores:

a. Existência de uma ligação entre a finalidade inicial e a finalidade do tratamento futuro pretendido;
b. Contexto da recolha dos dados pessoais, em particular no que se refere às expetativas razoáveis dos titulares dos dados quanto à sua posterior utilização com base na sua relação entre o titular dos dados e o responsável pelo seu tratamento;
c. Natureza dos dados pessoais, com especial cuidado para as categorias especiais de dados pessoais;
d. Eventuais consequências do tratamento posterior pretendido para os titulares dos dados;
e. Existência de salvaguardas e garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas [37].

O princípio da finalidade postula uma **delineação clara do objetivo**, ou seja, os titulares dos dados deverão ser alertados para os riscos, regras, garantias e direitos associados ao respetivo tratamento e para os meios de que dispõem para exercer os seus direitos no que concerne a esse tratamento.

Caso o titular dos dados tenha dado o seu consentimento ou o tratamento se baseie em disposições do direito da União ou de um Estado-Membro que constituam uma medida

[36] HEBERLEIN, Horst in EHMANN, Eugen e SELMAYR Martin (coordenação), "Datenschutz-Grundverordnung", 2017, p. 194.
[37] Como a anonimização, encriptação ou pseudonimização dos dados e a restrição do acesso aos dados.

necessária e proporcionada, numa sociedade democrática, para salvaguardar, em especial, os importantes objetivos de interesse público geral, o responsável pelo tratamento deverá ser autorizado a proceder ao tratamento posterior dos dados pessoais, independentemente da compatibilidade das finalidades.

3. Minimização dos dados

O princípio da minimização dos dados previsto no art. 5.º n.º 1 al. c) consagra que os dados tratados devem ser *"adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados",* por isso também pode ser designado como princípio da qualidade dos dados ou da pertinência dos dados. Este princípio deve ser encarado como uma norma de segurança, porque quanto menor a informação, menor será o risco.

Segundo ALEXANDRE PINHEIRO e CARLOS GONÇALVES[38] *"é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. Segundo este princípio, os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios (dimensão da adequação do princípio da proporcionalidade em sentido amplo)."*

Assim, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica, de modo a que os dados sejam conservados apenas durante o prazo estritamente necessário.

Os dados recolhidos têm de ser apenas aqueles estritamente necessários à concretização do objetivo do tratamento que foi transmitido ao titular. Portanto, *"ocorre uma relação estreita entre as finalidades do tratamento e os dados recolhidos. O tratamento é, necessariamente, limitado pela necessidade imposta pelas finalidades."*[39]

Alguma jurisprudência tem colocado em prática esta doutrina, vejamos, entre outros[40], o Ac. TJUE, de 20 de Maio de 2013, Österreichischer Rundfunk e outros, que nos

[38] PINHEIRO, Alexandre Sousa (coordenação) [et al.], *op. cit.,* p. 209.
[39] *Ibidem.*
[40] Cf. Ac. TJUE, de 8 de abril de 2014, proc. 293/12, Digital Rights Ireland, bem como o Ac. TJUE, de 30 de Maio de 2013, proc. C-342/12, Worten.

enuncia *"qualquer tratamento de dados pessoais deve ser conforme, por um lado, aos «princípios relativos da qualidade dos dados», enunciados no artigo 6.º da diretiva e, por outro, a um dos «princípios relativos à legitimidade do tratamento de dados» (...) os dados devem ser «**recolhidos para finalidades determinadas, explicitas e legítimas**» [artigo 6.º, n.º 1, alínea b), da Diretiva 95/46], bem como «**adequados, pertinentes e não excessivos**», relativamente a essas finalidades [artigo 6.º, n.º 1, alínea c)]. Além disso (...) o tratamento de dados pessoais é lícito, respectivamente, se «for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito» ou se «for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento [...] a quem os dados sejam comunicados".*[41]

4. Exatidão

Este princípio encontra-se previsto no art. 5.º n.º 1 al. d) e de acordo com este os dados pessoais são *"exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora".*

Reformulando, este princípio deve ser implementado em todas as operações de tratamento e prevê que os dados pessoais devam ser **corretos e atualizados**, ou seja deve ser assegurada a integridade dos dados e, sempre que razoavelmente possível, a sua atualização, assim, dados imprecisos devem ser apagados ou retificados sem demora, para que se garanta a sua precisão, isto porque existem casos em que dados imprecisos constituem um dano potencial para o titular dos dados[42]. Aqui chegados, permite-se afirmar que este princípio está intimamente relacionado com os direitos de acesso, de retificação dos dados e do seu apagamento, previstos nos arts. 15.º, 16.º e 17.º[43]. Este é um princípio indiciador de boa gestão da informação.

[41] Negrito nosso.
[42] P. ex. para concluir um contrato de crédito com uma instituição bancária, o banco geralmente verifica a capacidade creditícia do cliente em potencial, lançando mão de bases de dados especiais contendo dados sobre o histórico de crédito de particulares. Ora, se tal banco de dados fornecer dados incorretos ou desatualizados sobre um indivíduo, essa pessoa poderá sofrer efeitos negativos.
[43] Que serão alvo de desenvolvimento no capítulo IV.

Meramente a título exemplificativo vejamos o Ac. de 7 de Maio de 2009, Rijkeboer em que o TJUE considerou que "*este direito (...) implica que a pessoa em causa possa assegurar-se de que esses* ***dados pessoais são tratados com exactidão e de forma lícita****, ou seja, em especial, que os dados de base que lhe dizem respeito são* ***exactos*** *e são enviados a destinatários autorizados. (...) para poder efectuar as verificações necessárias, a pessoa em causa deve dispor de um* ***direito de acesso*** *aos dados que lhe dizem respeito e que estão em fase de tratamento."*[44]

5. Limitação da conservação

O princípio da limitação da conservação, conforme disposto no art. 5.º, n.º 1 al. e) consigna não só que os dados devem ser *"conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados"* bem como ainda que poderão *"ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação cientifica ou histórica ou para fins estatísticos, em conformidade com o n.º1 do artigo 89.º".*

Significa isto que os dados pessoais só devem ser conservados pelo **período necessário à prossecução das finalidades** do tratamento, e que após esse período o responsável pelo tratamento deverá proceder ao seu apagamento ou anonimização definitivos. Para que se cumpra devidamente este princípio, os limites de tempo devem ser estabelecidos pelo responsável pelo tratamento, de modo a garantir que os dados sejam mantidos por não mais do que o necessário.

No Ac. datado de 4 de Dezembro de 2008, Marper, o TEDH decidiu que a retenção indefinida das impressões digitais, amostras de células e perfis de ADN era desproporcionada e desnecessária numa sociedade democrática, considerando que o processo penal contra os titulares tinha terminado numa absolvição e arquivamento, respetivamente. Ou ainda no Ac. de 06 de Junho de 2006, Segerstedt-Wiberg e outros v.

[44] Negrito nosso.

Suécia, em que o TEDH constatou uma violação do art. 8.º da CEDH, uma vez que, o armazenamento contínuo dos dados não era pertinente, devido ao longo período decorrido.[45]

O TJUE no Ac. de 9 de Março de 2017, Manni entendeu que *"no estado atual do direito da União, cabe aos Estados-Membros determinar se as pessoas singulares, visadas no artigo 2.º, n.º 1, alíneas d) e j), desta última diretiva,* ***podem pedir*** *à autoridade encarregada da manutenção, respetivamente, do registo central, do registo comércio ou do registo das sociedades* ***que verifique, com base numa apreciação casuística, se justifica excecionalmente, por razões preponderantes e legítimas relativas à sua situação especial, limitar, findo um prazo suficientemente longo após dissolução da sociedade em causa, o acesso aos dados pessoais que lhes dizem respeito****, inscritos no registo."*[46]

Por último tal princípio é ainda patente no Ac. que data de 8 de Abril de 2014, Digital Rights Ireland, em que o TJUE decidiu invalidar a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações, que alterava a Diretiva 2002/58/CE, por desrespeito ao princípio da proporcionalidade, visto que os dados podiam ficar retidos por até dois anos. No presente caso, **inexistia critérios objetivos que determinassem o período estritamente necessário para conservação** daqueles dados, daí *"*(…) ***concluir que a Diretiva 2006/24 não prevê garantias suficientes, como exige o artigo 8.º da Carta, que permitam assegurar uma proteção eficaz dos dados conservados contra os riscos de abuso e contra qualquer acesso e utilização ilícita dos mesmos.*** *(…) não estabelece regras específicas e adaptadas à grande quantidade de dados cuja conservação é imposta por essa diretiva, ao caráter sensível destes dados e ao risco de acesso ilícito aos mesmo, regras que se destinariam, designadamente, a regular de maneira clara e estrita a proteção e a segurança dos dados em causa, a fim de garantir a sua plena integridade e confidencialidade."*[47]

[45] Ou ainda o Ac. 18 de Setembro de 2014, Brunet v. France, em que o TEDH entendeu que o período de conservação de registos pessoais até 20 anos, era excessivamente longo.
[46] Negrito nosso.
[47] Negrito nosso.

O TJUE considerou, e bem, que a diretiva interferia com o direito ao respeito da vida privada e com o da proteção de dados, até porque os dados recolhidos quando tomados no seu todo permitiam tirar conclusões muito precisas sobre a vida das pessoas.

6. Integridade e confidencialidade

O art. 5.º n.º 1 al. f) preconiza o princípio da integridade e confidencialidade[48], isto é, os dados deverão ser *"tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas".*

A **integridade e a confidencialidade** dos dados pessoais **são essenciais** para evitar efeitos adversos para o titular dos dados, por isso torna-se imperativo adotar medidas de segurança apropriadas (de natureza técnica e/ou organizacional), para evitar o acesso, uso, modificação, divulgação, perda, destruição ou dano acidentais, não autorizados ou ilegais a dados pessoais.

A adequação das medidas de segurança deve ser determinado caso a caso e revista regularmente, devendo estas serem coadunadas com o respetivo risco associado. Contudo adiantámos já que para que se alcance a fiabilidade e segurança dos sistemas ou suporte de conservação dos dados, podem ser utilizadas algumas técnicas tais como a pseudonimização[49] ou a encriptação, assim como procedimentos de limitação e autorização de acessos para a intervenção humana, p. ex., deverão ser mantidos *logs* de acesso, o controlo e verificação, em sede de auditorias internas, de possíveis acessos não autorizados e implementação de medidas de melhoria dos meios de segurança., bem como a adesão a um código de conduta aprovado ou a um mecanismo de certificação aprovado.

[48] Este princípio teve origem no direito-garantia criado pela jurisprudência alemã correspondendo ao "direito fundamental à garantia da confidencialidade e integridade dos sistemas técnico-informacionais" (*Grundrecht auf Gewahrlett tung der Integritat und Vertraulichkeit informationstechnischer System).*
[49] Definição constante do art. 4.º n.º 5.

7. Responsabilidade

Ao iniciar do capítulo, já tivemos oportunidade de referir em traços largos este princípio, repita-se, compete ao responsável pelo tratamento garantir o cumprimento dos princípios elencados neste capítulo e comprovar esse cumprimento, segundo o n.º 2 do art. 5.º.

Citando TATIANA DUARTE[50] *"o responsável pelo tratamento deve, ainda, envergar as vestes de mulher de César, porquanto não lhe bastará cumprir o Regulamento, terá de demonstrar que o cumpre*". Todavia, atrevemo-nos a afirmar que se exige mais ao responsável pelo tratamento do que se exigia à mulher de César, não basta ser, nem parecer, **terá de o provar**.

Esta responsabilidade permite transferir o dever de verificação inicial da legalidade por parte da CNPD para o responsável pelo tratamento, ou seja, baseia-se na eliminação do controlo administrativo prévio, em prol do princípio da liberdade de circulação no espaço europeu. Nem mesmo um regime de mera comunicação prévia mereceu acolhimento no Regulamento.[51] O sistema está, pois, construído segundo uma lógica de responsabilização (*accountability*[52]) dos responsáveis pelos tratamentos de dados e de alívio da tarefa administrativa de controlo baseada numa tarefa de *"controlo do controlo"*[53].

Os responsáveis pelo tratamento devem poder demonstrar a conformidade com as disposições de proteção de dados aos titulares de dados, ao público em geral e às autoridades de controlo a qualquer momento. Apesar deste princípio ser direcionado apenas para os responsáveis pelo tratamento, espera-se também que os subcontratantes o cumpram, uma vez que este está intimamente relacionado com o responsável e até porque sobre os subcontratantes também recaem várias obrigações.

[50] PINHEIRO, Alexandre Sousa (coordenação) [et al.], *op. cit.*, p. 144.
[51] Sobre a mera comunicação prévia ou comunicação prévia sem prazo cf. GONÇALVES, Pedro, *Reflexões sobre o Estado Regulador e o Estado Contratante*, *Direito Público e Regulação*, 2013, p. 163-165; MIRANDA, João, *Comentários ao Novo Código do Procedimento Administrativo*, 2015, p. 495-511.
[52] Terminologia utilizada no direito anglo-saxónico.
[53] A expressão é utilizada por Pedro Gonçalves num sentido diferente, de controlo das entidades privadas que foram objeto de acreditação para realizar a certificação e de (hetero)controlo– cf. *idem*, p. 162.

Os responsáveis pelo tratamento podem facilitar o cumprimento desse requisito de variadas formas, entre as quais[54]:

a. Registar as atividades de tratamento para que as possa disponibilizar quando solicitadas;
b. Em determinadas situações, designar um encarregado de proteção de dados que esteja envolvido em todas as questões relacionadas à proteção de dados pessoais;
c. Realizar avaliações de impacto da proteção de dados para tipos de tratamento que possam resultar em um alto risco aos direitos e liberdades das pessoas;
d. Garantir a proteção de dados por defeito e por conceção;
e. Implementar modalidades e procedimentos para o exercício dos direitos dos titulares dos dados;
f. Aderir a códigos de conduta aprovados ou mecanismos de certificação.

[54] Desenvolvidas no capítulo V.

CAPÍTULO III: PRESSUPOSTOS DA LICITUDE DO TRATAMENTO

O art. 6.º n.º 1 do RGPD enuncia-nos os diferentes pressupostos que constituem as causas de licitude do tratamento, os quais iremos explicar em seguida.

1. Consentimento[55]

Um dos principais pressupostos da licitude do tratamento dos dados reside na necessidade de consentimento do titular dos dados, para uma finalidade claramente definida.

1.1.*Definição*

O consentimento de acordo com o art. 4.º n.º 11 consiste numa *"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".*

1.2.*Condições aplicáveis ao consentimento*

O art. 7.º consigna que o *"responsável pelo tratamento deve poder demonstrar que o titular dos dados pessoais deu o seu consentimento para o tratamento",* sempre que o consentimento legitimar o tratamento de dados, assim, define as condições para que este ato seja considerado válido, nos termos que a seguir se apresenta.

O pedido de consentimento deve constar de uma declaração escrita e deve distinguir-se de outras matérias que também constem dessa declaração; deve ser inteligível, de fácil acesso e ser dotado de linguagem clara e simples. Assim, um consentimento dado de forma oral ou até mediante um consentimento tácito ou outro não oferece estas garantias, porquanto

[55] Para além da análise dos considerandos, é importante cf. GRUPO DE TRABALHO DO ARTIGO 29 "Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679", adotadas em 28 de novembro de 2017, sendo a última redação revista e adotada em 13 de abril de 2018.

não permite fazer prova de ter sido obtido de forma livre, específica, informada, explícita e através de ato inequívoco[56].

É necessário que o titular previamente conheça as condições do tratamento dos seus dados, mediante a prestação de um conjunto de informações prévias relativas ao tratamento, daí o titular gozar do direito à informação (de acordo com o considerando 42, o consentimento só será informado se o titular dos dados conhecer no mínimo a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina).

O consentimento deve ainda ser apresentando de forma destacada, distinta e clara de outros eventuais assuntos que façam parte do mesmo documento. Portanto, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do alcance. É possível identificar algumas presunções de que o consentimento não foi livre e voluntário, nomeadamente, casos de desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento[57]; quando não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico; e se a execução de um contrato, incluindo a prestação de um serviço e depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.

O titular dos dados deve ter a possibilidade de retirar o seu consentimento a qualquer momento, que deve ser tão fácil como o ato de consentir. Esta disposição obriga a que as organizações permitam a retirada do consentimento pela mesma forma em que foi concedido. No que concerne à retirada do consentimento, importa salientar que não fica comprometida a licitude do tratamento efetuado com base na sua prévia prestação.

Estabelece-se que a prestação de um serviço não pode ficar dependente de consentimento do tratamento do titular dos dados, se este não é necessário para a prestação de serviço.

Ora, o consentimento é entendido como uma manifestação de vontade, o que significa que não existe a figura do consentimento obrigatório, ou seja, segundo o Parecer

[56] Da Diretiva resultava que o consentimento podia resultar quer de uma ação quer de uma não ação.
[57] No domínio do tratamento de dados sensíveis em contexto laboral.

de 2017[58] "*se o consentimento estiver agregado a uma parte não negociável das condições gerais do contrato, presume-se que não foi dado livremente. Assim sendo, não se considera que o consentimento foi dado de livre vontade se o titular dos dados não o puder recusar nem o puder retirar sem ficar prejudicado"*. Ou seja, para que o consentimento seja livre o titular dos dados não pode ficar privado do acesso a um bem ou serviço ao não consentir.

1.3.*Consentimento das crianças*

No considerando 38 fica patente que o RGPD pretendeu que existissem regras específicas quando em causa esteja o consentimento de uma criança, exceto se este consentimento for solicitado num contexto de serviços preventivos ou de aconselhamento ao menor. Fora deste caso, quando os serviços forem disponibilizados às crianças com idade inferior a 16 anos é sempre necessário que o responsável parental consinta.

Tal medida justifica-se pelo facto de serem menores e por isso *"menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais."* De acordo com o art. 8.º a idade até à qual é necessário o aval do responsável parental pode ser alterada pelos Estados-Membros, sem nunca poder ser abaixo dos 13 anos.

A abertura aqui efetuada à definição pelos Estados-Membros sobre a idade (entre os 13 e os 16 anos) na qual será necessário pedir consentimento poderá gerar dificuldades de harmonização na utilização de serviços da sociedade da informação. Os operadores de redes sociais (p. ex. Facebook, Youtube, Instagram, entre outros) poderão ter dificuldade em enquadrar as diferentes regras neste âmbito, atendendo a que estes serviços não se encontram, pela sua natureza, limitados às fronteiras de cada Estado.

[58] GRUPO DE TRABALHO DO ARTIGO 29 "Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679", *op. cit.*, p. 6.

2. 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 art. 6.º n.º 1 al. b) constitui outra base para o tratamento legítimo, que abrange dois cenários diferentes:

Em primeiro lugar, a disposição abrange situações nas quais o tratamento seja necessário para a execução de um **contrato na qual o titular dos dados é parte**. Tal pode incluir, por exemplo, o tratamento dos dados relativos ao endereço da pessoa em causa para que os bens adquiridos em linha possam ser entregues ou o tratamento dos dados relativos ao cartão de crédito para que o pagamento seja efetuado.

Em segundo lugar, abrange as **relações pré-contratuais**, desde que a negociação **ocorra a pedido do titular dos dados**, e não por iniciativa do responsável pelo tratamento ou de terceiros. Por exemplo se uma pessoa solicitar a uma seguradora uma proposta de seguro automóvel, a seguradora pode tratar os dados necessários, designadamente, relativos à origem e à idade do automóvel, e outros dados relevantes proporcionados, de forma a preparar a proposta.

Realce-se que, deve existir um vínculo **direto, objetivo e substancial entre o contrato e o tratamento realizado.**

Assim sendo, questionámo-nos onde podemos enquadrar um exemplo corriqueiro, como é o de alguém proceder à compra de flores e pretender que seja entregue a pessoa diversa? Com que fundamento o vendedor das flores trata os dados pessoais desta terceira pessoa? Eis, que nos deparámos com o desafio constante que a vida prática nos oferece, sendo sempre mais criativa que qualquer legislador.

Para além disso, esta base de licitude, conforme descrita e analisada, demonstra facilmente a desnecessidade da esmagadora maioria dos pedidos de consentimento para os quais os cidadãos europeus têm vindo a ser bombardeados. Na dúvida sobre as regras e medidas a aplicar, os agentes do mercado têm vindo a pedir consentimentos para tudo, mesmo às pessoas ao abrigo de uma relação contratual prévia.

Porém, tal é gravoso para a atividade das empresas. De facto, o consentimento é livremente revogável, logo, ao utilizá-lo como base de licitude na execução do contrato as empresas abrem implicitamente a possibilidade de resolução unilateral dos contratos com os

seus clientes, ou pelo menos, a possibilidade de manutenção de um contrato com obrigações apenas unilaterais[59].

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

A necessidade do tratamento para o cumprimento de uma obrigação jurídica a que o responsável esteja sujeito poderá derivar de todas as fontes normativas, à exceção da fonte contratual. São exemplos que se enquadram neste pressuposto de licitude o caso da entidade patronal ter de fornecer à segurança social ou às autoridades fiscais dados relativos aos salários dos seus trabalhadores, ou quando as instituições financeiras sejam obrigadas a denunciar determinadas transações suspeitas às autoridades competentes nos termos das normas em matéria de luta contra branqueamento de capitais.

4. Necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular

Este fundamento parece-nos estar limitado pela expressão "*interesse vital*", a questões de vida ou morte ou, no mínimo, a situações que acarretam um risco de lesão ou de outros danos para a saúde da pessoa em causa. É o que sucede no caso de tratamento de dados relacionados com situações médicas urgentes. Este só tem lugar quando não se puder basear noutro fundamento. Neste sentido veja-se o Ac. 15 de Dezembro de 2009, Y. v. Turquia, que se debruçou sobre um caso de uma equipa de ambulância que comunicou à equipa do hospital que a pessoa que transportara *inconsciente* era seropositiva. O TEDH considerou não haver uma violação de direitos do titular dos dados neste caso (e no nosso entendimento, outra não podia ser a solução, considerando que em causa estava o interesse vital do próprio).

[59] No caso dos contratos em que a contraprestação pela prestação de serviços seja a utilização dos dados dos clientes para fins de marketing direto, p. ex.

Acontece que, em certas situações ao se verificar o pressuposto aqui em causa, verifica-se, ainda que a reboque, o tratamento serve importantes interesses públicos, é o caso de um titular de dados contaminado por uma epidemia passível de propagação. O tratamento de dados, *in casu*, não só salvaguarda o interesse vital do titular, mas também atinge fins humanitários. Outro exemplo ainda oferecido pelo considerado 46 é o das catástrofes naturais.

5. Necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento

Em relação a este pressuposto o já citado Parecer indica que: *"(...) abrange as situações nas quais o próprio responsável pelo tratamento tenha sido investido de autoridade pública ou de uma missão de interesse público (mas não necessariamente também de uma obrigação legal de tratar dados) e o tratamento seja necessário para o exercício dessa autoridade ou a execução dessa missão."*

O TJUE declarou no Ac. de 27 de Setembro de 2017, Puskar, que *"(...) não se opõe a um tratamento de dados pessoais pelas autoridades de um Estado-Membro para efeitos da cobrança de impostos e de luta contra a fraude fiscal (...) sem o consentimento das pessoas em causa, na condição, por um lado, de essas autoridades terem sido investidas pela legislação nacional de missões de interesse público, na acessão desta disposição, de a criação desta lista e na inscrição do nome das pessoas em causa serem efetivamente adequadas e necessárias para alcançar os objetivos prosseguidos e de haver indícios suficientes para presumir que a inscrição das pessoas em causa na lista é justificada e, por outro, de estarem cumpridos todos os requisitos de licitude."*

O TJUE declarou igualmente no Ac. de 16 de Dezembro de 2008, Huber, que *"um sistema de tratamento de dados pessoais respeitantes aos cidadãos da União que não são nacionais do Estado-Membro em causa (...) e que tenha por objetivo dar apoio às administrações encarregadas da aplicação da legislação sobre o direito de residência só cumpre a exigência da necessidade (...) interpretado à luz da proibição de qualquer discriminação exercida em razão da nacionalidade, se contiver* ***unicamente os dados necessários*** *à aplicação dessa legislação pelas referidas autoridades (...) não se podem*

considerar necessários, na acessão do artigo 7.º, alínea e), da Diretiva 95/46, a conservação e tratamento de dados pessoais nominativos no âmbito de um registo como registo central dos estrangeiros para fins estatísticos."[60]

Salienta-se nesta decisão que, não estando presente a dimensão da necessidade, o TJUE entendeu que o tratamento de dados não poderá ser realizado.

6. Necessário para efeito dos interesses legítimos perseguidos pelo responsável pelo tratamento ou por um terceiro

Por último, refere-se à necessidade do tratamento *"para efeito dos 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 de dados pessoais, em especial se o titular for uma criança."*

De acordo com o considerando 47 *"os interesses legítimos dos responsáveis pelo tratamento (...) podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável."*

A existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. São exemplos de interesses legítimos dos responsáveis, que podem constituir fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, designadamente quando:

a. Existir uma relação relevante e apropriada entre o titular dos dados e o responsável, em situações como a que aquele é cliente ou está ao serviço deste;
b. O tratamento for estritamente necessário aos objetivos de prevenção e controlo da fraude;
c. O tratamento for efetuado para efeitos de comercialização direta;

[60] Negrito nosso.

d. Os responsáveis que façam parte de um grupo empresarial ou de uma instituição associada a um organismo central transmitam dados pessoais no âmbito do - grupo de empresas para fins administrativos internos, incluindo o tratamento de dados pessoais de clientes ou funcionários; e
e. O tratamento é necessário para assegurar a segurança da rede e das informações, sobretudo quando o tratamento vise impedir o acesso não autorizado a redes de comunicações eletrónicas e a distribuição de códigos maliciosos e pôr termo a ataques de "negação a serviço" e a danos causados aos sistemas de comunicações informáticas e eletrónicas.

No âmbito deste fundamento, o TJUE declarou no Ac. de 24 de Novembro de 2011, Asociación Nacional de Establecimientos Financieros de Crédito que *"opõe a uma legislação nacional que, na inexistência do consentimento da pessoa em causa e para autorizar o tratamento dos seus dados pessoais necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados exige, além do respeito dos direitos e liberdades fundamentais dessa pessoa, que os referidos dados constem de fontes acessíveis ao público, excluindo assim de forma categórica e generalizada todo e qualquer tratamento de dados que não constem dessas fontes."*

Ou ainda o Ac. de 19 de Outubro de 2016, Patrick Breyer, que *"opõe a uma regulamentação de um Estado-Membro nos termos da qual um prestador de serviços de meios de comunicação em linha apenas pode recolher e utilizar dados pessoais de um utilizador desses serviços sem o consentimento deste na medida em essa recolha e essa utilização sejam necessárias para permitir e faturar a utilização concreta dos referidos serviços por esse utilizador, sem que o objetivo de garantir o funcionamento geral desses mesmos serviços possa justificar a utilização dos referidos dados após o termo de uma sessão de consulta desses meios de comunicação (...) não impõe a obrigação de comunicar dados pessoais a um terceiro a fim de lhe permitir instaurar uma ação de indemnização num tribunal cível por um dano causado pela pessoa interessada na proteção desses dados. Todavia, o artigo 7.º, alínea f), desta diretiva não se opõe a tal comunicação com base no direito nacional."*

Veja-se que o recurso ao critério dos interesses legítimos não abrange a prossecução de tarefas públicas, nomeadamente de carácter administrativo e exige, sempre, uma **ponderação** entre o interesse do responsável pelo tratamento, do titular dos dados e, eventualmente, de um terceiro.

CAPÍTULO IV: DIREITOS DO TITULAR DOS DADOS

O RGPD confere aos titulares dos dados pessoais objeto de tratamento um catálogo de direitos que devem ser salvaguardados pelo responsável pelo tratamento de dados, de modo a mitigar os desequilíbrios existentes.

1. Regras para o exercício dos direitos dos titulares dos dados

O art. 12.º enuncia as regras para exercício dos direitos dos titulares dos dados, neste sentido qualquer um dos direitos abaixo elencados implica para as empresas a procura e a implementação de soluções técnicas que lhe permitam dar resposta às solicitações dos titulares. Ou seja, o responsável pelo tratamento deverá fornecer os meios necessários para que os titulares possam fazer os pedidos[61].

1.1.Prazo

O art. 12.º n.º 3, exige que o responsável pelo tratamento forneça *"ao titular as informações sobre as medidas tomadas (...), sem demora injustificada e no prazo de um mês a contar da data de receção do pedido".* Na eventualidade de precisar de prorrogar o prazo para além do período de 30 dias, o mesmo pode ser alargado até três meses no máximo para os casos complexos, devendo o responsável informar o titular dos dados dos motivos da demora, no prazo de um mês a contar da data do pedido inicial.

1.2.Resposta

O responsável deve responder de forma clara, concisa e suficiente aos pedidos formulados. Quanto à forma a adotar existe liberdade de forma, a menos que se constate imposição legal ou contratual em contrário. No caso de as informações serem prestadas por

[61] P. ex. através da disponibilização de formulário constante do Anexo 2.

via escrita, com recurso a meios eletrónicos e por via oral, é necessário que o responsável pelo tratamento solicite que o titular comprove a sua identidade (n.º 1).

Em caso de indeferimento da pretensão do titular, o responsável pelo tratamento deve comunicar as razões que sustentam a decisão e informar da possibilidade de recorrer da decisão junto da entidade de controlo ou das instâncias jurisdicionais.

1.3.Custo

Relativamente a custos, nos termos do n.º 5, a regra é a prestação gratuita das informações e das comunicações para a satisfação da pretensão do titular, porém, no caso de os pedidos revestirem natureza infundada ou excessiva ou apresentarem caráter repetitivo, pode ser exigido o pagamento de uma taxa que visa suportar os encargos administrativos.

2. Direito a ser informado

2.1.Definição

O art. 12.º do RGPD prevê que deve ser fornecido aos titulares dos dados pessoais objeto de tratamento um conjunto amplo e abrangente de informações (concisas, transparentes, inteligíveis e facilmente acessíveis, através de uma linguagem clara), por escrito ou não, tanto nos casos em que a recolha dos dados seja realizada diretamente junto do titular como nos casos em que esta não se realize na sua presença. Este direito pressupõe uma **posição proactiva pelo responsáve**l e não uma ação indagatória por parte do titular dos dados.

2.2.Como cumprir?

Perante esta obrigação, o responsável pelo tratamento poderá incluir essas informações nos documentos de suporte[62] à recolha dos dados (formulários em papel ou em

[62] Veja-se a título exemplificativo a política de privacidade constante do Anexo 3.

website) ou fazê-los constar numa cláusula de um determinado contrato ou até num Regulamento Interno. A empresa ou a organização pode ainda optar pela entrega de um documento escrito ou incluir a informação no script dos operadores telefónicos.

O considerando 61 afirma uma das diferenças fundamentais entre os arts. 13.º e 14.º, baseado na dimensão temporal: *"as informações sobre o tratamento de dados pessoais relativos ao titular dos dados deverão ser a este fornecidas no momento da sua recolha junto do titular dos dados ou, se os dados pessoais tiverem sido obtidos a partir de outra fonte, dentro de um prazo razoável, consoante as circunstâncias."* Dada a dificuldade em interpretar a expressão "*prazo razoável*", o n.º 3 do art. 14.º enuncia critérios orientadores relativamente à definição de prazos, nos termos seguintes:

a. O prazo máximo definido em período de tempo deve ser de um mês, dependendo dos processos de tratamento- al. a);
b. Caso se trate de dados a utilizar para fins de comunicação, o mais tardar no momento da primeira comunicação- al. b);
c. Caso esteja prevista a divulgação junto de um destinatário, no limite, no momento da divulgação- al. c).

2.3.Isenções

Nos termos do art. 13.º n.º 4, e do art. 14.º, n.º 5, do RGPD, a obrigação de informar os titulares dos dados não se aplica se o titular já detiver todas as informações ou quando os dados pessoais não tiverem sido obtidos a partir do titular dos dados e a prestação de informações for impossível ou desproporcionada, nomeadamente quando os dados pessoais são tratados para fins de arquivo no interesse público, para fins de investigação científica ou histórica ou para fins estatísticos.

3. Direito de acesso

3.1.Noção

O direito de acesso encontra-se previsto no art. 15.º do RGPD e no n.º 1 do art. 35.º da CRP, e consiste em os titulares dos dados saberem se estão, ou não, a ser tratados dados

pessoais que lhes digam respeito, se os dados foram transmitidos para outra entidade ou o destino que lhes foi dado, bem como de aceder aos seus dados e a todas as informações respeitantes às respetivas operações de tratamento. O direito de aceder à informação permite que os próprios titulares validam o modo como a sua informação está a ser tratada.

Este é um direito que se queda a montante de outros direitos, tornando-se, por isso, **basilar no exercício dos outros direitos**, pois é aquele que permite o exercício posterior dos outros.[63]

Por exemplo no caso do Ac. datado de 27 de Outubro de 2009, Haralambie v. Romênia, o TEDH reiterou que os indivíduos que foram objeto de tratamento de dados pessoais tinham interesse em acedê-los. Todavia, o titular só teve acesso às informações pretendidas cinco anos depois do pedido, o que violou de forma clara e inequívoca o art. 8.º da CEDH. Note-se que, já há largos anos, este é um direito de maior interesse para os titulares dos dados, mas que nem sempre cumprido como se idealiza. Assim, o legislador por forma a efetivar os direitos dos titulares no ordenamento jurídico passou a sujeitar as organizações ao apertado crivo do prazo para o efeito.

4. Direito de retificação

O titular dos dados tem o direito de exigir que os dados a seu respeito sejam corretos, exatos, completos e atuais, para tanto pode o titular dos dados **retificar ou completar** os seus dados pessoais, quando estejam desatualizados, incorretos ou incompletos.

Note-se que a precisão dos dados pessoais é essencial para garantir um elevado nível de proteção de dados para os titulares dos dados e no mesmo sentido, tem entendido o TEDH, p. ex. no Ac. de 18 de Novembro de 2014, Cemalettin Canli v. Turquia por não ser dada a possibilidade de o titular retificar os dados considerou-se haver uma violação do art. 8.º da Carta.

[63] Neste sentido cf. Ac. TEDH, de 28 de Abril de 2009, K.H. e outros v. Eslováquia TEDH.

5. Direito ao apagamento ("o direito de ser esquecido")[64]

5.1.Noção

O n.º 1 do art. 17.º confere aos titulares dos dados pessoais o direito de solicitarem que os dados pessoais que lhes dizem respeito sejam apagados, criando assim nos responsáveis ou nos subcontratantes a obrigação de o fazer, com a maior brevidade.

5.2.Limitações

Este direito não é absoluto, sofre limitações que se encontram estabelecidas por lei. Assim, o direito de obter a eliminação dos dados pessoais é possível, se:

a. Os dados se revelarem desnecessários supervenientemente para as finalidades que estiveram na base da recolha ou do tratamento;
b. O titular dos dados retirar o consentimento (art. 6.º n.º 1 al. a) ou art. 9.º n.º 2 al. a)), quando o tratamento for necessariamente fundamentado neste e não exista outro fundamento legal para o tratamento dos dados;
c. O titular dos dados se opuser ao tratamento, nos termos do art. 21.º n.º 1, e o responsável pelo tratamento não demonstrar que existam interesses legítimos prevalecentes que justifiquem o tratamento, conforme o art. 21.º n.º 2;
d. Os dados foram tratados ilicitamente;
e. O apagamento dos dados for necessário para o cumprimento de uma obrigação legal a que o responsável pelo tratamento esteja sujeito;
f. Os dados foram recolhidos numa oferta de serviços da sociedade de informação a crianças com menos de 16 anos, sem o consentimento dado por quem exerce as responsabilidades parentais (art. 8.º n.º 1).

Mesmo que o titular dos dados possua um dos fundamentos anteriormente elencados para o apagamento dos dados, importa averiguar se estes dados se revelam necessários para o responsável pelo tratamento ou subcontratante, conforme consta do n.º 3 do mesmo artigo, ou seja, se são necessários ao exercício do direito à liberdade de expressão e de informação; para o cumprimento de uma obrigação legal de um Estado-Membro; para o exercício de

[64] Cf. Considerando 65.

funções de interesse público ou o exercício da autoridade pública; por motivos de saúde pública; para fins de arquivo, investigação ou estatística; para efeitos de declaração, exercício ou defesa de um direito num processo judicial. Se alguma destas situações ocorrer o direito ao esquecimento pode não ser levado a cabo pelo responsável pelo tratamento.

5.3.Esquecimento em linha

O n.º 2 do art. 17.º trata do direito a ser esquecido em linha, ou seja, na eventualidade de os dados entretanto terem sido divulgados a outras entidades, o responsável pelo tratamento deverá informar os restantes responsáveis pelo tratamento dos dados que o titular solicitou o *"apagamento das ligações para esses dados"* e se estes forem públicos, o responsável pelo tratamento deve informar os restantes responsáveis de que o titular solicitou o assim como das *"cópias e reproduções"*, tornando *"as medidas que forem razoáveis".*

A propósito do direito a ser esquecido em linha o TJUE já há muito se pronunciou[65]. Defendeu que a atividade de um motor de busca, como é o caso do Google, é considerada uma atividade que comporta o tratamento de dados, e consequentemente deve tal entidade ser considerada responsável pelo tratamento, até porque indexa, armazena e põe à disposição informações que contenham dados pessoais. Por ser intitulado por responsável pelo tratamento tem o dever de atender aos pedidos de esquecimento dos titulares**,** isto é*"(...) o operador de um motor de busca é obrigado a suprimir da lista de resultados, exibida na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, as ligações a outras paginas web publicadas por terceiros e que contenham informações sobre essa pessoa."*

Reconheceu ainda que esse direito não é absoluto, devendo ser avaliado caso a caso, e para o efeito forneceu orientações sobre os fatores a ter em conta durante o processo de ponderação – "*(...) esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em aceder à informação numa pesquisa sobre o nome dessa pessoa. No entanto, não será esse o caso de se afigurar que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada*

[65] Ac. TJUE, de 13 de maio de 2014, proc. n.º C-131/12, Google Spain.

pelo interesse preponderante do referido público em ter acesso à informação em questão, em virtude dessa inclusão."

Este Acórdão tratou de um pedido de um cidadão espanhol que havia requerido à Google que, através dos meios necessários, garantisse que não fossem devolvidos determinados resultados por parte do motor de busca propriedade daquela, aquando da procura efetuada pelo seu nome.

O TJUE reconheceu o direito ao esquecimento em linha e, consequentemente, o direito de supressão das ligações às informações pessoais, por parte dos motores de busca. No entanto, o TJUE não se acanhou ao enunciar que no presente caso o direito ao esquecimento em linha prevalece não só sobre o interesse económico do operador de busca, mas também sobre o direito à informação. Na sequência do acórdão, o GTA29 adotou orientações para a aplicação da decisão do TJUE, que incluem uma lista de critérios comuns a utilizar pelas autoridades de controlo no tratamento de queixas relacionadas com pedidos de supressão de indivíduos.

No sentido inverso, é nos trazido o Ac. TJUE, de 9 de março de 2017, Manni, que depois de uma avaliação ponderada nos n.ºs 53, 54, 56 e 57 sustentou que o titular dos dados não podia gozar do direito ao esquecimento, tendo em conta que *"(...) os dados (...) podem revelar-se necessários para, designadamente, apurar a legalidade de um ato praticado em nome dessa sociedade durante o período da sua atividade ou para que terceiros possam intentar uma ação contra os membros dos seus órgãos ou contra os seus liquidatários. Além disso, em função, designadamente dos prazos de prescrição aplicáveis nos diferentes Estados-Membros, podem surgir questões que imponham a necessidade de dispor desses dados mesmo vários anos após uma sociedade ter deixado de existir. (...) Nessas condições, os Estados-Membros (...) não podem garantir às pessoas (...) o direito de obter, por principio, após um determinado prazo a contar da dissolução da sociedade em causa a supressão dos dados pessoais que lhes dizem respeito, que foram inscritos no registo em aplicação dessa última disposição, ou o bloqueio desses dados para o público. Esta interpretação (...) não conduz, por outro lado, a uma ingerência desproporcionada nos direitos fundamentais das pessoas em causa, designadamente no direito ao respeito da vida privada, bem como no seu direito à proteção de dados pessoais, garantidos pelos artigos 7.º e 8.º da Carta."*

6. Direito à limitação do tratamento

O legislador introduziu o direito à limitação do tratamento no art. 18.º que conjetura que o titular dos dados tem o direito de exigir a limitação do tratamento junto do responsável, quando pretender contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; se 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; se o responsável pelo tratamento deixar de 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; se se tiver oposto ao tratamento até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

Uma vez exercido este direito, o responsável pelo tratamento deve informar a cada destinatário a quem os dados tenham sido transmitidos, salvo se, nos termos do art. 19.º, tal notificação se revelar impossível ou implicar um desproporcionado esforço. Os dados pessoais objeto desse exercício, só podem ser tratados mediante consentimento do seu titular; para efeitos de declaração; exercício ou defesa de um direito num processo judicial; para defesa dos direitos de outra pessoa singular ou coletiva; ou por motivos ponderosos de interesse público da União ou de um Estado-Membro.

7. Direito à portabilidade de dados

7.1.Noção

O art. 20.º do RGPD introduz um novo direito, que deriva diretamente do direito de acesso. Este direito permite aos titulares dos dados receber os dados pessoais que tenham fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e transmitir esses dados a outro responsável pelo tratamento sem impedimentos. Este direito é estribado no princípio do controlo do utilizador, cujo objetivo é conferir poderes de controlo do titular sobre os seus dados, o que apoia a liberdade de

escolha do utilizador, o controlo do utilizador e a capacitação do utilizador[66], uma vez que lhes permite obter e reutilizar os seus dados pessoais para as suas próprias finalidades e em diferentes serviços.

Quando o responsável responde a um pedido de portabilidade de dados, deve agir de acordo com as instruções do titular, o que significa que não é responsável pela conformidade do destinatário com a lei de proteção de dados, dado que o titular decide para quem transfere.

Importa ainda salientar que este direito de transmitir esses dados é efetuado independentemente da vontade do responsável a quem o titular tenha, inicialmente, fornecido os dados pessoais.

7.2.Requisitos

O exercício deste direito está subordinado à verificação cumulativa de quatro pressupostos:

a. Incidência sobre dados fornecidos pelo titular;
b. Tratamento baseado no consentimento (ao abrigo do art. 6.º n.º 1 al. a), ou do art. 9.º n.º 2 al. a)) ou baseado na execução de um contrato na qual o titular dos dados é parte (ao abrigo do art. 6.º n.º 1 al. b);
c. Tratamento circunscrito aos dados respeitantes ao titular, ou seja, os dados inferidos e os dados derivados que são criados pelo responsável pelo tratamento com base nos dados «fornecidos pelo titular dos dados», não podem serem recebidos pelo titular de dados e;
d. Tratamento realizado por meios automatizados.

No que concerne a este último requisito não se compreende a *ratio legis* do mesmo. Ora, de acordo com a definição constante do art. 4.º n.º 3 do RGPD que vai ao encontro do art. 35.º n.º 7 da CRP *"os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista em números anteriores, nos termos da lei."*

[66] Cf. GRUPO DE TRABALHO DO ARTIGO 29, "Orientações sobre o direito à portabilidade dos dados", (16/PT WP 242 rev. 01), adotada em 13 de dezembro de 2016, com a última redação revista e adotada em 5 de abril de 2017, p. 3.

Assim sendo, porque não se incluiu todos os dados pessoais neste direito à portabilidade? A legislação faz uma diferenciação, no nosso entendimento, injustificada, que impede o acionamento deste direito por parte dos titulares dos dados que vêm os seus dados organizados em ficheiros manuais.

Quando uma pessoa exerce o seu direito à portabilidade dos dados, fá-lo sem prejuízo de qualquer outro direito (tal como sucede com qualquer outro direito no âmbito do RGPD). Um titular de dados pode continuar a utilizar e beneficiar dos serviços do responsável pelo tratamento mesmo após uma operação de portabilidade de dados.

7.3.Meios técnicos

O art. 20.º n.º 2, impõe aos responsáveis pelo tratamento a obrigação de transmitir os dados portáveis diretamente para outros responsáveis pelo tratamento *"sempre que tal seja tecnicamente possível".*

Este direito tem como objetivo obter, reutilizar e transmitir os dados entre diferentes serviços e para os seus próprios fins, com isso *"espera-se que (...) promova oportunidades de inovação e de partilha segura de dados pessoais entre os responsáveis pelo tratamento sob o controlo do titular dos dados."* [67]

Todavia, não tendo o RGPD tornado obrigatório o desenvolvimento de formatos interoperáveis[68], nem imposto recomendações sobre o formato específico a ser fornecido, tem-se entendido que este armazenamento pode ser feito através de um dispositivo privado ou de uma nuvem privada, sem haver necessariamente lugar a uma transmissão dos dados para outro responsável pelo tratamento.

Face ao exposto, devido aos obstáculos que os titulares dos dados sentirão no exercício deste direito, por falta de formatos interoperáveis e de recomendações, defendemos que este direito será despido de aplicação prática (ou pelo menos não terá tanta aplicabilidade quanto a desejada).

[67] *Idem*, p. 6
[68] Pode ser definida em um sentido amplo como a capacidade dos sistemas de informação de trocar dados e permitir o compartilhamento de informações.

No nosso entendimento, devia este direito ser alvo de concretização legislativa pelos Estados-Membros, através da adoção de diretrizes que exigissem que as organizações dispussem de formatos interoperáveis, formatos estes pré-estabelecidos pelo legislador.

8. Direito de oposição

O art. 21.º n.º 1 do RGPD autoriza o titular dos dados a opor-se a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito que tenham por base interesses legítimos ou interesse público, incluindo a definição de perfis com base nessas disposições. [69]

O exercício do direito de oposição pressupõe a existência de um tratamento de dados legítimo que tenha como fundamento de legitimidade não o consentimento, nem uma obrigação legal, mas a prossecução de interesse público (art. 6.º n.º 1 al. e)), a realização de interesses legítimos do responsável pelo tratamento ou de um terceiro (art. 6.º n.º 1 al. f)), ou as condições previstas no art. 6.º n.º 4.

Este direito não se considera aplicável se o responsável apresentar uma ponderação de interesses em que invoque *"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 num processo judicial."* Trata-se dos requisitos de aplicação de interesse legítimo como fundamento de legitimidade para o tratamento de dados pessoais.

O tratamento de dados para efeitos de comercialização direta, permite que o titular dos dados se oponha a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização (n.º 2). Se assim for, os dados pessoais deixam de ser tratados para esse fim (n.º 3).

Mesmo quando o tratamento relativo a *profiling* for legítimo, o titular dos dados tem direito a opor-se nos termos do art. 21.º, que consagra um direito específico de oposição relativamente a decisões individuais automatizadas. De acordo com este artigo, o

[69] A este propósito ver o Ac. TJUE, de 9 de março de 2017, proc. C-398/15, Manni no que concerne ao reconhecimento por parte do TJUE da existência de um direito de se opor ao tratamento.

responsável pelo tratamento dos dados deve cessar o tratamento se existir oposição do titular dos dados, a não ser que apresente razões imperiosas e legítimas para o tratamento.

9. Direito de não ficar sujeito a decisões individuais automatizadas, incluindo definição de perfis[70]

Desde a implementação da Diretiva a tecnologia sofreu avanços significativos, permitindo aos responsáveis pelo tratamento reunir e analisar dados dos titulares de forma a criar perfis, tornando os titulares dos dados alvos para tratamento de dados intrusivos.

O art. 22.º consagra o direito à não sujeição a decisões individuais automatizadas, suscetíveis de serem tomadas por um responsável pelo tratamento, baseadas nos dados pessoais do titular, constantes do sistema informático daquele.

O n.º 1 consagra o direito do titular dos dados a não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito incluindo a definição de perfis, mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados (cf. considerando 71).

Este direito de não sujeição a decisões automatizadas abrange apenas aquelas decisões que produzam efeitos na esfera jurídica dos titulares ou afetem significativamente de forma similar.

Embora por princípio o titular dos dados tenha o direito de não ficar sujeito a decisões baseadas em tratamentos automatizados dos dados, incluindo o *profiling*, estas serão possíveis, nos termos do art. 22.º, quando:

a. Necessárias para a celebração de um contrato ou execução do mesmo entre o titular dos dados e o responsável pelo tratamento;
b. Autorizadas pela lei de um estado membro;

[70] Cf. definição constante do art. 4º nº 4.

c. Existir consentimento explícito do titular.

De acordo com o n.º 3, nos casos previstos em a. e c., o responsável pelo tratamento deve aplicar medidas para salvaguardar os direitos e legítimos interesses daquele, designadamente a informação específica ao titular dos dados, ou seja, o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. Se tais decisões puderem ter um impacto significativo na vida das pessoas por exemplo[71], na qualidade de crédito, é necessária uma proteção especial para evitar consequências negativas.

10. Limitações aos direitos dos titulares de dados

Para além das limitações específicas de cada um dos direitos dos titulares de dados existe um conjunto de restrições comuns a todos os direitos e que são referidas no art. 23.º do RGPD. Estamos a considerar limitações necessárias num contexto de uma sociedade democrática, para salvaguardar como refere o texto do RGPD: segurança do Estado, defesa, segurança pública, prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sansões penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, outros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social, defesa da independência judiciária e dos processos judiciais, prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas, uma missão de controlo, de inspeção ou de Regulamento associada, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas als. a), e) e g), a defesa do titular dos dados ou dos direitos e liberdades de outrem, a execução de ações cíveis.

[71] Para avaliar rapidamente a credibilidade de um cliente futuro, as agências de crédito reúnem determinados dados. Esses dados pessoais são posteriormente convertidos em um algoritmo de pontuação, que calcula um valor global representando a capacidade de crédito do cliente em potencial.

CAPÍTULO V: RESPONSÁVEL PELO TRATAMENTO E SUBCONTRATANTE

Secção I: Obrigações Gerais

1. Subcontratação

O RGPD define o **responsável pelo tratamento**, ou *controller* na terminologia inglesa, no seu art. 4.º n.º 7 como *"a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; 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."*

E **subcontratante**[72]**,** ou *processor* na terminologia inglesa, no seu art. 4.º 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."*

Na Diretiva os subcontratantes tinham, essencialmente, de cumprir deveres relativos à segurança e à confidencialidade. Com o Regulamento, apesar de o responsável pelo tratamento dos dados continuar, em grande parte, a ser o responsável pelo cumprimento das regras de proteção de dados pessoais, o subcontratante fica obrigado a diversos deveres a que, até agora, não estava obrigado, veja-se a título exemplificativo a obrigatoriedade de registo das atividades de tratamento (art. 30.º n.º 2), o cumprimento da segurança no tratamento dos dados (art. 32.º) ou a nomeação de EPD (art. 37.º).

O Regulamento preceitua ainda que os subcontratantes são responsabilizados pelo incumprimento das regras do RGPD, nos termos previstos no art. 82.º, *"se não tiver cumprido as obrigações decorrentes do presente regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo*

[72] De acordo com a CNPD o termo correto será subcontratado e não subcontratante como consta do Regulamento. No entanto será adotada a terminologia usada no RGPD.

tratamento", podendo, inclusivamente, ficar sujeitos ao pagamento das coimas previstas no art. 83.º do RGPD.

Tal alteração legislativa justifica-se porque a decisão de contratar um subcontratante cabe em exclusivo ao responsável pelo tratamento, que pode optar por levar a cabo o tratamento de dados dentro da sua própria organização ou externalizar[73].

A relação entre o responsável pelo tratamento e o subcontratante deve constar de um documento escrito, para o efeito o art. 28.º do Regulamento apresenta de forma detalhada a forma e o conteúdo deste contrato[74], prevendo-se inclusivamente a possibilidade de a Comissão vir a estabelecer cláusulas contratuais tipo. A não existência deste contrato é uma violação da obrigação de fornecer documentação por escrito de responsabilidades mútuas.

2. Responsabilidade do responsável pelo tratamento

O art. 24.º n.º 1 consigna duas obrigações indissociáveis do responsável pelo tratamento. A primeira é a obrigação que *"tendo em conta a natureza, o contexto, as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento."*

Por medidas técnicas e organizativas, o legislador abarca não só as plataformas físicas, informáticas ou digitais, mas também todos os procedimentos manuais, com ou sem intervenção humana - que afetarão o tratamento (*vide* art. 24.º, n.º 2 e 3).

A segunda obrigação é a de revisão e atualização dessas medidas consoante as necessidades.

[73] A externalização de qualquer serviço implica abdicar do controlo inerente à circunstância desse serviço ser levado a cabo internamente.
[74] Exemplo constante do Anexo 4.

3. Proteção de dados desde a conceção e por defeito

3.1. Privacy by design

De acordo com o art. 25.º n. º1 encontra-se plasmada a ideia de *"privacy by design"* ou *"proteção desde a conceção*" que se traduz numa *"abordagem que assenta na necessidade de garantir a privacidade durante todo o processo de desenvolvimento de um novo produto/processo. É uma abordagem pró-ativa que permite que, aquando da conceção de um novo produto ou de um novo serviço, se considere o risco que tal representa para a privacidade, ao invés de apenas serem consideradas estas questões posteriormente. As empresas e as organizações devem avaliar cuidadosamente e implementar medidas e procedimentos técnicos e organizacionais adequados desde o início para garantir que o tratamento está em conformidade com o RGPD e protege os direitos dos titulares dos dados em causa."*[75]

Ou seja, o responsável pelo tratamento, ao adotar os meios técnicos e organizativos a aplicar ao tratamento deverá ponderar, desde logo na conceção do tratamento, as técnicas mais avançadas existentes no mercado (*"state of the art")*, os custos de aplicação de tais meios, a natureza do tratamento, o âmbito, nomeadamente, em termos de categorias de dados, volume de dados tratados, extensão territorial ou número de titulares abrangidos, o contexto do tratamento, as finalidades do tratamento dos dados, e os riscos de tratamento no que respeita aos direitos e liberdades das pessoas singulares, sendo este graduado não apenas em função da gravidade, em abstrato, da sua verificação; mas também da probabilidade da sua efetiva concretização.

3.2. Privacy by default

O n.º 2 do art. 25.º consagra o princípio da "*proteção de dados por defeito*" ou "*privacy by default*", segundo o qual só os dados pessoais tratados devem cingir-se ao mínimo estritamente necessário às finalidades do tratamento pretendido, proibindo-se a

[75] MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão, *Regulamento Geral de Proteção de Dados: Manual Prático*, 2018, p. 36.

recolha de dados que excedam tais finalidades. A este respeito, a atuação das organizações deve limitar-se ao mínimo necessário, quer quanto "*à quantidade de dados pessoais recolhidos, à extensão de seu tratamento, ao seu prazo de conservação e à sua acessibilidade*", assim como às pessoas ou entidades que aos mesmos têm acesso.

3.3. Súmula

Em suma, os princípios de "*privacy by design*" e "*privacy by default*" auxiliam o responsável pelo tratamento e o subcontratante desde um momento embrionário, o que só por si exprime um grande avanço no objetivo de estar *compliant* neste sentido vejamos que *"a necessidade de proteção de dados deverá ser considerada, desde logo, no desenvolvimento de um novo produto/processo, de modo a garantir que somente os dados pessoais necessários para cada propósito específico do tratamento sejam recolhidos (acesso por tipo de utilizador, em função da sua necessidade), vedando-se a recolha de dados pessoais completamente desnecessários."*[76]

4. Documentação e registo de atividade de tratamento

O art. 30.º consagra uma obrigação[77] que não existia na Diretiva, e que é uma das manifestações do dever de *accountability*, consiste no dever dos responsáveis pelo tratamento de dados, e dos subcontratantes (art. 30.º n.º 2), de documentar de forma detalhada todas as atividades relacionadas com o tratamento de dados pessoais, não só as que resultam da obrigação de manter um registo como também as relativas a outros procedimentos internos, de modo a que a organização esteja apta a demonstrar o cumprimento de forma transparente de todas as obrigações decorrentes do RGPD.

A obrigação de proceder ao registo de tratamentos dos dados pessoais já foi encetada aquando do enquadramento do preceituado no n.º 2 do art. 5.º na medida em que estabelece que "*o responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo («responsabilidade»)",* e do art. 24.º n.º 1 que prevê que o

[76] *Ibidem.*
[77] Em bom rigor, trata-se, antes, de um dever, atenta à definição legal de obrigação, contida no art. 397.º do CC.

responsável pelo tratamento de dados pessoais deve "*poder comprovar que o tratamento é realizado em conformidade*."

Segundo a primeira parte do n.º 5 do art. 30.º apenas as entidades que empregam mais de 250 trabalhadores estão sujeitas a esta obrigação de registo, exceto se o tratamento efetuado for suscetível de implicar um risco para os direitos e liberdades do titular dos dados; não for ocasional; abranger dados sensíveis; ou abranger dados penais ou relativos a condenações penais e infrações referidas no art. 10.º.

Aos responsáveis pelo tratamento de dados que devem conservar um registo das atividades de tratamento de dados[78] ou aos que pretendem, de forma voluntária fazê-lo, o art. 30.º n.º 1 define as informações que deste registo deve constar, diga-se:

a. Identificação (nome e contactos do responsável pelo tratamento ou responsável conjunto pelo tratamento ou do seu representante, bem como do EDP);

b. Finalidades dos tratamentos dos dados;

c. Descrição das categorias de titulares de dados e das categorias de dados pessoais;

d. Categorias de destinatários a quem os dados pessoais foram ou serão divulgados;

e. As transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e a documentação que comprove a existência das garantias adequadas (se aplicável);

f. Prazos previstos para o apagamento das diferentes categorias de dados;

g. Descrição geral das medidas técnicas e organizativas no domínio da segurança, incluindo, consoante o que for adequado: a pseudonimização e a cifragem dos dados pessoais, a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, a capacidade de restabelecer a disponibilidade e o acesso dos dados pessoais de forma atempada no caso de um incidente físico ou técnico e um processo para testar, apreciar e avaliar

[78] Ver exemplo constante do Anexo 5.

regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Já no art. 30.º n.º 2 estão elencadas as informações que deverão constar dos registos das atividades de tratamento de dados pessoais, realizadas pelos subcontratantes e/ou pelos seus representantes, em nome de um responsável pelo tratamento, que são, por conseguinte, menores[79].

Esta obrigação relaciona-se com o facto de as notificações/autorizações prévias atuais deixarem, na sua maioria, de ser obrigatórias, pelo que este registo e a existência do EPD acabam por ser as principais formas de demonstrar a conformidade com a lei perante as autoridades de proteção de dados.

Secção II: Segurança dos dados pessoais

1. O reforço de políticas e procedimentos de segurança de dados

A segurança dos dados apresenta-se como fundamental no Regulamento o que, em termos gerais, impõe regras mais exigentes para a segurança dos dados[80], vejamos o seu art. 32.º que exige *"tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante"* sejam aplicadas as medidas técnicas e organizativas necessárias para garantir um nível de segurança adequado. Este artigo aponta sugestões específicas de medidas de segurança consideradas adequadas:

a. A pseudonimização e a cifragem dos dados pessoais;
b. A capacidade de garantir a confidencialidade, integridade (proteção contra qualquer forma de perda de dados), disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, o que exige do responsável pelo tratamento a implementação de um sistema de gestão de segurança da informação;

[79] Modelo constante do Anexo 6.
[80] Ainda com algum paralelismo com o art. 17.º da Diretiva.

c. A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
d. Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas adotadas;
e. O cumprimento de um código de conduta (art. 40.º) ou de um processo de certificação (art. 42.º).

Ou ainda através das seguintes **regras organizacionais internas**:

a. Formação regular aos funcionários sobre as regras de segurança de dados e suas obrigações, especialmente em matéria de confidencialidade;
b. Distribuição e descrição clara das responsabilidades e competências;
c. Utilização de dados pessoais apenas de acordo com as instruções da pessoa competente ou de acordo com as regras estabelecidas;
d. Proteção contra acesso a locais de hardware e software, incluindo controlos sobre a autorização de acesso;
e. Certificação de que as autorizações de acesso a dados pessoais foram concedidas pela pessoa com poderes para o ato, exigindo-se para o efeito documentação;
f. Protocolos automatizados de acesso eletrónico a dados pessoais e controlo regular de tais protocolos;
g. Documentação exaustiva de modo a demonstrar que não ocorreram transmissões ilegais de dados;
h. Formação e educação sobre segurança dos dados;
i. Os procedimentos de verificação também devem ser implementados para assegurar que as medidas apropriadas não apenas existam no papel, mas sejam implementadas e funcionem na prática (como auditorias internas ou externas).

A jurisprudência tem se vindo a pronunciar neste sentido, vejamos o Ac. do TEDH, de 17 de julho de 2008, I v. Finland em que o TEDH concluiu que houve uma violação do art. 8.º da CEDH, uma vez que o sistema de registo do hospital não esclarecia retroativamente o uso de registos de pacientes, pois revelava apenas as últimas cinco consultas.

2. Notificação de uma violação de dados pessoais

Em caso de uma violação de dados pessoais, que é definida no art. 4.º n.º 12, as organizações devem, de forma a evitar investigações por parte das autoridades de controlo e possíveis aplicações de sanções criar uma política adequada de resposta que inclua um plano de ação e de implementação rápida.

2.1. À autoridade de controlo

No caso de uma violação de dados pessoais[81], o art. 33.º n.º 1 estabelece que os responsáveis pelo tratamento ficam obrigados a notificar[82] as autoridades de proteção de dados (em Portugal a CNPD) *"sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma".*

Esta notificação não é obrigatória se a violação dos dados pessoais não for suscetível de resultar num risco[83] para os direitos e liberdades dos titulares dos dados.

Note-se que o prazo de 72 horas não se encontra previsto para o subcontratante. Porém, é de entender que o prazo imposto para comunicar a violação ao responsável deverá ser ainda mais reduzido, atento o conceito de demora injustificada aplicável a ambos.

Assim, é fundamental que o responsável pelo tratamento, ou o subcontratante, seja capaz de detetar qualquer violação de dados assim que a mesma ocorra e notificar nos termos definidos no Regulamento. Esta notificação deve conter[84]:

a. A descrição da natureza da violação de dados pessoais, incluindo, sempre que possível, as categorias e o número aproximado de pessoas em causa, bem como as categorias e o número aproximado de registo de dados pessoais em questão;
b. O nome e os dados de contacto do responsável pela proteção de dados;
c. Descrição das consequências prováveis da violação de dados pessoais;

[81] Na Diretiva não se encontrava qualquer definição de "violação de dados pessoais", nem se fazia referência à necessidade de notificação às autoridades de proteção de dados nem aos titulares dos dados pessoais.
[82]A CNPD já publicou um modelo de formulário para as situações de violações de dados, disponível no Anexo 7.
[83] Quanto a nós, bastará a existência de um risco mínimo para ser necessário o cumprimento da obrigação em causa.
[84]Tendo em conta o prazo é permitido no n.º 4 que as informações sejam fornecidas faseadamente.

d. Descrição das medidas tomadas/propostas pelo responsável pelo tratamento, para reparar a violação de dados pessoais, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos negativos.

Considerando que em alguns casos, já mencionados, o registo das atividades é obrigatório o responsável pelo tratamento dos dados fica incumbido de manter registados os incidentes de violação de dados pessoais, podendo a autoridade de proteção de dados verificar o seu cumprimento.

2.2. Ao titular dos dados

De acordo com o art. 34.º n.º 1 sempre que a violação de dados seja suscetível de representar um alto risco para os direitos e liberdades dos seus titulares, deve o responsável pelo tratamento dos dados comunicar tal violação ao titular dos dados, em linguagem acessível e simples, sem demora injustificada.

Diga-se ainda, que o n.º 3 do art. 33.º estabelece um conjunto de derrogações a esta obrigação, designadamente quando o responsável pelo tratamento tenha implementado medidas de proteção técnicas e organizativas adequadas, e essas medidas tenham sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais ininteligíveis a qualquer pessoa que não autorizada a aceder os mesmo, como criptografia, quando o responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados não for suscetível de se concretizar ou se a notificação implicar um esforço desproporcionado, neste caso, os titulares de dados podem ser informados sobre a violação através de outros meios, como uma comunicação pública ou medidas semelhantes.

Secção III: Breve alusão ao estudo da avaliação de impacto sobre a proteção de dados

Segundo o GTA29 *"uma AIPD é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses*

riscos. As AIPD são instrumentos importantes em matéria de responsabilização, uma vez que ajudam os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas adequadas para assegurar a conformidade com o regulamento"[85].

Trata-se de uma solução *ex ante*, já que é realizada antes de iniciar o tratamento e são uma forma útil de os responsáveis pelo tratamento de dados aplicarem sistemas de tratamento de dados que estejam em conformidade jurídica.

São dimensionáveis e podem assumir diferentes formas, ou seja, os responsáveis pelo tratamento de dados gozam de flexibilidade para determinar a estrutura e a forma com vista a que se encaixe nas práticas de trabalho existentes. Porém, o RGPD no seu n.º 7 do art. 35.º define os requisitos básicos para uma AIPD eficaz. Este tipo de avaliação é de caráter obrigatório, conforme dispõe o art. 35.º quando o tratamento implicar a avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado de dados, incluindo *profiling*, que levem a decisões que afetem o titular dos dados, operações de tratamento em larga escala de dados sensíveis e/ou o controlo sistemático de zonas acessíveis ao público em grande escala.

A realização de uma AIPD implica a solicitação obrigatória pelo responsável de um parecer ao EDP, nos casos em que este exista, mas a sua fundamentação e conclusões não são vinculativas para o responsável. A autoridade de controlo também deve ser consultada antes de se iniciar qualquer tipo de tratamento quando a avaliação de impacto indicar que existe um risco elevado[86], não mitigado pela tomada de medidas, devendo comunicar-lhe, nessa consulta, as informações previstas no art. 36.º n.º 3 do RGPD.

[85] GRUPO DE TRABALHO DO ARTIGO 29 "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", (WP 248 rev.01), adotada em 04/04/2017, p. 4.

[86] O Grupo de Trabalho do Artigo 29 emitiu diretrizes sobre as avaliações de impacto de proteção de dados, como já referenciada supra. Desenvolveu nove critérios para ajudar a determinar se uma avaliação de impacto de proteção de dados é necessária, introduzindo a regra de que as operações que atendam a dois ou mais critérios exigirão a AIPD.

Secção IV: Encarregado de proteção de dados

1. Elo de ligação

Umas das principais novidades introduzidas pelo RGPD é a figura do encarregado de proteção de dados (EPD), ou na terminologia inglesa o *Data Protection Officer* (DPO), plasmada nos arts. 37.º e ss. A figura não existia na Diretiva 95/46/CE, no entanto não é uma novidade para diversos países da UE, cuja legislação interna já contemplava uma figura similar, com destaque para a lei alemã, onde o Regulamento nitidamente se inspirou[87]. A figura do EPD é vista como uma pedra angular da responsabilização, uma vez que facilita o cumprimento, ao mesmo tempo que atuam como intermediários entre as autoridades de controlo[88], os titulares dos dados e o responsável pelo tratamento. O EDP assegura que os direitos e liberdades dos titulares dados não são suscetíveis de serem violados aquando do tratamento. O EPD é uma pessoa à qual é atribuída a responsabilidade formal de assegurar que a empresa que o contrata está devidamente *compliance* com as regras da proteção de dados.

2. Designação obrigatória

Conforme o art. 37.º a nomeação de um EPD pelo responsável pelo tratamento dos dados ou pelo subcontratante é obrigatória para as autoridades ou organismos públicos, entidades que controlem regularmente dados pessoais em grande escala, entidades que controlem regularmente dados pessoais sensíveis em grande escala ou dados pessoais relativos a condenações penais e infrações. Diga-se, no entanto, que o RGPD se socorreu de conceitos indeterminados[89] para definir as situações em que é obrigatório nomear um DPO.

[87] A Lei Federal Alemã de Proteção de Dados (Bundesdatenschutzgesetz) impõe às entidades em que pelo menos 9 trabalhadores trabalhem em tratamento automatizado de dados, ou em que pelo menos 20 procedam ao tratamento não automatizado de dados, a nomeação de um encarregado de proteção de dados.
[88] Devendo para o efeito a sua designação ser notificada à CNPD, através de formulário próprio que consta do Anexo 8.
[89] Veja-se nesse sentido os esclarecimentos do GRUPO DE TRABALHO DO ARTIGO 29, "Orientações sobre os encarregados da proteção de dados (EPD)", (WP 243 rev.01), adotada em 13/12/2016.

Além disso, o art. 37.º n.º 4, do RGPD prevê que o responsável pelo tratamento, o subcontratante ou as associações e outros organismos representativos de categorias de responsáveis pelo tratamento ou subcontratantes possam facultativamente ou de acordo com a legislação do Estado-Membro designar um EPD[90].

O EPD deve ser designado com base nas suas *"qualidades profissionais",* e nos seus *"conhecimentos especializados"* em matéria de proteção de dados[91], entre os quais se considera essencial um adequado conhecimento da legislação e práticas tanto nacionais como europeias de proteção de dados, conhecimento das operações de processamento realizadas e conhecimento das tecnologias de informação e de segurança dos dados, de modo a promover uma cultura de proteção de dados dentro da organização.

O EPD tanto pode pertencer à estrutura interna do responsável pelo tratamento ou do subcontratante como ser contratado em regime de prestação de serviços, com as vantagens daí advenientes, como a independência e isenção no exercício das funções em caso de ser externo e o conhecimento aprofundado do funcionamento da organização no caso de ser interno.

3. Funções

As suas funções são exercidas com autonomia, o que significa que o EDP pode exercer outras funções, desde que não fique sujeito a um eventual conflito de interesses[92]. Em termos gerais, o EPD deve:

a. Ter capacidade para informar, aconselhar e monitorizar a administração da empresa/instituição, bem como os seus trabalhadores, a respeito das obrigações constantes do RGPD, assim como das outras disposições de proteção de dados em vigor na UE ou noutros Estados-Membros.

[90] Prevê-se que na Europa sejam necessários cerca de 28.000 EPD.
[91] Apesar de a lei não referir qualificações especiais para o exercício destas funções, o que se verifica nos países onde já existia esta figura é que elas são exercidas essencialmente por profissionais da área legal ou de IT.
[92] Os cargos suscetíveis de gerar conflitos no seio da organização podem incluir os cargos de gestão superiores, outras funções em níveis inferiores da estrutura organizacional, se esses cargos ou funções levarem à determinação das finalidades e dos meios de tratamento ou se o EPD externo for chamado a representar o responsável pelo tratamento e o subcontratante junto dos tribunais no âmbito de processos respeitantes a questões de proteção de dados.

b. Manter-se atualizado, recorrendo a formação e sensibilização para matérias de proteção de dados pessoais;
c. Realizar auditorias;
d. Aconselhamento em AIPD;
e. Colaborar com as autoridades de proteção de dados;
f. Relacionar-se com os titulares dos dados nomeadamente no âmbito do exercício dos seus direitos;
g. Estar vinculado à obrigação de sigilo ou de confidencialidade.

4. Direitos

Assim, em função da natureza das operações de tratamento e das atividades e dimensão da organização, deve ser concedido ao EPD:

a. Apoio ativo às funções do EPD por parte dos quadros de gestão superiores;
b. Tempo suficiente para que os EPD desempenhem as suas tarefas;
c. Apoio adequado em termos de recursos financeiros, materiais e humanos, sempre que necessário;
d. Acesso a outros serviços no seio da organização, para que os EPD possam receber apoio, contributos ou informações essenciais por parte destes outros serviços;
e. Formação contínua, pois tem direito a manter-se atualizado;
f. Acesso a todas as operações de tratamento e dados pessoais tratados pela entidade;
g. Não correr o risco de ser destituído ou penalizado pelo facto de exercer as funções.

Tudo sob pena de a empresa estar em risco de ser condenada no pagamento de uma coima por violação das obrigações e deveres decorrentes do RGPD.

CAPÍTULO VI: SANÇÕES

1. *Corporate Risk*

Os dados pessoais, que são na sua génese um "*direito do homem*", passam a ser também um "*Corporate Risk*", tendo em conta as coimas elevadas, que aliadas a uma maior fiscalização das autoridades de proteção de dados vão obrigar as organizações a olhar seriamente para as questões de privacidade. Nas palavras de BECCARIA, se o legislador surge como o *"hábil arquitecto cujo ofício é o de se opor às direções desastrosas da [força da] gravidade e de consolidar aquelas que contribuem para a segurança da construção"*[93], JOSÉ MOUTINHO E ANTÓNIO RAMALHO entendem que o legislador *"criou um edifício cuja excessiva solidez não se adaptará às forças das Constituições nacionais e ruirá sobre si mesma"*[94], isto porque *"a tutela dos bens jurídicos subjacentes à proteção de dados não se cria pela imposição externa de sanções desproporcionais ao agente da infração (…) devendo ser antes o fruto de um labor de sensibilização que faça brotar da consciência jurídica comum a compreensão dos referidos valores e a importância do seu respeito para tutela da pessoa humana"*[95]. Analisemos o seu regime.

2. Sanções

2.1.Natureza

Para a definição de crime e de contraordenação atendemos ao critério formal, *rectius*: nominal[96] – ou seja, se a prática de um facto declarado for passível de "*pena*" por lei (art. 1.º

[93] BECCARIA, Cesare Beccaria, *Dos delitos e das penas*, 2009, p. 73.
[94] MOUTINHO, José Lobo e RAMALHO, David Silva, Notas sobre o regime sancionatório da proposta Regulamento Geral sobre Proteção de Dados do Parlamento Europeu e do Conselho, in «Fórum de Proteção de Dados», n. º1, 2015, p. 31
[95] *Ibidem.*
[96] Segundo MOUTINHO, José Lobo, *Direito das contra-ordenações- Ensinar e Investigar*, 2008, p. 29 e 30 «É que para, por seu turno, se apurar quando estamos perante uma coima não parece bastar uma mera equivalência de natureza (sanção pecuniária não convertível em prisão), como demonstram os casos, não só das multas disciplinares, como das multas processuais e das multas aplicáveis às pessoas coletivas em caso de crime. Tudo vem, pois, a depender do facto de o texto da lei conter a palavra "coima" para designar a sanção correspondente ao facto ilícito. A opção por um critério nominal é, sem dúvida, de entre todas, a mais pragmática, na medida em que poupa o intérprete à questão da qualificação».

n.º 1 do CP), estaremos perante um crime, se a prática de um facto preencher um tipo legal no qual se comine uma "*coima*" (art. 1.º do RGCO) – estaremos perante uma contraordenação. Ora, as sanções aplicáveis às infrações puníveis por força do RGPD são expressamente qualificadas como "*coimas*"[97] e são impostas pelas autoridades de controlo, segundo o art. 83.º n.º 9. Desta qualificação decorre a aplicabilidade subsidiária do RGCO, isto é, naquilo que o art. 83.º for omisso este diploma colmatará as lacunas.

2.2.Quantum das coimas

Veja-se que o Regulamento estabelece no art. 83.º dois níveis de aplicação de coimas:

a. Coimas **até €20.000,00** ou, no caso de uma empresa, **até 4% do seu volume de negócios anual**, a nível mundial, correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado, para o caso de incumprimento de obrigações do responsável pelo tratamento e do subcontratante, previstas nos arts. 8.º, 11.º, 25.º a 39.º e 42.º e 43.º, de obrigações dos organismos de certificação, previstas nos arts. 42.º e 43.º e de obrigações do organismo de supervisão que se refere o art. 41.º n.º 4.
b. Coimas **até €10.000.000** ou, no caso de uma empresa, **até 2% do seu volume de negócios anual**, a nível mundial, correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado, estando em causa violações dos princípios básicos do tratamento, nos termos dos arts. 5.º a 7.º e 9.º, violações dos direitos previstos nos arts. 12.º a 22.º, violações das regras sobre transferências previstas nos arts. 44.º a 49.º, violações do direito do Estado-Membro adotado o abrigo do Capítulo IX (art. 85.º a 91.º) ou ainda violações dos art. 58. º n.º 1 e n.º 2.

2.2.1. Limites máximos e (não) mínimos

Do exposto, note-se que o RGPD criou um limite máximo sancionatório aplicável, no entanto não definiu os limites mínimos para as sanções que prevê, possibilitando assim a

[97] A versão alemã também qualifica as sanções como "GelbuBen", que são exatamente as sanções correspondentes à definição legal das contra-ordenações ("Gesetz über Ordnungswidrigkeiten"). Já a versão inglesa fala em "administrative fines" e a francesa em "amendes administratives".

aplicação de coimas de valor reduzido (no limite um euro, ou 3,74 euros se considerarmos a legislação portuguesa, mais concretamente o RGCO).

Perante uma moldura tão dilatada entre os montantes mínimos e máximos das coimas, as autoridades de controlo nacional são alvo de sérias dificuldades no momento de fixar a medida da coima concretamente aplicável.

Já há muito se tem apontado na doutrina que a fixação das sanções viola as normas da CRP, isto porque para além de suscitar problemas de proporcionalidade, na medida em que às infrações de ínfima gravidade possam fazer-se seguir sanções de gravidade inversamente severas, também se verifica um desrespeito pelo princípio da legalidade previsto no art. 29.º CRP já que *"(…) sanções com limites tão distantes entre si (…) traduziriam a transferência da função legislativa (ou normativa) para o aplicador da sanção e, portanto, a ausência de qualquer garantia contra o arbítrio"*[98].

A jurisprudência do Tribunal Constitucional no Ac. n.º 85/2012 e nos Acs. n.ºs 78/2013 e 612/2014, tem-se caracterizado de uma acrescida tolerância relativamente a coimas de elevada amplitude e com máximos extremamente elevados, apesar de algumas divergências a respeito da concretização dessa exigência.[99] Apesar de tudo e já como o velho ditado popular nos ensina *"quando a esmola é demais o pobre desconfia"*, com isto queremos dizer que não nos parece que o TC continue a ser tão benevolente em relações aos limites máximos das coimas. As sanções em causa não se mostram aptas a resistir às exigências de nenhuma das várias orientações assumidas pelo TC, até porque estamos a falar de coimas até €10.000.000 ou €20.000.000. Daí que se afigure necessário que a legislação nacional preveja um regime que, respeitando embora o topo estabelecido no Regulamento, possa também respeitar os princípios constitucionais da proporcionalidade e da legalidade.

Lembremo-nos que EDUARDO CORREIA, enquanto Ministro da Justiça, exorou no relatório do diploma que introduziu as contra-ordenações em Portugal: "*para obviar […] a perigos e abusos, submete-se a aplicação da coima a um estrito princípio de legalidade"*[100].

[98] MOUTINHO, José Lobo - Legislador português precisa-se. Algumas notas sobre o regime sancionatório no Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679) in «Fórum de Proteção de Dados», n.º 4, 2017, p. 4 a 57, em especial p. 56 e 57.
[99] Cf. Acs. TC n.º 574/95, 547/01 e 41/2004.
[100] Relatório do Decreto-Lei n.º 232/79, de 24 de Julho, nº 5.

2.3.Ne bis in idem

Como Portugal ainda não adotou legislação interna sobre proteção de dados após a entrada em vigor do RGPD, no presente momento, no nosso país, a Lei n.º 67/98, de 26 de outubro, a Lei da Proteção Dados Pessoais continua a ser a lei portuguesa em matéria de proteção de dados. Esta lei transpôs para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24/10/95, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que, ao momento presente, ainda se encontra em vigor. A este propósito, cumpre citar o comunicado[101] da Autoridade de Controlo portuguesa em matéria de proteção de dados, a CNPD, emitido no dia 25 de maio de 2018, que explicou que enquanto não for aprovada legislação nacional que complemente o RGPD e que venha a revogar a Lei n.º 67/98 de 26 de outubro, esta lei se mantém em vigor em tudo o que não contrarie o Regulamento.

Acontece que, muitos dos comportamentos presentemente previstos na Lei n.º 67/98 como ilícitos penais estão agora tipificados no RGPD como ilícitos contraordenacionais. Apesar de revestirem a natureza de contraordenação, as coimas são mais graves do que as multas previstas na lei nacional. Lançando mão do art. 20.º do RGCO, segundo o qual nos enuncia que se o mesmo facto constituir simultaneamente crime e contraordenação, será o agente sempre punido a título de crime. Tal punição a título de crime levará a uma violação do RGPD já que implicará a aplicação do regime penal português em detrimento do direito da UE, e consequentemente de um regime menos severo para as organizações.

Conforme CRISTINA PIMENTA COELHO[102] nos ensina *"deverá, assim, ser seriamente repensado o Direito Penal da proteção de dados, limitando-se os ilícitos penais a casos particularmente graves que envolvam um grande número de titulares de dados lesados ou em que haja um enriquecimento ilícito à custa de um tratamento abusivo de dados*

[101] Comunicado da CNPD - Aplicação do novo quadro legal de proteção de dados, de 25 de maio de 2018 *"…A partir de hoje, 25 de maio de 2018, o RGPD tem plena aplicação em toda a União Europeia e, por isso, também em Portugal. Enquanto não for aprovada legislação nacional que complemente o RGPD e que venha a revogar a Lei n.º 67/98, de 26 de outubro, esta lei manter-se-á em vigor em tudo o que não contrarie aquele diploma europeu. No que diz respeito aos tratamentos de dados pessoais relativos à prevenção, investigação e repressão criminal, a Lei n.º 67/98 tem integral aplicação, sem qualquer alteração, até à transposição da Diretiva 2016/680…"*

[102] PINHEIRO, Alexandre Sousa (coordenação) [et al.], *op. cit.,* p. 650.

pessoais, com um agravamento significativo da moldura penal face ao quadro atualmente vigente."

2.4. Responsáveis pelas contra-ordenações

Afinal quem são os responsáveis pelas coimas?

No contexto sancionatório, o Regulamento usa da expressão "*empresa*". O art. 4.º n.º 18 e n.º 19 definem empresa (*enterprise*) e grupo de empresas (*group of undertakings*). No entanto, a expressão "*empresa*" no regime sancionatório, não é a definida no RGPD. Através da leitura do considerando 150 extrai-se que o legislador pretendeu esclarecer a quem compete a responsabilidade ao expor que *"sempre que forem impostas coimas a empresas, estas deverão ser entendidas como empresas nos termos dos artigos 101.º e 102.º do TFUE para esse efeito".* Sucede que as regras do Tratado para que se apela versam sobre práticas anti concorrenciais e, embora usem a expressão "*empresa*", não incluem expressamente qualquer definição da mesma. Só através da jurisprudência do Tribunal de Justiça e dos Direitos nacionais (entre nós, art. 3.º do Regime Jurídico da Concorrência, aprovado pela Lei n.º 19/2012, de 8 de Maio[103]), podemos clarificar o conceito.

Implementa-se assim a dúvida sobre a noção de "*empresa*" utilizada nas normas sancionadoras que traz consigo a indeterminação sobre a sanção a aplicar a empresas integradas em grupos, uma vez que a coima a aplicar às "*empresas*" tem como máximo uma percentagem do seu *"volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior"* (cf. art. 83.º n.º 4, 5 e 6) e este é naturalmente diferente consoante se considere a empresa em si e por si ou o grupo de empresas em que ela se insira. Mais uma vez, exige-se legislação interna.

[103] De acordo com o qual se considera "*qualquer entidade que exerça uma atividade económica que consista na oferta de bens ou serviços num determinado mercado, independentemente do seu estatuto jurídico e do seu modo de financiamento" (n.º 1) e uma única empresa "o conjunto de empresas que, embora juridicamente distintas, constituem uma unidade económica ou mantêm entre si laços de interdependência decorrentes, nomeadamente: a) De uma participação maioritária no capital; b) Da detenção de mais de metade dos votos atribuídos pela detenção de participações sociais; c) Da possibilidade de designar mais de metade dos membros do órgão de administração ou de fiscalização; d) Do poder de gerir os respetivos negócios*" (n.º 2)

2.5. Ponderação na aplicação

O art. 83.º n.º 2 prevê o princípio da proporcionalidade e procede à enumeração dos fatores a ter em consideração na aplicação das coimas.

2.5.1. Princípio da proporcionalidade

O princípio da proporcionalidade prevê que as coimas possam ser aplicadas para além ou em vez das medidas referidas no art. 58.º n.º 2 al. a) a h) e j), ou seja, nem sempre a violação das normas do RGPD dará lugar à aplicação de coimas. Pode a autoridade de controlo decidir repreender, advertir ou ordenar a adoção de medidas que levem ao cumprimento do RGPD. Quer isto dizer que há sempre que fazer uma avaliação casuística para determinar se há ou não razões para aplicar uma coima.

2.5.2. Fatores

Este preceito esclarece que *"ao decidir sobre a aplicação de uma coima e sobre o montante da coima em cada caso individual"*, são tidas *"em devida consideração"* uma série de circunstâncias, entre as quais importa destacar a natureza, a gravidade e a duração da infração, o caráter intencional ou negligente, as categorias de dados afetados, o grau de cooperação com a autoridade de controlo, as medidas tomadas para atenuar os danos sofridos, o grau de responsabilidade ou eventuais infrações anteriores, a via pela qual a infração chegou ao conhecimento da autoridade de controlo, o cumprimento das medidas ordenadas contra o responsável pelo tratamento ou subcontratante, o cumprimento de um código de conduta ou quaisquer outros fatores agravantes ou atenuantes, entre outras.

Este elenco é não taxativo, o que permite aos Estados-Membros consagrar na legislação interna, outros critérios que se afigurem pertinentes, nomeadamente a situação económica do infrator.

2.5.3. Como ponderar?

Do exposto no art. 83.º n.º 2 não é possível distinguir com clareza os casos em que só deve ser aplicada a coima daqueles em que deve ser cumulada com medidas corretivas ou daqueles em que se impõe somente medidas corretivas.

No entanto, o RGPD atribui no seu art. 70.º n.º 1 al. k) competência ao Comité europeu para a proteção de dados[104], para elaborar *"diretrizes dirigidas às autoridades de controlo em matéria de aplicação das medidas a que se refere o artigo 58.º, n.ºs 1, 2 e 3, e de fixação de coimas nos termos do artigo 83.º"*. Neste ponto, uma vez mais reitera-se a importância de o legislador intervir, para que as sanções aplicadas sigam critérios proporcionais e equitativos.

3. Margem de discricionariedade dada aos Estados-Membros[105]

Em matéria de sanções existem vários pontos que deverão ser alvo de intervenção, alguns deles já referidos ao longo desse capítulo dedicado às sanções. Para além dos já referidos, o art. 84.º prevê que *"os Estados-Membros estabelecem as regras relativas às outras sanções aplicáveis em caso de violação do disposto no presente regulamento, nomeadamente às violações que não são sujeitas a coimas nos termos do art. 83.º [106], e tomam todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas".*

Fica, assim, claro que cabe aos Estados-Membros, não só a determinação de outras sanções (designadamente penais) para as violações ao Regulamento, como ainda a previsão

[104] De acordo com o art. 68.º do Regulamento, *"o Comité é composto pelo diretor de uma autoridade de controlo de cada Estado-Membro e da Autoridade Europeia para a Proteção de Dados, ou pelos respetivos representantes"* (n.º 3). *"Quando, num determinado Estado-Membro, haja mais do que uma autoridade de controlo com responsabilidade pelo controlo da aplicação do presente regulamento, é nomeado um representante comum nos termos do direito desse Estado-Membro"* (n.º 4).

[105] Como refere HENRIQUES, Miguel Gorjão, *Direito da União Europeia*, 2014, p. 297, a "autossuficiência normativa" de que gozam os Regulamentos, "não implica que todo e cada regulamento seja em si mesmo preciso e suficiente, ao ponto de dispensar qualquer atuação normativa por parte da União ou dos Estados membros. É o que acontece, no primeiro caso, com os Regulamentos adotados ao abrigo de processo legislativo e que prevêem a adoção de atos delegados ou de execução. E, no segundo caso, com aqueles (muitos) Regulamentos que, expressa ou implicitamente, habilitam os Estados membros a adotar medidas de aplicação legislativas, regulamentares, administrativas e financeiras necessárias à sua efetiva aplicação, reconhecendo a estes, inclusivamente, poderes discricionários".

[106] Por lapso, na publicação oficial diz-se "7983.º", resultado de não se ter eliminado o número do art. em que a matéria vinha tratada na Proposta, que era o 79.º.

de sanções aplicáveis às infrações que não são sujeitas a coimas nos termos do art. 83.º.[107] Assim sendo, parece indeclinável uma intervenção do legislador nacional, pelo menos para o efeito de prever e determinar os termos do sancionamento das infrações ao Regulamento não previstas nos n.ºs 4 a 6 do art. 83.º.

Em suma, em matéria sancionatória, apesar de estarmos perante um Regulamento, torna-se imperativo a mediação de lei portuguesa, que preveja as infrações ao Regulamento não diretamente nele tipificadas, que estabeleça normas incriminadoras e que segundo JOSÉ MOUTINHO E ANTÓNIO RAMALHO permita respeitar a reserva relativa da Assembleia da República[108] em matéria de regime geral das contra-ordenações, adiante-se que segundo este autor esta competência é violada com a aprovação do regime sancionatório apenas pelo RGPD.

Outro caso de "abertura" estabelecido aos Estados-Membros é o do art. 83.º n.º 7 em consonância com o considerando 150, que dispõe que cabe a estes determinar se as autoridades e organismos públicos deverão estar sujeitas a coimas, e em que medida o serão, sem prejuízo da possibilidade de aplicação de medidas de correção. Uma vez que não foi aprovada a lei portuguesa destinada a executar o RGPD, considera-se que não há base legal para a aplicação de coimas a entidades públicas. Diferente, foi o entendimento da CNPD, através da Deliberação n.º 984/2018, de 9 de outubro, homologada pela respetiva Presidente, Filipa Calvão, em 11 de outubro de 2018, que aplicou a uma entidade pública empresarial mais concretamente ao Centro Hospitalar Barreiro Montijo, EPE, uma coima de €400.000, ao abrigo do RGPD. Aguarda-se a decisão do tribunal que vier a recair sobre esta decisão da CNPD.

[107] O mesmo deriva do considerando 152

[108] MOUTINHO, José Lobo e RAMALHO, David Silva, Notas sobre o regime sancionatório da proposta Regulamento Geral sobre Proteção de Dados do Parlamento Europeu e do Conselho, in «Fórum de Proteção de Dados», n. º1, 2015, p. 20-35

CAPÍTULO VII: TUTELA JUDICIAL E RESPONSABILIDADE CIVIL

De modo a tornar eficazes as regras europeias de proteção de dados, é necessário estabelecer mecanismos que permitam aos indivíduos combater as violações de seus direitos e buscar compensação por qualquer dano sofrido. Vejamos, de seguida, quais são:

1. Via administrativa: direito de apresentar reclamação a uma autoridade de controlo

O n.º 1 do art. 77.º vem densificar o direito de reclamar perante a autoridade de controlo, esclarecendo que tal direito não interfere ou preclude o direito de utilizar outras vias, designadamente graciosas ou contenciosas.

Ou seja, a prévia reclamação perante a autoridade de controlo não é condição necessária para se poder recorrer contenciosamente, de acordo, aliás, com as regras de Direito Administrativo vigentes em Portugal. Mas também significa que é possível utilizar os meios graciosos normais (reclamação e recurso hierárquico) quando o ato em causa tenha sido praticado ao abrigo de disposições de direito administrativo, não sendo a autoridade de controlo a única entidade competente para apreciar queixas relativas à matéria da proteção de dados e a eventuais violações do RGPD.

De acordo com o n.º 1 do art. 77.º o titular dos dados pode apresentar uma reclamação a uma de três autoridades de controlo: à autoridade do Estado-Membro da sua residência habitual, à autoridade do seu local de trabalho ou à autoridade do local onde foi alegadamente praticada a infração. Este preceito dota o titular dos dados do poder de escolher aquela que considere mais conveniente aos seus interesses.

Em consonância com o disposto no art. 57.º n.º 1 al. f), o n.º 2 do art. 77.º estabelece um dever de informação, que impende sobre a autoridade de controlo onde foi apresentada a reclamação, estabelecendo que o reclamante deve ser informado do respetivo andamento e das suas conclusões e, inclusivamente, do seu direito a agir judicialmente contra a própria autoridade de controlo.

O RGPD exige que as autoridades de supervisão adotem medidas para facilitar a apresentação de queixas, como a criação de um formulário eletrónico de apresentação de reclamações[109]. As queixas devem ser investigadas e a autoridade supervisora deve informar a pessoa em causa do resultado do processo que trata da reclamação.

2. Via judicial

2.1.Contra uma autoridade de controlo

O n.º 1 do art. 78.º consagra o direito de recorrer judicialmente contra as decisões juridicamente vinculativas da autoridade de controlo, *maxime* daquelas que imponham coimas ou que desatendam reclamações. A Diretiva não consagrava este direito, decorria antes das normas do direito português uma vez que a CNPD, é uma entidade administrativa cujas decisões são passíveis de recurso judicial.

O direito de ação judicial contra uma autoridade de controlo não preclude o recurso às vias administrativas ou à resolução extrajudicial de litígios, nem é prejudicado pelo facto de estas terem sido utilizadas. O n.º 2 do art. 78.º explicita que o titular dos dados tem direito à via judicial se ocorrer omissão da autoridade de controlo no que toca à obrigação de informar o titular dos dados sobre o andamento e resultado de reclamações que lhe tenham sido apresentadas ao abrigo do disposto no art. 77.º, por mais de 3 meses.

O n.º 3 consagra uma regra de competência jurisdicional, estabelecendo que as ações contra as autoridades de controlo devem ser propostas nos tribunais dos Estados-Membros respetivos.

2.2.Contra um responsável pelo tratamento ou um subcontratante

Como resulta do n.º 1 do art. 79.º do RGPD, o direito de ação judicial quando se considere ter havido violação dos direitos que lhe assistem não preclude o recurso às vias

[109] Cf. Anexo 9 que disponibiliza o método de apresentação da queixa.

administrativas ou à resolução extrajudicial de litígios, nem mesmo é prejudicado pelo facto de estas terem sido utilizadas.

O n.º 2 consagra uma regra de competência jurisdicional, estabelecendo que as ações contra os responsáveis pelo tratamento ou contra os subcontratantes são, em princípio, propostas nos tribunais do Estado-Membro em que estes tenham estabelecimento. Atribui igualmente competência aos tribunais do Estado-Membro em que o titular dos dados tenha a sua residência habitual, exceto se o responsável pelo tratamento ou o subcontratante for uma autoridade no exercício dos seus poderes públicos.

3. Representação dos titulares dos dados

Em consonância com o disposto no considerando 142, e de modo a facilitar o exercício dos direitos dos titulares, o art. 80.º n.º 1 atribui ao titular dos dados o direito de mandatar um organismo, organização ou associação sem fins lucrativos que seja constituído ao abrigo do direito do Estados-Membros para o representar no tocante aos direitos previstos nos arts. 77.º a 79.º, quando considerar que estes foram violados. Exige-se que tal entidade tenha por objeto atividades relacionadas com a proteção dos dados pessoais e que os respetivos fins sejam de interesse público.

Essas entidades sem fins lucrativos devem ter objetivos estatutários dentro da esfera de interesse público e estar ativo no campo da proteção de dados. Podem apresentar a reclamação ou exercer o direito a recurso judicial em nome do titular dos dados. O Regulamento dá aos Estados-Membros a opção de decidir - de acordo com o direito nacional - se um organismo pode apresentar reclamações em nome de titulares de dados, sem ser mandatado por esses titulares de dados.

4. Direito de indemnização e responsabilidade

O resultado de uma ação administrativa ou judicial é o reconhecimento da existência de um dano perante uma violação de dados pessoais, nesse sentido o lesado deve dirigir-se ao responsável pelo tratamento e/ou ao subcontratante para exigir a indemnização a que se acha com direito. Deverá, assim, verificar-se o preenchimento dos vários pressupostos da

responsabilidade civil extracontratual, a saber a prática de ato ilícito, a culpa, a existência de um dano e o nexo de causalidade entre o ato ilícito culposo e o prejuízo sofrido.[110]

O n.º 2 do art. 82.º esclarece em que casos pode o subcontratante ser responsabilizado perante lesados, determinando que o mesmo só é responsável pelos danos causados pelo tratamento se não tiver cumprido as obrigações decorrentes do RGPD dirigidas especificamente aos subcontratantes (*vide* art. 28.º) ou se não tiver seguido as instruções lícitas do responsável pelo tratamento. Não conhecendo o lesado tais instruções, afigura-se que, em termos processuais, deverá demandar quer o responsável pelo tratamento, quer o subcontratante e aguardar pelas respetivas defesas. O regime ora consagrado no RGPD traduz-se numa inversão do ónus da prova, favorável aos interesses dos lesados, a quem basta demonstrar que os prejuízos sofridos foram causados, cabendo à outra parte demonstrar que não é responsável pelos danos, ou seja, que o facto não lhe pode ser imputável.

No seguimento do n.º 4, e em conformidade com o previsto no considerando 146, o n.º 5 do art. 82.º vem atribuir direito de regresso a quem, sendo corresponsável, pagou a totalidade da indemnização, prevendo que deve ser apurada a medida da responsabilidade de cada um. É imperativo apurar o *quantum* da responsabilidade de cada um.

O TJUE no Ac. de 6 de Outubro de 2015, Schrems, considerou que o esquema *Safe Harbor* tinha várias deficiências, o que comprometia os direitos fundamentais dos cidadãos da UE, nomeadamente o direito a um recurso legal efetivo., afirmando que *"uma regulamentação dessa proteção que implique uma ingerência nos direitos fundamentais garantidos (...) deve (...) estabelecer regras clara e precisas que regulem o âmbito e a aplicação de uma medida e imponham exigências mínimas, de modo a que as pessoas cujos dados pessoais estejam em causa disponham de garantias suficientes que permitam proteger eficazmente os seus dados contra os riscos de abuso e contra qualquer acesso e qualquer utilização ilícita desses dados. A necessidade de dispor destas garantias é ainda mais importante quando os dados pessoais sejam sujeitos a tratamento automático e exista um risco significativo de acesso ilícito aos mesmos (Acórdão Digital Rights Ireland).*

(...) uma decisão adotada ao abrigo desta disposição (...) não obsta a que uma autoridade de controlo (...) examine o pedido de uma pessoa relativo à proteção dos seus direitos e

[110] Sobre a matéria dos pressupostos da responsabilidade civil, *vide* PRATA, Ana [et al.], *Código Civil Anotado*, vol. I, 2017, p. 627 e ss.

liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que foram transferidos de um Estado-Membro para esse país terceiro, quando essa pessoa alega que o direito e as práticas em vigor neste último não asseguram um nível de proteção adequado."

É matéria assente no TJUE que o titular deve dispor de garantias suficientes para salvaguarda dos seus direitos, tendo por isso invalidado a Decisão 2000/520 sobre o *Safe Harbor* por a mesma não dispor destas.

CONCLUSÃO

Com o desenvolvimento desta dissertação não assumimos o propósito de fazer uma análise exaustiva do Regulamento, mas apenas uma análise prática e diretamente vocacionada para as principais implicações que o novo quadro legal acarreta.

Ora, se é verdade que as leis devem ter a capacidade de transmitir aos seus destinatários, de forma clara e precisa, os seus direitos e deveres, mais verdade ainda é que nem sempre assistimos a isto, e não raras vezes desencontramo-nos nos conceitos indeterminados e na complexidade da teia legislativa.

Sendo a proteção de dados uma área transversal na sociedade, permite-se afirmar que são raras, ou atrevemo-nos ainda a dizer, inexistentes, as organizações na União Europeia (e fora dela) que não estão sujeitas ao Regulamento aqui em estudo. É um regime jurídico que por incluir conceitos de difícil absorção e por estar interligado com outros domínios do conhecimento, designadamente a informática, exige um esforço acrescido e concertado, a ser desenvolvido com o auxílio dos Estados-Membros através da adoção de legislação interna que clarifique o regime.

Tendo em conta a atualidade e a pertinência das questões do Regulamento Geral de Proteção de Dados n.º 679/2016 UE do Parlamento Europeu e do Conselho, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, foi realizada uma análise detalhada sobre as principais imposições do Regulamento, tendo-se atendido em primeiro lugar ao seu enquadramento como direito fundamental e ainda à sua evolução legislativa.

Tendo sido Portugal o primeiro país a consagrar este direito na CRP, seria de esperar que esta fosse uma matéria alvo de um desenvolvimento acrescido. Porém, as preocupações na área da proteção de dados só começaram a surgir com a aprovação do RGPD, e em grande medida pela imposição de avultadas coimas.

Assim, considerámos de extrema importância lançar mão num primeiro momento do regime geral previsto no Regulamento, para que as organizações se encontrem em *compliance*, e, por conseguinte, imunes às coimas previstas.

Quando nos referimos a regime geral, falámos em primeiro lugar do seu âmbito de aplicação e dos princípios norteadores da atividade das organizações que desempenham um papel de bússola, e que por isso se tornam fundamentais para o cumprimento do Regulamento.

Não menos importante é ainda referir a panóplia dos direitos conferidos aos titulares dos dados. Com o Regulamento, os titulares dos dados beneficiaram de um conjunto de direitos, a que corresponde um conjunto de obrigações para as organizações, de modo a lhes ser dado um maior controlo sobre a sua privacidade.

Ainda neste âmbito e tendo em conta a particularidade e importância da matéria para o nosso estudo, foi realizada uma análise às obrigações que recaíram sobre o responsável pelo tratamento e sobre o subcontratante. Obrigações estas acrescidas, tendo em conta que foi descartado o modelo de autorização prévio. Atualmente as organizações têm de cumprir a legislação em vigor, decidir como a cumprir e ainda provar que a cumprem. Face ao exposto, o registo das atividades passou a ter uma relevância exacerbada nas instituições, pois trata-se de uma ferramenta imprescindível para a demonstração de cumprimento das normas relativas à proteção de dados pessoais.

Note-se, contudo, que a transferência para os responsáveis pelos tratamentos dos dados da responsabilidade pelo cumprimento do Regulamento (autorresponsabilização), e a canalização dos recursos públicos para a tarefa de controlo sucessivo, não é, *per se*, garantia de uma tutela eficaz dos direitos fundamentais no âmbito de tratamentos de dados pessoais.

A UE de modo a garantir que cada preceito do Regulamento seja levado na devida conta decidiu sancionar os incumprimentos com coimas que podem chegar até aos vinte milhões de euros ou 4% do valor anual de negócios. A União só não impõe que o direito à proteção de dados deva ser respeitado como coage as instituições a pensarem no mesmo.

Todavia, no quadro legal atual a autoridade administrativa não tem conhecimento de quem está a realizar tratamentos dados pessoais, com exceção de alguns casos. O que, em termos práticos pode resultar na aplicação de menos coimas do que o esperado, isto porque o controlo por parte da CNPD será limitado às situações em que há queixas ou denúncias de tratamentos ilícitos, notificação da violação dos dados pessoais ou se restrinja aos organismos públicos e às empresas de maior dimensão.

Daí termos igualmente abordado o direito que o titular dos dados pessoais possui de apresentar uma queixa e/ou intentar ação judicial contra um responsável pelo tratamento ou contra uma entidade subcontratante, nos termos do n.º1 do art. 79º do RGPD, bem como o direito previsto no art. 82º, n.º1, que prevê que qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do RGPD, tenha direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos.

Por tudo o que foi dito, constata-se que a União Europeia inaugurou a regulação do direito fundamental à proteção de dados. Agora cabe aos Estados-Membros investir na adoção de legislação interna e na investigação para consciencializar e auxiliar os cidadãos, de modo a que a aplicação do mesmo seja a mais coerente e correta!

BIBLIOGRAFIA

Livros:

1. BECCARIA, Cesare, *Dos delitos e das penas*, 3.ª edição, Lisboa: Fundação Calouste Gulbenkian, Serviço de Educação e Bolsas, Lisboa, 2009, ISBN 9789723108163.

2. CALVÃO, Filipa Urbano, *Direito da Proteção de Dados Pessoais: Relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina*, 1.ª edição, Universidade Católica, 2018, ISBN 978-989-8835-40-6.

3. CASTRO, Catarina Sarmento, *Direito da Informática, Privacidade e Dados Pessoais*, Almedina, Coimbra, 2005, ISBN 9789724024240.

4. Conselho da Europa e Agência de Direitos Fundamentais da União Europeia, Handbook *on European data protection law – 2018 edition*, Serviço das Publicações da União Europeia, [S.l.], 2018, ISBN 978-92-871-9849-5.

5. EHMANN, Eugen e SELMAYR Martin (coordenação) [et al.], *Datenschutz-Grundverordnung*, 2017.

6. FAZENDEIRO, Ana, *Regulamento Geral de Proteção de Dados- Algumas notas sobre o RGPD*, 2.ª edição, Almedina, Coimbra, 2018, ISBN 978-972-40-7154-1.

7. GOMES, Carla Amado, NEVES, Ana Fernanda e SERRÃO, Tiago (coordenação), *Comentários ao Novo Código do Procedimento Administrativo*, 2.ª edição, Associação Académica da Faculdade de Direito de Lisboa, Lisboa, 2015.

8. GONÇALVES, Maria Eduarda, *Direito da Informação, Novos Direitos e Formas de Regulamentação na Sociedade da Informação*, Almedina, Coimbra, 2003, ISBN 9789724019086.

9. GONÇALVES, Pedro, *Reflexões sobre o Estado Regulador e o Estado Contratante, Direito Público e Regulação*, Cedipre, Coimbra Editora, Coimbra, 2013, ISBN 9789723221473.

10. HENRIQUES, Miguel Gorjão, *Direito da União*, 7.ª edição, Coimbra: Almedina, Coimbra, 2014, ISBN 9789724055541.

11. MACHADO, Jónatas E. M., *Direito da União Europeia*, 1.ª edição, Coimbra: Wolters Kluwer Portugal- Coimbra Editora, Coimbra, 2010, ISBN 9789723218589.

12. MAÑAS, José Luís Piñar [et al.], *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de protección de datos*, Editorial Reus, 2016.

13. MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão, *Regulamento Geral de Proteção de Dados: Manual Prático*, 2.ª edição revista e ampliada, Vida Económica, 2018, ISBN 978-989-768-445-6.

14. MARTINS, Lourenço e MARQUES, Garcia, *Direito de Informática, Lições de Direito da Comunicação*, Almedina, Coimbra, 2000, ISBN 972-40-1399-5.

15. MOUTINHO, José Lobo, *Direito das contra-ordenações- Ensinar e Investigar*, Universidade Católica Editora, Lisboa, 2008, ISBN 9789725402078.

16. PINHEIRO, Alexandre Sousa (coordenação) [et al.], *Comentário ao Regulamento Geral de Proteção de Dados,* Almedina, Coimbra, 2018, ISBN 978-972-40-7786.

17. PINHEIRO, Alexandre Sousa, *Privacy Proteção de Dados Pessoais: A Construção Dogmática do Direito à identidade Informacional,* 1.ª edição, Associação Académica da Faculdade de Direito de Lisboa, Lisboa, 2015, ISBN 5606939008169.

18. PORTO, Manuel Lopes e ANASTÁCIO, Gonçalo (coordenação) [et al.], Tratado de Lisboa Anotado e Comentado, Almedina, Coimbra, 2012, ISBN 9789724046136.

19. PRATA, Ana [et al.], *Código Civil Anotado*, vol. I, Almedina, Coimbra, 2017, ISBN 9789724069937.

20. SALDANHA, Nuno, *Novo Regulamento Geral de Proteção de Dados- O que é? A quem se aplica? Como implementar?,* 1.ª edição, FCA, 2018, ISBN 978-972-72-2889-8.

Outros ficheiros:

1. EUROPEAN DATA PROTECTION SUPERVISIOR, *A grande oportunidade da Europa – Recomendações da AEPD sobre as opções da UE para a reforma da proteção de dados (Parecer 3/2015)*, 2015, disponível em: https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_pt.pdf (consultado a 29/01/2019).

2. GRUPO DE TRABALHO DO ARTIGO 29 "Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679", adotadas em 28 de novembro de 2017, sendo a última redação revista e adotada em 13 de abril de 2018, disponível em https://www.cnpd.pt/bin/rgpd/docs/wp259rev0.1_PT.pdf (consultado a 01/01/2019).

3. GRUPO DE TRABALHO DO ARTIGO 29, "Orientações sobre o direito à portabilidade dos dados", (16/PT WP 242 rev. 01), adotada em 13 de dezembro de 2016, com a última redação revista e adotada em 5 de abril de 2017, Disponível em https://www.cnpd.pt/bin/rgpd/docs/wp242rev01_pt.pdf (consultado a 15/01/2019)

4. GRUPO DE TRABALHO DO ARTIGO 29, "Orientações sobre os encarregados da proteção de dados (EPD)", (WP 243 rev.01), adotada em 13/12/2016, Disponível em https://www.cnpd.pt/bin/rgpd/docs/wp243rev01_pt.pdf (consultado a 07/01/2019).

5. GRUPO DE TRABALHO DO ARTIGO 29 "Orientações sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do

subcontratante", (WP 244 rev.01), adotada em 13/12/2016, Disponível em https://www.cnpd.pt/bin/rgpd/docs/wp244rev01_pt.pdf (consultado a 07/01/2019).

6. GRUPO DE TRABALHO DO ARTIGO 29 "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", (WP 248 rev.01), adotada em 04/04/2017, Disponível em https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf (consultado a 06/01/2019).

7. GRUPO DE TRABALHO DO ARTIGO 29 "Parecer 03/2014 relativo à notificação da violação de dados pessoais", (WP250rev.01), adotado em 03/10/2017, disponível em https://www.cnpd.pt/bin/rgpd/docs/wp250rev01_pt.pdf (consultado a 26/01/2019).

8. GRUPO DE TRABALHO DO ARTIGO 29 "Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»", (WP 169), adotado em 16/02/2010, Disponível em https://www.gpdp.gov.mo/uploadfile/others/wp169_pt.pdf (consultado a 02/01/2019).

9. GRUPO DE TRABALHO DO ARTIGO 29 "Parecer 8/2010 sobre a lei aplicável", (WP 179), adotado em 16/12/2010, Disponível em https://www.gpdp.gov.mo/uploadfile/others/wp179_pt.pdf (consultado a 05/10/2019).

10. GRUPO DE TRABALHO DO ARTIGO 29 "Parecer 15/2011 sobre a definição de consentimento" (WP187), adotado em 13/07/2011, Disponível em https://www.gpdp.gov.mo/uploadfile/others/wp187_pt.pdf (consultado a 26/11/2018).
11. GRUPO DE TRABALHO DO ARTIGO 29 "Parecer 06/2012 sobre o projeto de decisão da Comissão relativa às medidas aplicáveis à notificação da violação de

dados pessoais em conformidade com a Diretiva 2002/58/CE relativa à privacidade e às comunicações eletrónicas", (WP197), adotado em 12/07/2012, Disponível em https://www.gpdp.gov.mo/uploadfile/2016/0112/20160112121132800.pdf (consultado a 26/11/2018).

12. GRUPO DE TRABALHO DO ARTIGO 29 "Parecer 3/2013 sobre a limitação da finalidade", (WP 203), adotado em 02/04/2013, Disponível em https://www.gpdp.gov.mo/uploadfile/2017/0127/20170127113421380.pdf, (consultado a 01/12/2018).

13. GRUPO DE TRABALHO DO ARTIGO 29 "Parecer 05/2014 sobre técnicas de anonimização", (GT216), adotado em 10/04/2014, Disponível em https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf (consultado a 10/11/2018).

14. GRUPO DE TRABALHO DO ARTIGO 29 "Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE", (WP197), adotado em 12/07/2012, Disponível em https://www.gpdp.gov.mo/uploadfile/2016/0112/20160112121132800.pdf (consultado a 12/12/2018).

15. MOUTINHO, José Lobo - Legislador português precisa-se. Algumas notas sobre o regime sancionatório no Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679) in «Fórum de Proteção de Dados», n.º 4 (2017). Págs. 40–57. ISSN 2183-7066.

16. MOUTINHO, José Lobo e RAMALHO, David Silva, Notas sobre o regime sancionatório da proposta Regulamento Geral sobre Proteção de Dados do Parlamento Europeu e do Conselho, in «Fórum de Proteção de Dados», n. º1 (2015), Págs. 20-35. ISSN 2183-7066.

17. PINTO, Paulo Mota, *O Direito à Reserva sobre a Intimidade da Vida Privada in* Boletim da Faculdade de Direito - Universidade de Coimbra LXIX, 1993, p. 479-586.

Outros links na internet:

1. https://www.cnpd.pt

2. https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679

3. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt

4. https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_pt

5. https://ec.europa.eu/info/law/law-topic/data-protection/reform_pt

6. http://curia.europa.eu/juris/recherche.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-293%252F12&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=10905516

7. https://www.echr.coe.int/Pages/home.aspx?p=home

8. http://www.sg.pcm.gov.pt/sobre-nos/regulamento-geral-de-prote%C3%A7%C3%A3o-de-dados.aspx

9. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_pt

JURISPRUDÊNCIA

1. Acórdão do Tribunal de Justiça de 6 de Novembro de 2003, processo C-101/01 – Bodil Lindqvist, ECLI:EU:C:2003:596, disponível em http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9063485;

2. Acórdão do Tribunal de Justiça de 11 de Dezembro de 2014, processo C-212/13 – František Ryneš, ECLI:EU:C:2014:2428, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=9063485;

3. Acórdão do Tribunal de Justiça de 20 de Maio de 2003, processo C-465/00 – Österreichischer Rundfunk e outros, ECLI:EU:C:2003:294, disponível em http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48330&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=9063485;

4. Acórdão do Tribunal de Justiça de 8 de Abril de 2014, processo C-293/12 – Digital Rights Ireland e Seitlinger e outros, ECLI:EU:C:2014:238, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9063485;

5. Acórdão do Tribunal de Justiça de 30 de Maio de 2013, processo C-342/12 – Worten, ECLI:EU:C:2013:355, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=137824&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9063485;

6. Acórdão do Tribunal de Justiça de 7 de Maio de 2009, processo C-553/07 – Rijkeboer, ECLI:EU:C:2009:293, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=74028&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=9063485;

7. Acórdão do Tribunal de Justiça de 9 de Março de 2017, processo C-398/15 – Manni, ECLI:EU:C:2017:197, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=188750&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9063485;

8. Acórdão do Tribunal de Justiça de 27 de Setembro de 2017, processo C-73/16 – Puškár, ECLI:EU:C:2017:725, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=195046&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9063485;

9. Acórdão do Tribunal de Justiça de 16 de Dezembro de 2008, processo C-524/06 – Huber, ECLI:EU:C:2008:724, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=76077&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9063485;

10. Acórdão do Tribunal de Justiça de 24 de Novembro de 2011, processo C-468/10 – Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), ECLI:EU:C:2011:777, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=115205&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9063485;

11. Acórdão do Tribunal de Justiça de 19 de Outubro de 2016, processo C-582/14 – Breyer, ECLI:EU:C:2016:779, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9063485;

12. Acórdão do Tribunal de Justiça de 13 de Maio de 2014, processo C-131/12 – Google Spain e Google, ECLI:EU:C:2014:317, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9063485;

13. Acórdão do Tribunal de Justiça de 6 de Outubro de 2015, processo C-362/14 – Schrems, ECLI:EU:C:2015:650, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=9063485;

14. Acórdão do Tribunal de Justiça de 16 de Dezembro de 2008, processo C-73/07 – Satakunnan Markkinapörssi e Satamedia, ECLI:EU:C:2008:727, disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=76075&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=9063485;

15. Acórdão do Tribunal Europeu dos Direitos do Homem de 18 de Novembro de 2014, processo 22427/04 – Case of Cemalettin Canli v. Turkey, disponível em https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-89623%22]};

16. Acórdão do Tribunal Europeu dos Direitos do Homem de 17 de Julho de 2008, processo 20511/03 – Case of I. v. Finland, disponível em https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-87510%22]};

17. Acórdão do Tribunal Europeu dos Direitos do Homem de 4 de Dezembro de 2008, processo 30562/04 e 30566/04 – Case of S. and Marper v. The United Kingdom, disponível em https://hudoc.echr.coe.int/spa#{%22fulltext%22:[%22s.%20v.%20marper%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-90051%22]};

18. Acórdão do Tribunal Europeu dos Direitos do Homem de 18 de Setembro de 2014, processo 21010/10 – Case of Affaire Brunet v. France, disponível em http://hudoc.echr.coe.int/fre?i=001-146389;

19. Acórdão do Tribunal Europeu dos Direitos do Homem de 27 de Outubro de 2009, processo 21737/03 – Case of Haralambie v. Romania, disponível em http://hudoc.echr.coe.int/fre?i=001-123267;

20. Acórdão do Tribunal Europeu dos Direitos do Homem de 28 de Abril de 2009, processo 32881/04, Case of K. H. and Others v. Slovakia, disponível em http://hudoc.echr.coe.int/fre?i=001-92418;

21. Acórdão do Tribunal Europeu dos Direitos do Homem de 06 de Junho de 2006, processo 62332/00 – Case of Segerstedt-Wiberg and Others v. SWEDEN, disponível em http://hudoc.echr.coe.int/eng?i=001-75591;

22. Acórdão do Tribunal Europeu dos Direitos do Homem de 15 de Dezembro de 2009, processo 648/10- Case of Y v. Turkey, disponível em http://hudoc.echr.coe.int/eng?i=001-183961;

23. Acórdão do Tribunal Constitucional n.º 85/2012, de 15 de Fevereiro de 2012, processo 367/11, 1.ª secção, relatora Conselheira Pamplona Oliveira, disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20120085.html;

24. Acórdão do Tribunal Constitucional n.º 574/95, de 18 de Outubro de 1995, processo 357/94, 2.ª secção, relator Conselheiro Messias Bento, disponível em http://www.tribunalconstitucional.pt/tc/acordaos/19950574.html;

25. Acórdão do Tribunal Constitucional n.º 547/01, de 07 de Dezembro de 2001, processo 481/00, 3.ª secção, relatora Conselheira Maria dos Prazeres Beleza, disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20010547.html;

26. Acórdão do Tribunal Constitucional n.º 41/2004, de 14 de Janeiro de 2004, processo 375/03, 2.ª secção, relator Conselheiro Fernanda Palma, disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20040041.html;

27. Acórdão do Tribunal Constitucional n.º 78/2013, de 31 de Janeiro de 2013, processo 624/12, 2.ª secção, relator Conselheiro João Cura Mariano, disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20130078.html;

28. Acórdão do Tribunal Constitucional n.º 612/2014, de 30 de Setembro de 2014, processo 227/14, 3.ª secção relator Conselheiro Carlos Fernandes Cadilha, disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20140612.html.

LEGISLAÇÃO CONSULTADA

1. Carta dos Direitos Fundamentais da União Europeia, adotada em 07 de Dezembro de 2000, OJ C 326, 26.10.2012, p. 391–407, ELI: http://data.europa.eu/eli/treaty/char_2012/oj;

2. Código Civil, aprovado pelo Decreto-lei nº 47 344, de 25 de Novembro de 1966, na versão decorrente da aplicação da Lei n.º 64/2018, de 29 de outubro;

3. Código Penal, aprovado pelo Decreto-lei n.º 48/95, de 15 de Março, na versão decorrente da aplicação da Lei n.º 44/2018, de 9 de agosto;

4. Convenção Europeia dos Direitos do Homem, adotada em 04 de Novembro de 1950, aprovada para ratificação através da Lei n.º 65/78, de 13 de Outubro, publicada em Diário da República n.º 236, I Série de 13 de Outubro de 1978;

5. Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, adotada em 28 de Janeiro de 1981, aprovada para ratificação pela Resolução da Assembleia da República n.º 23/93, de 9 de Julho e retificada pela Retificação n.º 10/93, de 20 de Agosto, publicada no Diário da República, I Série-A, n.º 195/93;

6. Constituição da República Portuguesa, na versão decorrente da aplicação da Lei Constitucional n.º 1/2005 - Diário da República n.º 155/2005, Série I-A de 2005-08-12;

7. Decreto-Lei n.º 232/79, de 24 de Julho que institui o ilícito de mera ordenação social, publicado no Diário da República n.º 169/1979, Série I de 1979-07-24;

8. Decreto-Lei n.º 433/82, de 27 de Outubro que institui o ilícito de mera ordenação social, na versão decorrente da aplicação da Lei n.º 109/2001, de 24 de Dezembro, publicado no Diário da República n.º 296/2001, Série I-A de 2001-12-24;

9. Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, JO L 281 de 23.11.1995, p. 31—50, ELI: http://data.europa.eu/eli/dir/1995/46/oj;

10. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, JO L 119 de 4.5.2016, p. 89—131, ELI: http://data.europa.eu/eli/dir/2016/680/oj;

11. Diretiva 2002/58/CE, do Parlamento e do Conselho, de 12 de Julho de 2002, JO L 201 de 31.7.2002, p. 37—47, ELI: http://data.europa.eu/eli/dir/2002/58/oj;

12. Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março de 2006, JO L 105 de 13.4.2006, p. 54—63, ELI: http://data.europa.eu/eli/dir/2006/24/oj;

13. Diretiva 68/151/CEE, do Conselho, de 9 de Março de 1968, JO edição especial portuguesa, Cap. 17, Vol. 001 p. 3-6, ELI: http://data.europa.eu/eli/dir/1968/151/oj;

14. Tratado sobre o Funcionamento da União Europeia, na decorrência da redação que lhe é dada pelo Tratado de Lisboa adotado em 13 de Dezembro de 2007, versão consolidada publicada no Jornal Oficial da União Europeia, C 202, 7 de junho de 2016;

15. Lei n.º 19/2012, de 8 de Maio, que aprova o novo regime da concorrência, na versão que lhe foi dada pela Lei n.º 23/2018, de 05 de Junho, publicada no Diário da República n.º 107/2018, Série I de 2018-06-05;

16. Lei n.º 67/98, de 26 de outubro, publicado em Diário da República n.º 247/1998, Série I-A de 1998-10-26, na versão que lhe foi dada pela Lei n.º 103/2015, de 24 de agosto, publicada no Diário da República n.º 164/2015, Série I de 2015-08-24;

17. Proposta de Lei n.º 120/XIII, publicada no Diário da Assembleia da República, II Série A n.º 89/XIII/3 de 26 de março de 2018;

18. Regulamento Geral de Proteção de Dados (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, JO L 119 de 4.5.2016, p. 1—88, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

ANEXOS

ANEXO 1: ARTIGO 35.º DA CONSTITUÇÃO DA REPÚBLICA PORTUGUESA

Artigo 35.º

Utilização da informática

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

ANEXO 2: FORMULÁRIO PARA EXERCER DIREITOS

FORMULÁRIO

_____ (NOME), portador do cartão de Cidadão n.º _____, válido até ___/___/_____, declara para os devidos efeitos, que nos termos dos artigos 12.º a 22.º do Regulamento Geral de Proteção de Dados 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, pretende exercer (selecionar a opção pretendida):

	Direito de acesso
	Direito de retificação
	Direito de apagamento/esquecimento
	Direito à limitação do tratamento
	Direito de portabilidade dos dados
	Direito de oposição
	Direito de não sujeição a decisões individuais automatizadas, incluindo a definição de perfis
	Direito a reclamação
	Direito de retirar o seu consentimento

Nos termos e com os seguintes fundamentos:

_____

_____

_____

Para dar cumprimento ao direito exercido dou expressamente consentimento para a resposta ser enviada para: _____

Data: ___/___/_____

_____

(Assinatura conforme documento de identificação)

ANEXO 3: POLÍTICA DE PRIVACIDADE

POLÍTICA DE PROTEÇÃO DE DADOS

Considerando que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito a XXX, LDA. vem definir a sua Política de Proteção de Dados.

É nosso compromisso preservar a sua privacidade, pois encaramos seriamente o tratamento dos dados pessoais que recolhemos no âmbito da nossa atividade.

Com esta Política de Proteção de Dados pretendemos esclarecê-lo o melhor possível, afirmando o nosso compromisso e respeito para com as novas regras de privacidade e de proteção de dados pessoais, adotadas no âmbito do Regulamento Geral de Proteção de Dados (Regulamento UE 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016).

Tendo em conta que o já referido Regulamento, este nos seus artigos 13.º e 14.º, impõe o fornecimento de certas informações aos titulares dos dados, estas consideram-se prestadas pela leitura da presente política.

Quem é o responsável pelo tratamento dos seus dados pessoais?

O Responsável pelo tratamento dos seus dados pessoais é:

XXX, LDA., com sede em Rua xxx n.º xx, 9500-000, Ponta Delgada, São Miguel, Açores.

Contactos: Telefone xxxxxxxxx; Fax xxxxxxxxx; e-mail: xxxxx@xxxxx.pt

Tal entidade será referenciada, daqui em diante, nesta Política de Privacidade, como XXX.

O que são dados pessoais?

Entende-se por "dado pessoal" qualquer informação, de qualquer natureza e independentemente do respetivo suporte, relativa a uma pessoa singular identificada ou identificável (titular dos dados).

É considerada identificável a pessoa que possa ser reconhecida, direta ou indiretamente, em especial por referência a um identificador, como por exemplo, um nome, número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Como recolhemos os seus dados?

Alguns dos dados pessoais são recolhidos através de interações consigo e obtemos alguns deles através dos seus acessos no nosso website. Deste modo, tanto recolhemos informações pessoais, como dados do seu dispositivo.

Que dados pessoais recolhemos?

A XXX recolhe e trata os dados pessoais necessários à prestação dos seus serviços e/ou subscrições.

- Quando nos contacta de forma a diligenciar um contrato serão necessários **dados pessoais** como: o seu nome, idade, profissão, número do cartão de cidadão/bilhete de identidade, contribuinte fiscal, data de nascimento, dados de contacto (e-mail, número de telefone e endereço postal).

  Tendo em conta que a transmissão de alguns destes dados é obrigatória, se estes não forem fornecidos, a XXX poderá não disponibilizar o serviço/contrato solicitado.

- O nosso website não requer qualquer forma de registo, havendo assim a possibilidade de o visitar sem se identificar. Todavia, com o acesso ao nosso website são recolhidos de forma automática um conjunto de dados informáticos, que são gravados de forma temporária em ficheiros próprios, sendo eliminados de forma também automática após determinado período. A recolha destes dados tem objetivos meramente técnicos. Os dados em questão são os seguintes: endereço do processador requerente; data e hora de acesso; nome do ficheiro transferido; volume dos dados transmitidos; indicação sobre se a transferência foi efetuada com êxito; dados de identificação do software do navegador e do sistema operativo; sítio Web a partir do qual acedeu ao nosso sítio; nome do fornecedor de serviço de Internet.

O nosso website tem ao dispor dos seus visitantes um serviço gratuito de subscrição de newsletters. Para poder usufruir deste serviço terá necessariamente de fornecer o seu endereço de e-mail no campo existente para o efeito, podendo a subscrição das newsletters ser cancelada a todo o tempo, bastando, para o efeito, seguir as indicações nesse sentido presentes no final de cada newsletter.

Quais são as finalidades da recolha dos seus dados?

Usamos os seus dados pessoais para os seguintes fins:

- **Prestação e gestão dos serviços contratados/subscritos**

Sempre que for parte do contrato ou se as diligências forem realizadas a seu pedido, os seus dados serão utilizados em todos os atos necessários para a execução deste mesmo contrato.

Ocasionalmente, podemos contactá-lo por e-mail e/ou SMS por motivos administrativos.

Uma vez que estas comunicações são de natureza operacional e não são realizadas para efeitos de marketing, continuará a recebê-las mesmo que tenha optado por não receber comunicações de marketing.

Também utilizaremos os seus dados pessoais para responder aos seus pedidos, sugestões ou contactos e, claro, para melhorar os nossos serviços.

- **Comunicações de Marketing**

Caso nos tenha indicado que deseja receber a nossa Newsletter, começará a receber newsletters por parte da XXX, com as melhores oportunidades de negócio no ramo, divulgação de novos produtos, eventos, feiras, campanhas, etc.

Importa realçar que os seus dados pessoais nunca serão partilhados com outras empresas para efeitos de marketing, a não ser com o seu consentimento.

- **Estudo, melhoria, desenvolvimento e adequação dos nossos serviços aos seus interesses e necessidades**

Através do tratamento dos seus dados pessoais, conseguimos, adaptar, os nossos serviços às suas necessidades e preferências.

Também podemos recolher informações sobre como utiliza o nosso website, nomeadamente que produtos procura, para percebermos quais são os seus gostos e preferências.

- **Cumprir os nossos objetivos administrativos e comerciais.**

Os objetivos de negócio, para os quais usamos as suas informações, incluem contabilidade, faturação e auditoria, verificação de cartão de crédito ou outro, análise de fraude, segurança, efeitos jurídicos e processuais, estudos estatísticos e desenvolvimento e manutenção de sistemas.

- **Cumprir com exigências legais (prevenção de fraudes e investigações)**

Por obrigação legal, nomeadamente tendo por base a Lei 83/2017, de 18 de Agosto, que estabelece as medidas de combate ao branqueamento de capitais e ao financiamento do terrorismo podemos ter de fornecer os seus dados pessoais a certas entidades.

Quais são os fundamentos jurídicos do processamento dos seus dados pessoais?

A nossa legitimidade para proceder ao presente tratamento dos seus dados pessoais encontra-se prevista:

1. Na alínea b) do n.º 1 do art. 6.º do RGPD quando a recolha e processamento dos seus dados pessoais baseia-se principalmente na **relação contratual** que tem connosco;

2. Na alínea a) do n.º 1 do art. 6.º do RGPD quando lhe enviamos as nossas newsletters, pois é com base no seu **consentimento** que as disponibilizámos**;**

3. Na alínea c) do n.º 1 do art. 6.º do RGPD se o tratamento for necessário para o cumprimento de uma **obrigação jurídica** a que estamos sujeitos.

Por quanto tempo serão conservados os dados?

O período durante o qual os dados são armazenados varia consoante a finalidade para que foram recolhidos, caso não exista uma exigência legal específica.

Existem, no entanto, requisitos legais que obrigam a conservar os dados por um determinado período.

Quais são os direitos enquanto titulares dos dados?

Tem o direito de solicitar ao responsável pelo tratamento dos dados, o exercício dos seguintes direitos:

1. **Direito de acesso do titular dos dados:** tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às informações previstas no Regulamento Geral de Proteção de Dados.

2. **Direito de retificação:** o titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito.

3. **Direito ao apagamentos dos dados ("direito a ser esquecido"):** o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique, nomeadamente, um dos seguintes motivos: 1) os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; 2) o titular retira o consentimento em que se baseia o tratamento dos dados (quando o mesmo se baseie no consentimento) e se não existir outro fundamento jurídico para o referido tratamento; 3) o titular opõe-se ao tratamento e não existem interesses legítimos prevalecentes que justifiquem o tratamento; 4) os dados pessoais foram tratados ilicitamente; 5) os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; 6) os dados pessoais foram recolhidos no contexto de serviços da sociedade da informação.

   Contudo, importa informar que este direito comporta algumas exceções.

4. **Direito à limitação do tratamento:** o titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma das seguintes situações: a) contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; b) 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; c) 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; d) se tiver oposto ao tratamento, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

5. **Direito de oposição:** o titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente 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 num processo judicial.

   Quando os dados pessoais 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 os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.

   Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim.

6. **Direito de portabilidade dos dados:** o titular dos dados tem, nos termos e nas condições definidas na lei, o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, 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: a) O tratamento se basear no consentimento ou num contrato; e b) O tratamento for realizado por meios automatizados.

7. **Direito de não ficar sujeito a nenhuma decisão automatizada, incluindo definição de perfis:** 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 significativamente de forma similar.

8. **Direito de retirar o consentimento:** se o tratamento dos dados se basear no consentimento, o titular dos dados tem o direito de retirar o seu consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado.
9. **Direito ao conhecimento da existência de uma violação de dados**
10. **Direito de apresentar reclamação a uma autoridade de controlo:** o titular dos dados tem o direito de, a qualquer momento, apresentar uma reclamação à autoridade de supervisão e controlo competente, ou seja, à Comissão Nacional de Proteção de Dados (CNPD), sediada na Avenida D. Carlos I, n.º 134, 1.º, 1200-651 Lisboa, com os seguintes contactos: telefone - +351213928400; fax - +351213976832; email – geral@cnpd.pt

O exercício destes direitos é gratuito, exceto se fizer pedidos injustificados ou excessivos. Neste caso, pode ser cobrada uma taxa razoável baseada em custos administrativos.

Caso pretenda exercer qualquer um dos direitos mencionados, deverá contactar-nos através:

1. De um pedido enviado, por carta registada, para:

   XXX, LDA.

   Rua XXX, 9500-000

   Ponta Delgada, São Miguel, Açores

2. De formulário próprio, disponível na nossa loja, situada na morada acima referida
3. De um pedido enviado, por endereço de correio eletrónico, para: xxxxx@xxxxx.pt

Há a possibilidade de divulgação dos dados pessoais?

Os seus dados pessoais podem ser comunicados a prestadores de serviços da XXX, subcontratados ou terceiros, para efeitos da prestação dos serviços, e a autoridades judiciais, fiscais e regulatórias, com a finalidade do cumprimento de imposições legais.

Assumimos o compromisso de o proteger

Porque assumimos o compromisso de o proteger adotámos as medidas técnicas e organizativas que foram adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com a legislação aplicável, nomeadamente:

- Assegurámos que o tratamento é lícito, leal e transparente, enquadrado no que foi transmitido ao titular no momento da recolha e o titular dos dados poderá verificar como é feito o tratamento desses mesmos dados;
- Os dados são recolhidos para finalidades determinadas, explícitas e legítimas, não sendo tratados para finalidades distintas a menos que exista um claro interesse superior que o preveja;
- Os dados pessoais recolhidos são adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para os quais são tratados;
- Os dados são exatos e atualizados sempre que necessário;
- Os dados são conservados durante o tempo estritamente necessário e permitem a identificação dos titulares dos dados apenas durante o período necessário para as finalidades quais são tratados, assim foi implementada uma política de manutenção, arquivo e apagamento dos dados de modo a garantir que esses não sejam conservados durante um período superior ao estritamente necessário;
- Os dados são tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, bem como de todos os demais direitos que lhe assistem enquanto titular de dados;
- Assegurámos a anonimização dos dados pessoais, sempre que tal for exigido;
- Respeitámos o sigilo profissional em relação aos dados pessoais tratados;

- A XXX definiu regras claras de contratualização do tratamento de dados pessoais com os seus subcontratantes e exige que estes adotem as medidas técnicas e organizacionais necessárias para protegê-los.

Não obstante todas as medidas de segurança adotadas, é necessário alertar que quando acede à Internet, deve tomar, regularmente, precauções e adotar medidas de segurança adicionais, nomeadamente através da utilização de um computador e browser atualizados.

A XXX poderá proceder, a qualquer momento, a modificações ou atualizações à presente Política de Proteção de Dados, alterações essas que serão devidamente atualizadas nas nossas Plataformas.

Sugerimos assim que as consulte regularmente para estar a par de eventuais alterações.

Para qualquer pedido ou esclarecimento não hesite em contactar-nos.

ANEXO 4: CONTRATO DE SUBCONTRATAÇÃO

CONTRATO DE SUBCONTRATAÇÃO EM MATÉRIA DE PROTEÇÃO DE DADOS PESSOAIS

ENTRE: ----------

PRIMEIRO OUTORGANTE: XXXXX, LDA., pessoa coletiva n.º XXXXXXXXX, matriculada na Conservatória do Registo Comercial de Ponta Delgada-Açores, com sede na Rua XXXXX n.º XX, 9500-000 Ponta Delgada, São Miguel, neste ato devidamente representada pelo sócio gerente XXX XXX XXX, adiante designado "**RESPONSÁVEL PELO TRATAMENTO**". ----------

E ----------

SEGUNDO OUTORGANTE: XXXXX, LDA., pessoa coletiva n.º XXXXXXXXX, matriculada na Conservatória do Registo Comercial de Ponta Delgada-Açores, com sede na Rua XXXXX n.º XX, 9500-000 Ponta Delgada, São Miguel, neste ato devidamente representada pelo sócio gerente XXX XXX XXX, adiante designada "**SUBCONTRATANTE**". ----------

CONSIDERANDO QUE:

a) Ambas as partes chegaram a contrato anteriormente (a seguir designado "contrato principal"), que regula a prestação de serviços pelo subcontratante ao responsável pelo tratamento; ----------

b) A prestação habitual destes serviços requer necessariamente o processamento de dados pessoais; ----------

c) Alguns dos dados tratados não pertencem aos aqui Outorgantes; ----------

d) O responsável pelo tratamento apenas recorre ao aqui subcontratante porque este apresenta garantias suficientes de execução de medidas técnicas e organizativas

adequadas de forma a que o tratamento satisfaça os requisitos do Regulamento Geral de Proteção de Dados 2016/679, do Parlamento Europeu e do Conselho, de 27 de Abril 2016 (adiante designado RGPD), e assegura a defesa dos direitos do titular dos dados. ----------

Entre os Outorgantes é celebrado, de boa fé, o referido contrato de forma a ajustá-lo aos requisitos do Regulamento Geral sobre a Proteção de Dados Pessoais, nos termos e condições das cláusulas seguintes: ----------

CLÁUSULA PRIMEIRA

(Objeto)

1. Define-se como objetivos primordiais deste contrato: ----------

a) Garantir e reforçar as obrigações estabelecidas, para ambas as partes, pelo Regulamento 2016/679, do Parlamento Europeu e do Conselho, de 27 de Abril 2016, relativo à Proteção de Dados; ----------

b) Documentar todo o acesso limitado de dados pessoais por parte do subcontratante; -

c) Fortalecer o quadro de confidencialidade que deve ser mantido pelo subcontratante, como entidade responsável pelo processamento de tais dados pessoais, em resultado da realização dos serviços regulamentados no contrato principal. ----------

CLÁUSULA SEGUNDA

(Duração)

1. O presente contrato entrará em vigor no dia da sua assinatura e terá o mesmo prazo que o contrato principal. ----------

2. Os acordos de proteção de dados, confidencialidade e sigilo serão válidos por tempo indeterminado, continuando em vigor após a rescisão do contrato principal, por qualquer razão. ----------

CLÁUSULA TERCEIRA

(Natureza)

O subcontratante encontra-se vinculado ao responsável pelo tratamento, por um contrato de prestação de serviços na área informática, executando todos os serviços nesta área e assumindo a responsabilidade técnica pela mesma. ----------

CLÁUSULA QUARTA

(Finalidade)

1. O subcontratante tem acesso a dados pessoais, disponibilizados pelo responsável pelo tratamento, estritamente necessários para as finalidades acordadas no contrato principal, nomeadamente para: ----------

a) Criação/evolução de um sistema informático de registo de dados de clientes vendedores, de potenciais clientes compradores e de comerciais; ----------

b) Apoio na utilização do sistema de faturação e subsequente submissão via portal das Finanças; ----------

CLÁUSULA QUINTA

(Tipo de dados pessoais e as categorias dos titulares dos dados)

1. O subcontratante tem acesso aos seguintes dados pessoais: ----------

a) Dos clientes vendedores: nome, NIF, contactos, morada, dados dos imóveis de que são proprietários; ----------

b) Dos potenciais compradores: nome, contactos; ----------

c) Dos comerciais: nome, contactos, morada, NIF, BI, IBAN. ----------

CLÁUSULA SEXTA

(Obrigação de apresentar garantias e defender direitos)

1. Sobre o subcontratante recai a obrigação de: ----------

a) Apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de forma a que o tratamento dos dados seja conforme com os requisitos do RGPD; ----------

b) Assegurar a defesa dos direitos do titular dos dados. ----------

CLÁUSULA SÉTIMA

(Contratação de outro subcontratante)

1. O subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral. --

a) Em caso de 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. ----------

2. Se o subcontratante contratar outro subcontratante para a realização de operações específicas de tratamento de dados por conta do responsável pelo tratamento, são impostas a esse outro subcontratante, as mesmas obrigações em matéria de proteção de dados, aqui estabelecidas entre o responsável pelo tratamento e o subcontratante, nomeadamente: ----------

a) Apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de forma a que o tratamento seja conforme com os requisitos do presente Regulamento; ----------

b) Assegurar a defesa dos direitos do titular dos dados; ----------

3. Se esse outro subcontratante não cumprir as suas obrigações em matéria de proteção de dados, o subcontratante inicial continua a ser plenamente responsável, perante o responsável pelo tratamento, pelo cumprimento das obrigações desse outro subcontratante. ----------

CLÁUSULA OITAVA

(Instruções)

No tratamento dos dados pessoais o subcontratante obedecerá às 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. ----------

CLÁUSULA NONA

(Confidencialidade das pessoas autorizadas)

1. O subcontratante declara ter conhecimento de que todas as informações e, em particular, as informações pessoais, que lhe foram facultadas em resultado da prestação dos serviços, são absolutamente confidenciais e, nesse sentido, obriga-se sob sua total responsabilidade a: ----------

a) Utilizar a informação exclusivamente para o fim para o qual foi facilitada de acordo com o contrato principal, comprometendo-se também a não a usar de qualquer forma que exceda a referida finalidade; ----------

b) Não divulgar a informação nem a comunicar sob nenhuma forma a terceiros, nem mesmo para sua conservação; ----------

c) Garantir que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade, durante e após o término do relacionamento com o responsável pelo tratamento; ----------

2. O subcontratante é obrigado a manter o sigilo absoluto sobre as informações que teve conhecimento como consequência da prestação do objeto de serviço do contrato principal e compromete-se a exigir o mesmo dever de sigilo aos seus funcionários que intervêm em qualquer fase do processamento de dados pessoais. ----------

3. Esta obrigação mantém-se para o subcontratante, mesmo depois de terminar a sua relação com o responsável pelo tratamento, e para os seus colaboradores, mesmo depois de terminada a sua relação com o subcontratante. ----------

CLÁUSULA DÉCIMA

(Segurança do Tratamento)

1. 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 subcontratante aplica 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 a cifragem dos dados pessoais; ----------

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

c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; ----------

d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento; ----------

e) Aprovação de uma política de proteção de dados pessoais, que contemple a revisão periódica das práticas de gestão de dados pessoais; ----------

f) Nomeação de um ponto de contacto para questões relacionadas com a segurança e privacidade dos dados pessoais; ----------

g) Definição de responsabilidade pela proteção de dados pessoais; ----------

h) Identificação dos colaboradores com acesso a dados pessoais e execução de formação adequada sobre melhores práticas para práticas para proteção de dados; -

i) Implementação de procedimento de avaliação do risco dos processos que envolvam o tratamento de dados pessoais; ----------

j) Caso exista tratamento de dados de categoria especial, implementação de taxonomia para categorização de dados pessoais e procedimento para controlo e tratamento diferenciado dos dados de categoria especial (é considerado tratamento de dados de categoria especial o que revele a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos, dados de saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa); ----------

k) Implementação de procedimento para a identificação e gestão de violações de segurança em matéria de dados pessoais; ----------

l) Comunicação de violações de segurança em matéria de dados pessoais ao responsável pelo tratamento; ----------

m) Adoção de revisões periódicas/auditorias a processos e sistemas que envolvam o tratamento de dados pessoais; ----------

n) Capacidade de o responsável pelo tratamento aceder aos resultados das revisões/auditorias e propor outras sobre os processos e sistemas utilizados; --------

o) Adoção de procedimentos de controlo do acesso a instalações físicas onde estão armazenados, física ou digitalmente, os dados pessoais; ----------

p) Adoção de medidas de proteção de dados pessoais em suporte físico (por exemplo, documentação), especialmente quando estes são armazenados, transferidos ou destruídos; ----------

q) Aplicação de medidas de identificação e autenticação dos utilizadores com acesso a dados pessoais; ----------

r) Definição de perfis de utilizador que limitam o acesso e utilização de dados pessoais;

s) Implementação de medidas de limitação e minimização do acesso a dados pessoais nos sistemas de informação do subcontratante, como a pseudonimização, encriptação, anonimização ou eliminação de dados; ----------

t) Encriptação de dados pessoais contidos em suporte físicos, bem como na transmissão de dados com o responsável pelo tratamento; ----------

u) Registo e controlo de acessos a repositórios/sistemas de informação com dados pessoais (*logs*); ----------

v) Capacidade de recuperação de dados pessoais em caso de destruição, perda ou alteração; ----------

2. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. ----------

3. O responsável pelo tratamento e o subcontratante tomam medidas para assegurar que qualquer pessoa singular que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, só procede ao seu tratamento mediante instruções do responsável pelo tratamento, exceto se tal lhe for exigido pelo direito da União ou de um Estado-Membro. ----------

CLÁUSULA DÉCIMA PRIMEIRA

(Assistência para dar resposta aos pedidos dos titulares dos dados)

O subcontratante prestará 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. ----------

CLÁUSULA DÉCIMA SEGUNDA

(Assistência para cumprimento de obrigações)

O subcontratante prestará assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações de segurança no tratamento, notificação à autoridade de controlo e aos titulares em caso de violação de dados pessoais, avaliação de impacto sobre a proteção de dados e consulta prévia, tal como previstas nos artigos 32.º a 36.º do RGPD, tendo em conta a natureza de tratamento e a informação ao dispor do subcontratante. ----------

CLÁUSULA DÉCIMA TERCEIRA

(Consequências do término do contrato)

1. Com o término do contrato principal, qualquer que seja a causa, o subcontratante deverá, imediatamente: ----------

a) Proceder à devolução ao responsável pelo tratamento de toda a informação, pessoal ou não, que tenha sido objeto de tratamento como resultado da prestação de serviços, independentemente do suporte em que tenha sido facultada; ----------

b) Proceder à destruição física de qualquer tipo/suporte/ficheiro/meio que contenha informação, pessoal ou não e que, por qualquer motivo, não tenha sido devolvido ao responsável pelo tratamento, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros. ----------

CLÁUSULA DÉCIMA QUARTA

(Obrigações)

1. O subcontratante obriga-se ainda a: ----------

a) Disponibilizar ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no contrato; ----------

b) Facilitar e a contribuir para as auditorias, inclusive as inspeções, conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado; ----------

c) Informar imediatamente o responsável pelo tratamento se, no seu entender, alguma instrução violar o RGPD ou outras disposições do direito da União ou dos Estados-Membros em matéria de proteção de dados. ----------

CLÁUSULA DÉCIMA QUINTA

(Código de conduta ou procedimento de certificação)

O cumprimento de um código de conduta ou de um procedimento de certificação poderá ser utilizado como elemento para demonstrar o cumprimento de todas estas obrigações por parte do subcontratante. ----------

CLÁUSULA DÉCIMA SEXTA

(Incumprimento)

O incumprimento dos deveres aqui enunciados e a verificação de inexistência de garantias de *compliance* é fundamento de resolução do contrato principal com justa causa, podendo implicar o dever de indemnizar o responsável pelo tratamento por eventuais violações que sejam imputadas ao subcontratante. ----------

CLÁUSULA DÉCIMA SÉTIMA

(Responsabilidade)

O subcontratante deve suportar todos os custos (incluindo honorários de advogados) e indemnizar o responsável pelo tratamento por danos e perdas (incluindo penalidades administrativas) decorrentes de reclamações judiciais ou extrajudiciais de terceiros ou de procedimentos de sanção abertos pela Comissão Nacional de Proteção de Dados ou outra entidade reguladora, que sejam consequência da violação por parte do subcontratante de qualquer das obrigações estabelecidas neste contrato ou na atual legislação relevante em matéria de Proteção de Dados. ----------

CLÁUSULA DÉCIMA OITAVA

(Alteração)

Ambas as partes declaram que podem surgir questões não contempladas nos termos deste contrato e que determinadas questões poderão renegociar-se, tendo assim de se proceder a alterações ou a aditamentos, devendo estas ocorrer sob a forma ora subscrita por ambas as partes, com expressa menção das cláusulas alteradas, aditadas ou suprimidas. -----

CLÁUSULA DÉCIMA NONA

(Foro convencional)

Fica estabelecido o foro do Tribunal Judicial da Comarca dos Açores, com renúncia expressa a qualquer outro, para resolução de todo e qualquer litígio emergente da validade, interpretação e aplicação do presente contrato. ----------

CLÁUSULA VIGÉSIMA

(Legislação subsidiária)

Em tudo o que o presente contrato for omisso, regerá a legislação aplicável. ---------

O presente contrato lavrado no dia 25 de Maio de 2018, em dois exemplares, ambos valendo como originais, destinando-se um a cada um dos Outorgantes, os quais prescindem reciprocamente e de forma irrevogável do reconhecimento notarial das assinaturas e as demais formalidades exigidas por Lei, não tendo a sua falta sido causada culposamente, e por isso, renunciam, em consequência, ao direito de invocar qualquer invalidade que de tal falta possa resultar, reconhecendo plena validade ao presente contrato, comprometendo-se ainda, a qualquer momento reconhecerem as suas assinaturas desde que para tal solicitado por escrito por qualquer dos Outorgantes. ----------

Assim acordam de boa fé do que vão assinar, pois as vontades manifestadas

correspondem às reais vontades declaradas, e por o acharem conforme, assinam o presente contrato. ----------

Ponta Delgada, 25 de Maio de 2018

Pelo Responsável pelo Tratamento,

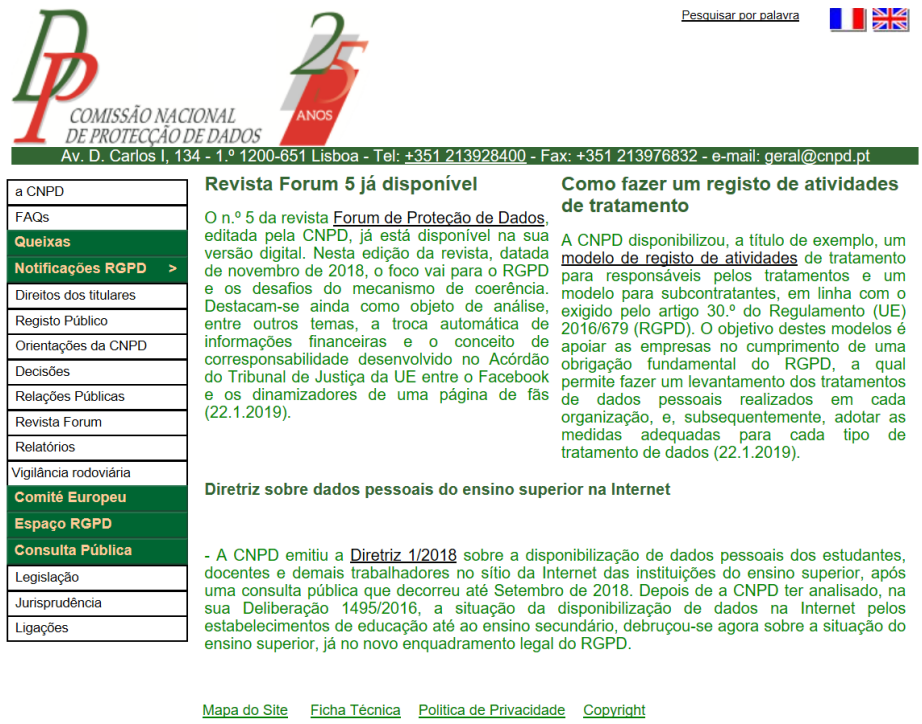
_____

Pelo subcontratante,

_____

ANEXO 5: MODELO DE REGISTO PARA O RESPONSÁVEL PELO TRATAMENTO

Página inicial da Comissão Nacional de Proteção de Dados, disponível em http://www-cnpd.pt/



Pesquisar por palavra

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

25 ANOS

Av. D. Carlos I, 134 - 1.º 1200-651 Lisboa - Tel: +351 213928400 - Fax: +351 213976832 - e-mail: geral@cnpd.pt

- a CNPD
- FAQs
- Queixas
- Notificações RGPD >
- Direitos dos titulares
- Registo Público
- Orientações da CNPD
- Decisões
- Relações Públicas
- Revista Forum
- Relatórios
- Vigilância rodoviária
- Comité Europeu
- Espaço RGPD
- Consulta Pública
- Legislação
- Jurisprudência
- Ligações

Revista Forum 5 já disponível

O n.º 5 da revista Forum de Proteção de Dados, editada pela CNPD, já está disponível na sua versão digital. Nesta edição da revista, datada de novembro de 2018, o foco vai para o RGPD e os desafios do mecanismo de coerência. Destacam-se ainda como objeto de análise, entre outros temas, a troca automática de informações financeiras e o conceito de corresponsabilidade desenvolvido no Acórdão do Tribunal de Justiça da UE entre o Facebook e os dinamizadores de uma página de fãs (22.1.2019).

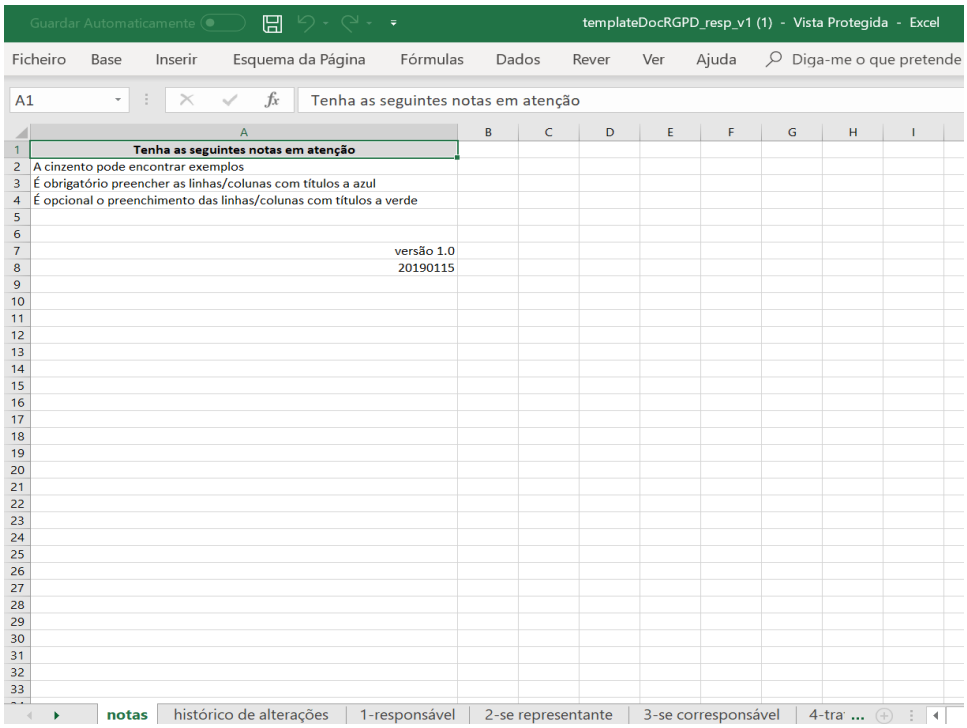
Como fazer um registo de atividades de tratamento

A CNPD disponibilizou, a título de exemplo, um modelo de registo de atividades de tratamento para responsáveis pelos tratamentos e um modelo para subcontratantes, em linha com o exigido pelo artigo 30.º do Regulamento (UE) 2016/679 (RGPD). O objetivo destes modelos é apoiar as empresas no cumprimento de uma obrigação fundamental do RGPD, a qual permite fazer um levantamento dos tratamentos de dados pessoais realizados em cada organização, e, subsequentemente, adotar as medidas adequadas para cada tipo de tratamento de dados (22.1.2019).

Diretriz sobre dados pessoais do ensino superior na Internet

- A CNPD emitiu a Diretriz 1/2018 sobre a disponibilização de dados pessoais dos estudantes, docentes e demais trabalhadores no sítio da Internet das instituições do ensino superior, após uma consulta pública que decorreu até Setembro de 2018. Depois de a CNPD ter analisado, na sua Deliberação 1495/2016, a situação da disponibilização de dados na Internet pelos estabelecimentos de educação até ao ensino secundário, debruçou-se agora sobre a situação do ensino superior, já no novo enquadramento legal do RGPD.

Mapa do Site | Ficha Técnica | Política de Privacidade | Copyright



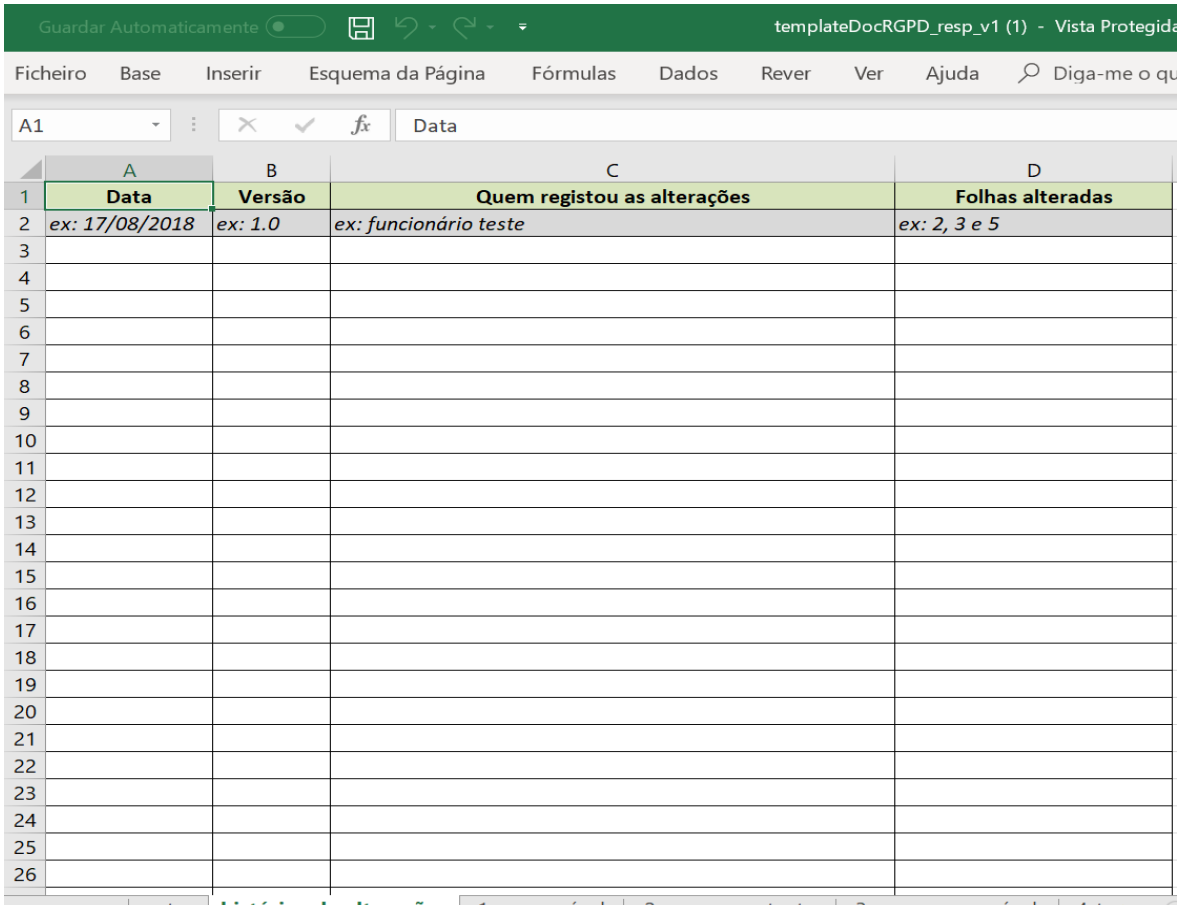
Guardar Automaticamente templateDocRGPD_resp_v1 (1) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende

A1 Tenha as seguintes notas em atenção

	A	B	C	D	E	F	G	H	I
1	**Tenha as seguintes notas em atenção**								
2	A cinzento pode encontrar exemplos								
3	É obrigatório preencher as linhas/colunas com títulos a azul								
4	É opcional o preenchimento das linhas/colunas com títulos a verde								
5									
6									
7	versão 1.0								
8	20190115								

notas | histórico de alterações | 1-responsável | 2-se representante | 3-se corresponsável | 4-tra ...



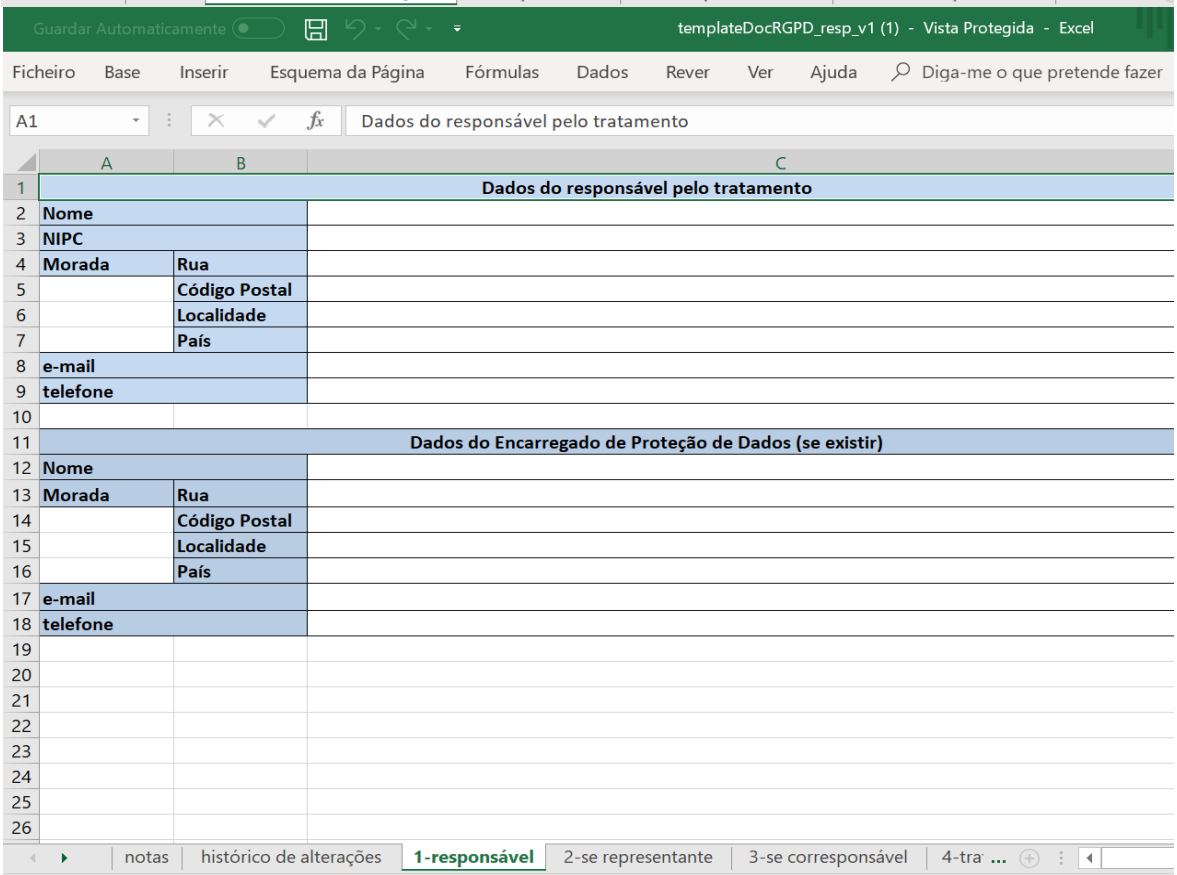
templateDocRGPD_resp_v1 (1) - Vista Protegida

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o qu

A1 Data

	A	B	C	D
1	**Data**	**Versão**	**Quem registou as alterações**	**Folhas alteradas**
2	*ex: 17/08/2018*	*ex: 1.0*	*ex: funcionário teste*	*ex: 2, 3 e 5*

notas | **histórico de alterações** | 1-responsável | 2-se representante | 3-se corresponsável | 4-tra ...



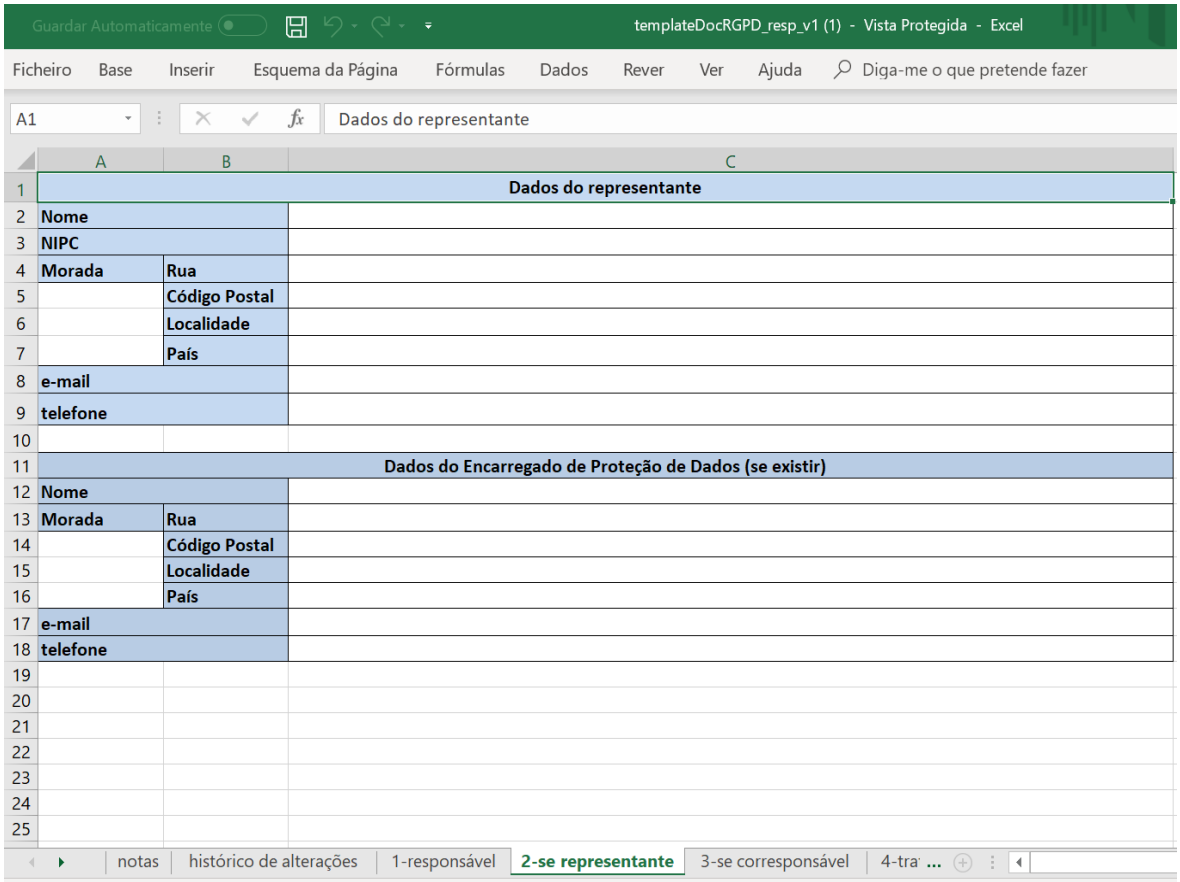
templateDocRGPD_resp_v1 (1) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

A1 Dados do responsável pelo tratamento

	A	B	C
1	**Dados do responsável pelo tratamento**		
2	**Nome**		
3	**NIPC**		
4	**Morada**	**Rua**	
5		**Código Postal**	
6		**Localidade**	
7		**País**	
8	**e-mail**		
9	**telefone**		
10			
11	**Dados do Encarregado de Proteção de Dados (se existir)**		
12	**Nome**		
13	**Morada**	**Rua**	
14		**Código Postal**	
15		**Localidade**	
16		**País**	
17	**e-mail**		
18	**telefone**		

notas | histórico de alterações | **1-responsável** | 2-se representante | 3-se corresponsável | 4-tra ...



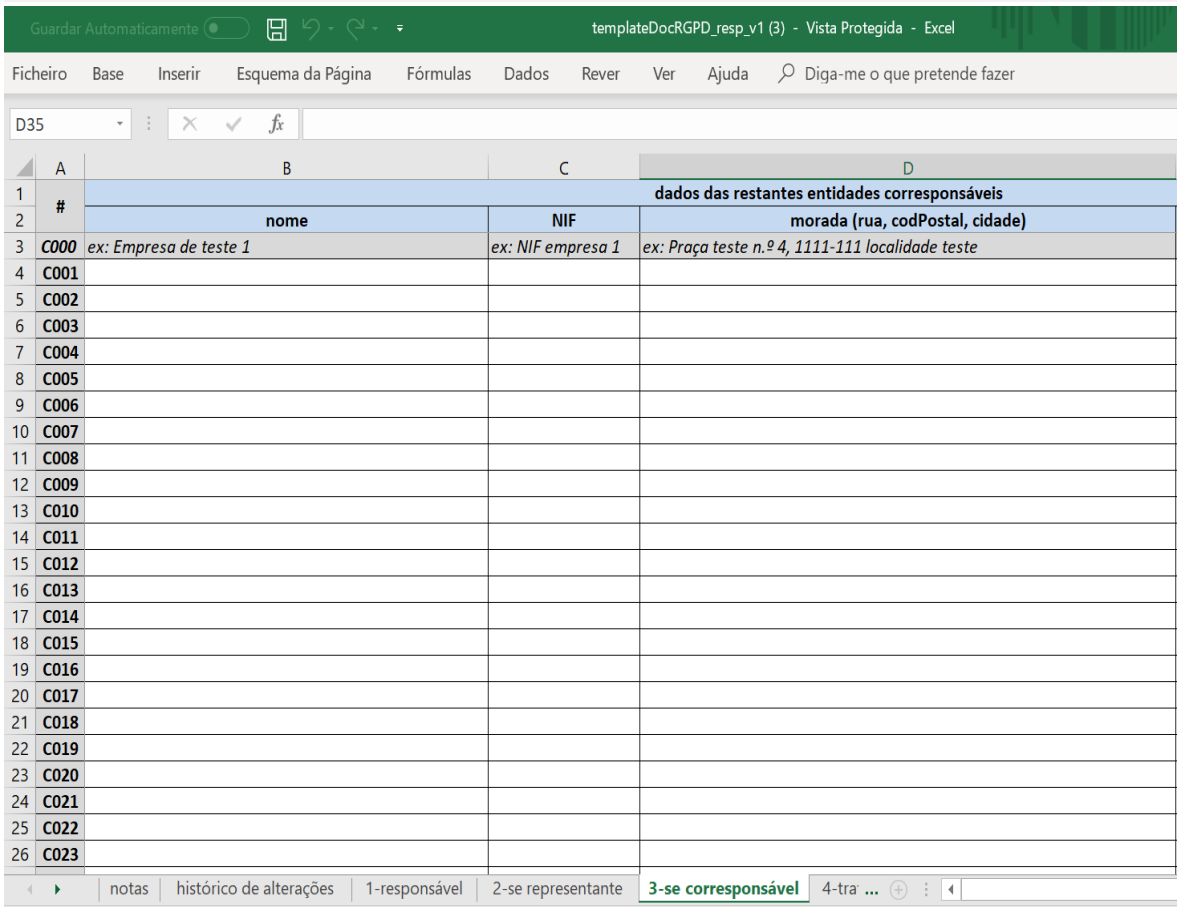
templateDocRGPD_resp_v1 (1) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

A1 Dados do representante

	A	B	C
1	**Dados do representante**		
2	**Nome**		
3	**NIPC**		
4	**Morada**	**Rua**	
5		**Código Postal**	
6		**Localidade**	
7		**País**	
8	**e-mail**		
9	**telefone**		
10			
11	**Dados do Encarregado de Proteção de Dados (se existir)**		
12	**Nome**		
13	**Morada**	**Rua**	
14		**Código Postal**	
15		**Localidade**	
16		**País**	
17	**e-mail**		
18	**telefone**		
19			
20			
21			
22			
23			
24			
25			

notas | histórico de alterações | 1-responsável | **2-se representante** | 3-se corresponsável | 4-tra ...



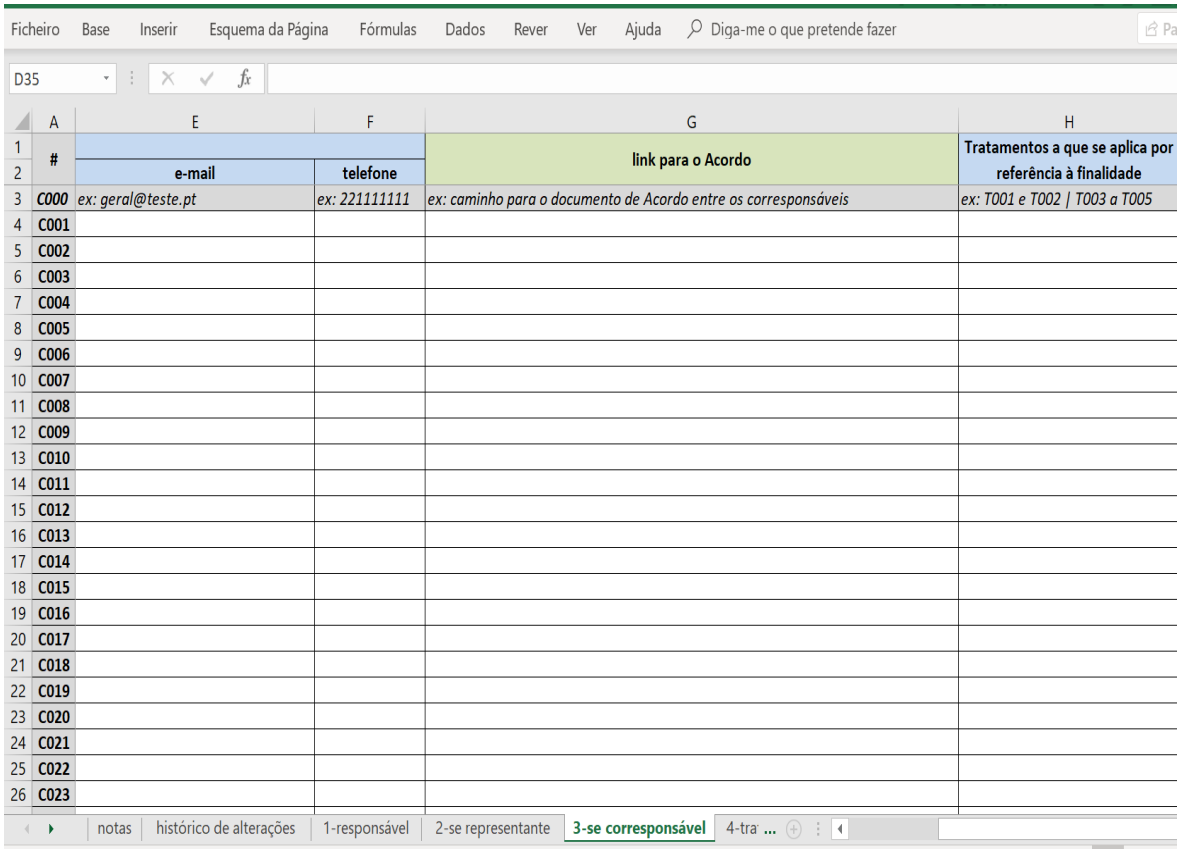
templateDocRGPD_resp_v1 (3) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

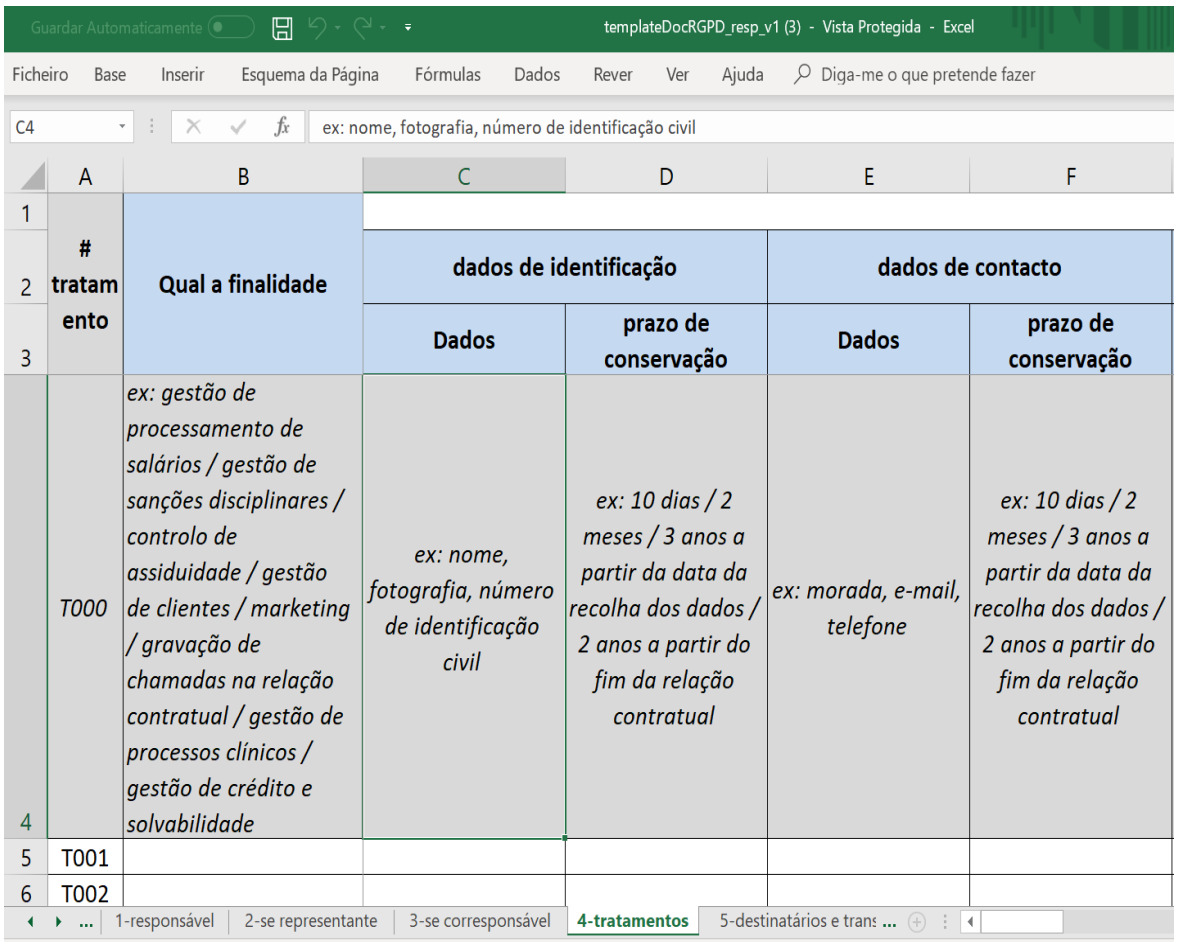
D35

	A	B	C	D
1	#			**dados das restantes entidades corresponsáveis**
2		**nome**	**NIF**	**morada (rua, codPostal, cidade)**
3	***C000***	*ex: Empresa de teste 1*	*ex: NIF empresa 1*	*ex: Praça teste n.º 4, 1111-111 localidade teste*
4	**C001**			
5	**C002**			
6	**C003**			
7	**C004**			
8	**C005**			
9	**C006**			
10	**C007**			
11	**C008**			
12	**C009**			
13	**C010**			
14	**C011**			
15	**C012**			
16	**C013**			
17	**C014**			
18	**C015**			
19	**C016**			
20	**C017**			
21	**C018**			
22	**C019**			
23	**C020**			
24	**C021**			
25	**C022**			
26	**C023**			

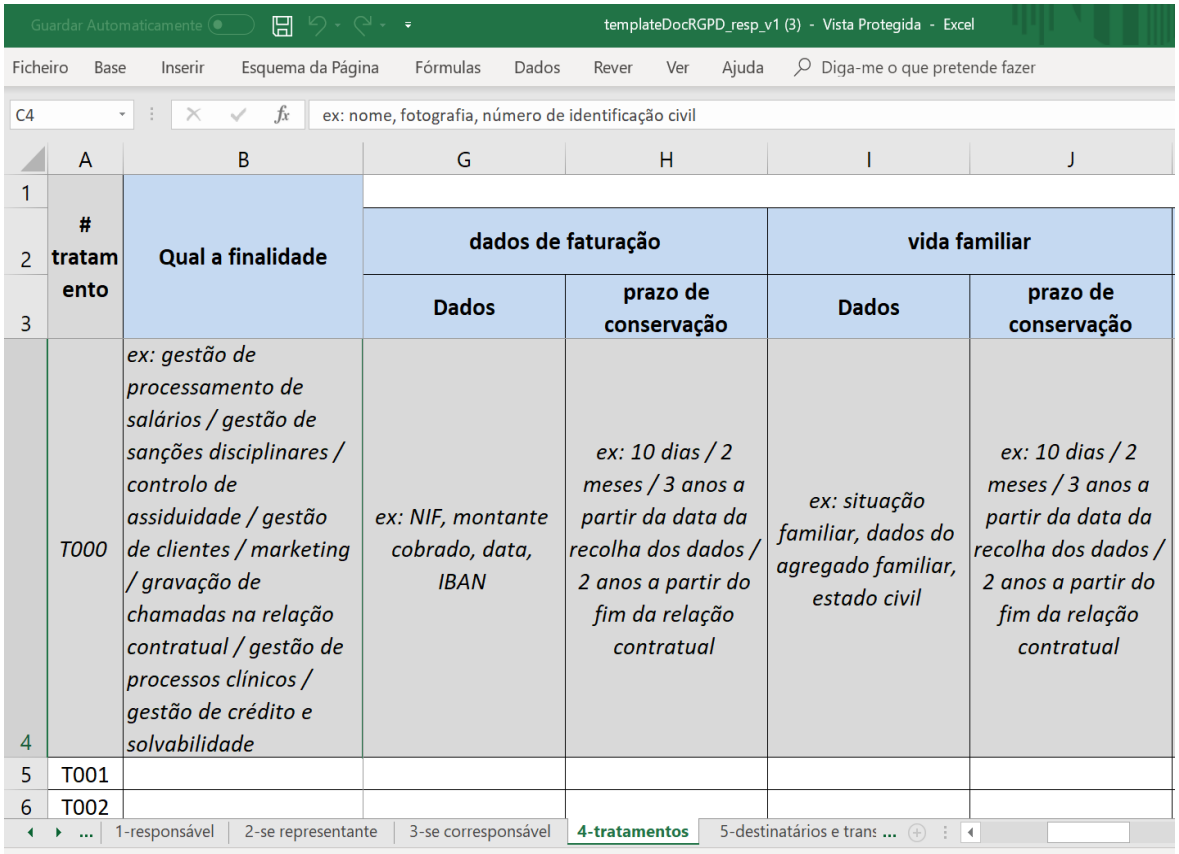
notas | histórico de alterações | 1-responsável | 2-se representante | **3-se corresponsável** | 4-tra ...



#	e-mail	telefone	link para o Acordo	Tratamentos a que se aplica por referência à finalidade
C000	*ex: geral@teste.pt*	*ex: 221111111*	*ex: caminho para o documento de Acordo entre os corresponsáveis*	*ex: T001 e T002 | T003 a T005*
C001				
C002				
C003				
C004				
C005				
C006				
C007				
C008				
C009				
C010				
C011				
C012				
C013				
C014				
C015				
C016				
C017				
C018				
C019				
C020				
C021				
C022				
C023				



# tratamento	Qual a finalidade	dados de identificação		dados de contacto	
		Dados	prazo de conservação	Dados	prazo de conservação
T000	*ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade*	*ex: nome, fotografia, número de identificação civil*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: morada, e-mail, telefone*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*
T001					
T002					

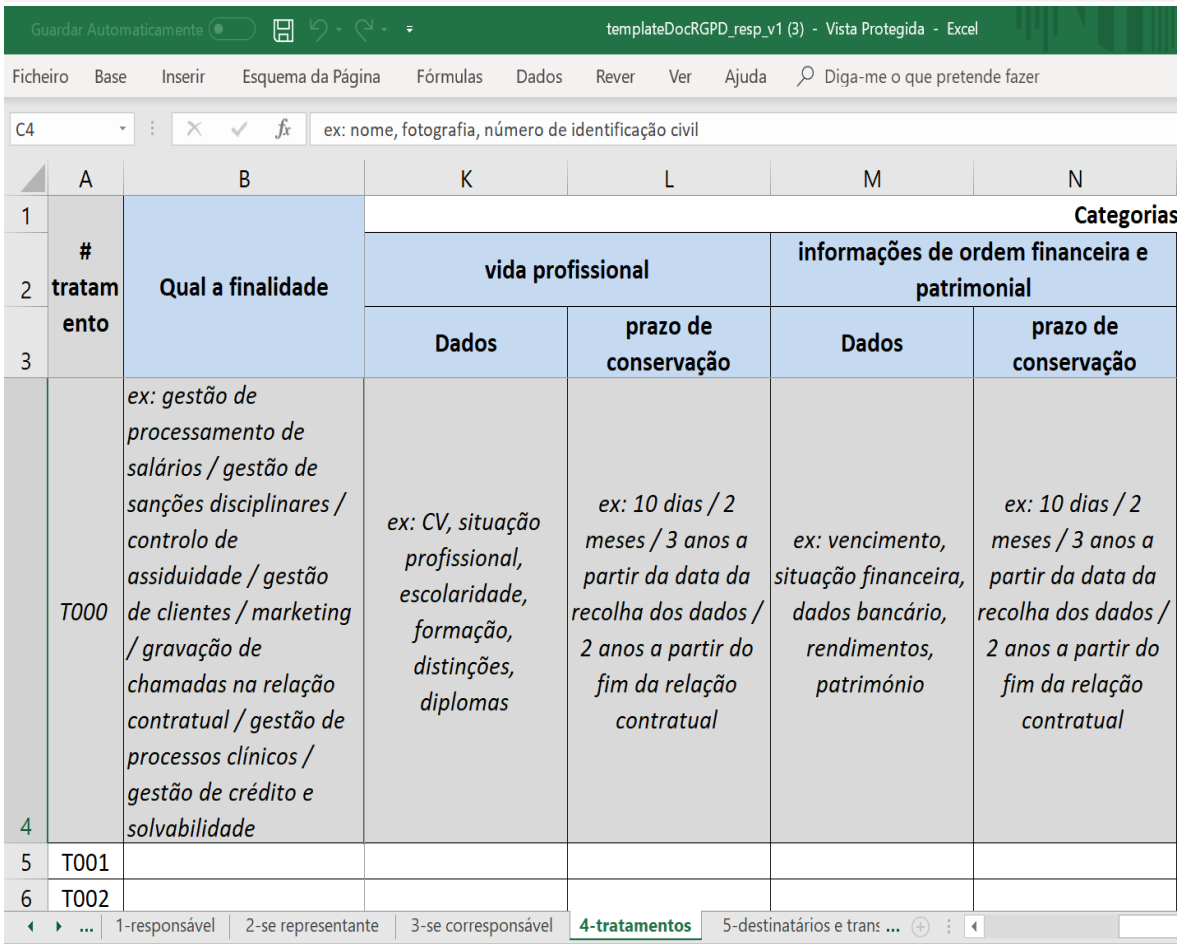

templateDocRGPD_resp_v1 (3) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

C4 ex: nome, fotografia, número de identificação civil

	A	B	G	H	I	J
1						
2	**# tratamento**	**Qual a finalidade**	**dados de faturação**		**vida familiar**	
3			**Dados**	**prazo de conservação**	**Dados**	**prazo de conservação**
4	*T000*	*ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade*	*ex: NIF, montante cobrado, data, IBAN*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: situação familiar, dados do agregado familiar, estado civil*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*
5	T001					
6	T002					

... 1-responsável 2-se representante 3-se corresponsável **4-tratamentos** 5-destinatários e trans ...

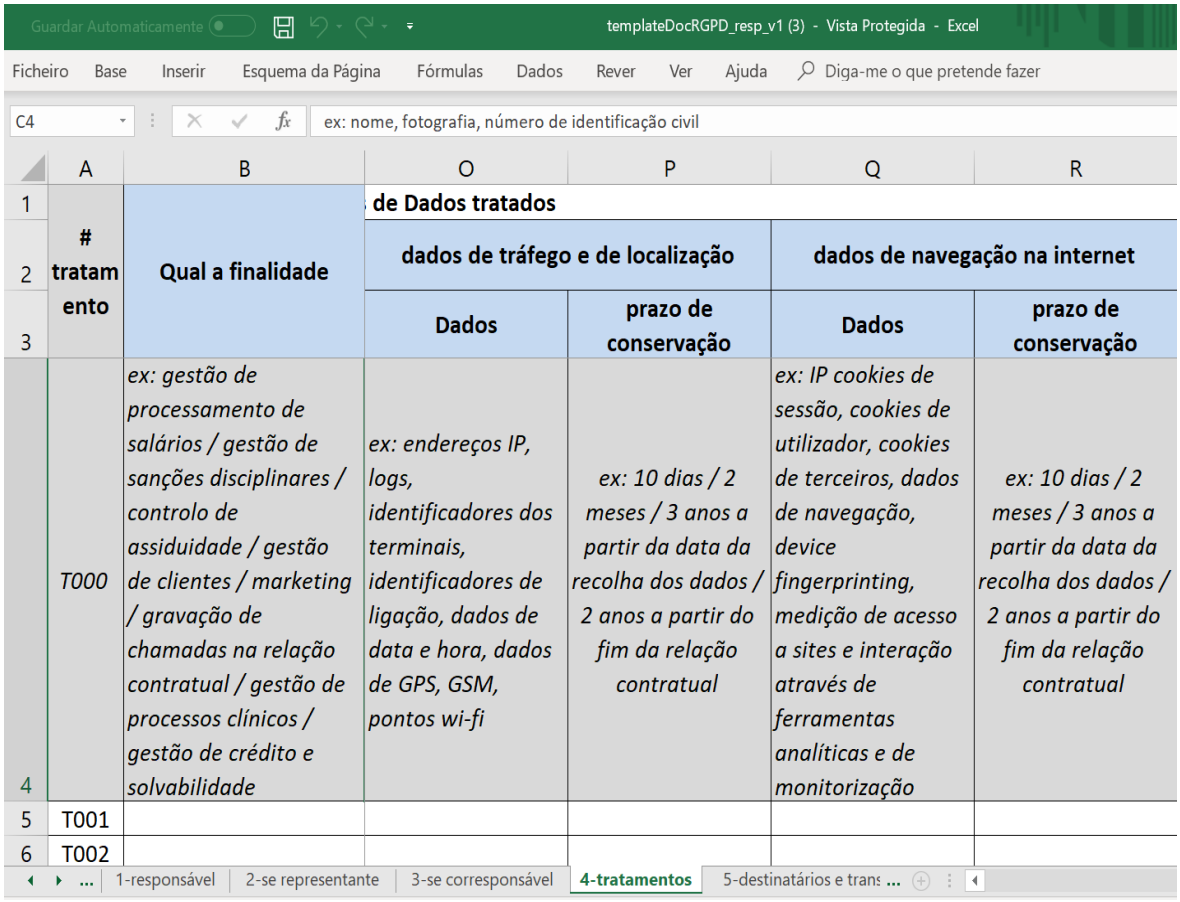

templateDocRGPD_resp_v1 (3) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

C4 ex: nome, fotografia, número de identificação civil

	A	B	K	L	M	N
1						**Categorias**
2	**# tratamento**	**Qual a finalidade**	**vida profissional**		**informações de ordem financeira e patrimonial**	
3			**Dados**	**prazo de conservação**	**Dados**	**prazo de conservação**
4	*T000*	*ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade*	*ex: CV, situação profissional, escolaridade, formação, distinções, diplomas*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: vencimento, situação financeira, dados bancário, rendimentos, património*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*
5	T001					
6	T002					

... 1-responsável 2-se representante 3-se corresponsável **4-tratamentos** 5-destinatários e trans ...

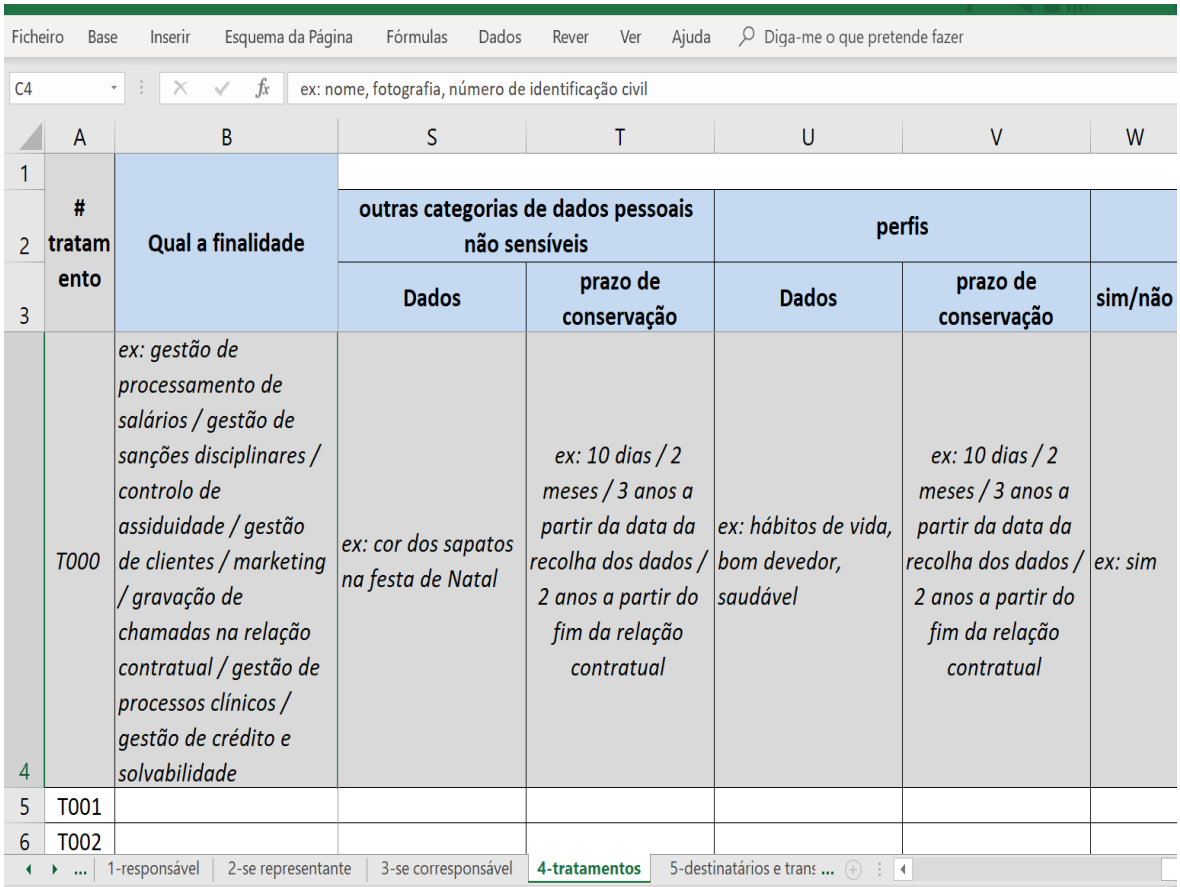

templateDocRGPD_resp_v1 (3) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

C4 ex: nome, fotografia, número de identificação civil

	A	B	O	P	Q	R
1			de Dados tratados			
2	# tratamento	Qual a finalidade	dados de tráfego e de localização		dados de navegação na internet	
3			Dados	prazo de conservação	Dados	prazo de conservação
4	T000	*ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade*	*ex: endereços IP, logs, identificadores dos terminais, identificadores de ligação, dados de data e hora, dados de GPS, GSM, pontos wi-fi*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: IP cookies de sessão, cookies de utilizador, cookies de terceiros, dados de navegação, device fingerprinting, medição de acesso a sites e interação através de ferramentas analíticas e de monitorização*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*
5	T001					
6	T002					

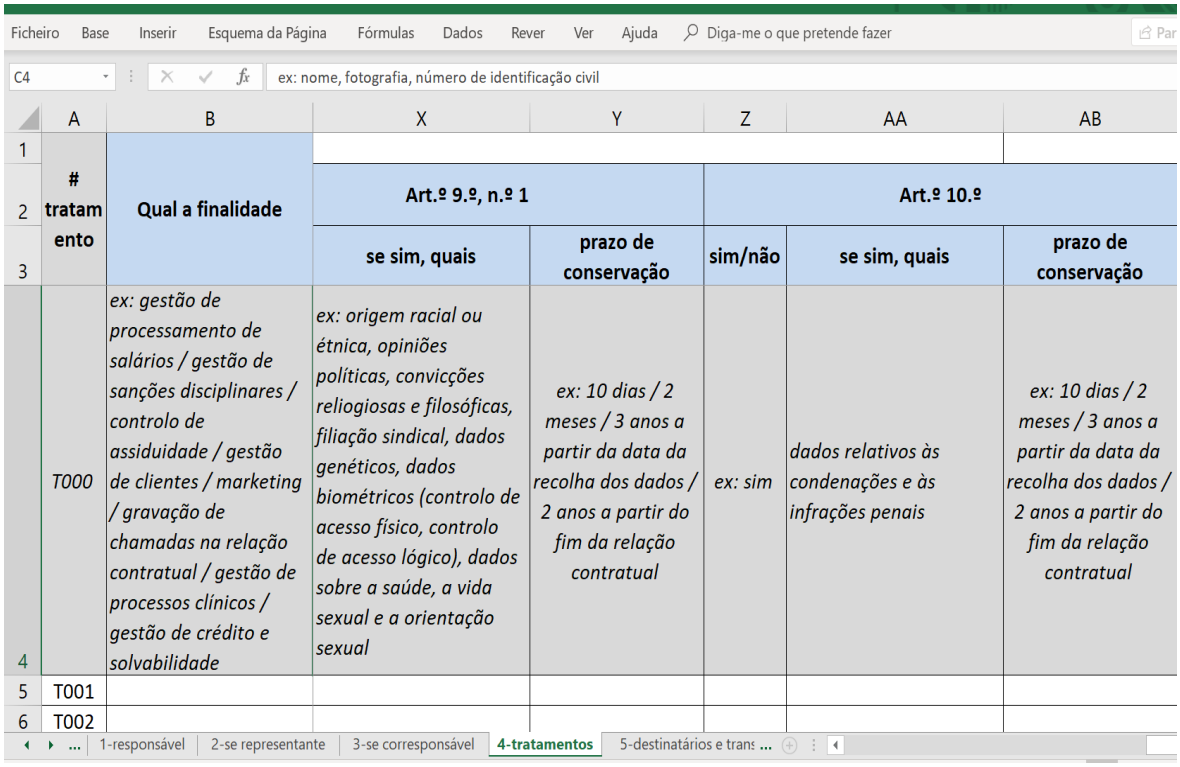
... 1-responsável 2-se representante 3-se corresponsável **4-tratamentos** 5-destinatários e trans ...


Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

C4 ex: nome, fotografia, número de identificação civil

	A	B	S	T	U	V	W
1							
2	# tratamento	Qual a finalidade	outras categorias de dados pessoais não sensíveis		perfis		
3			Dados	prazo de conservação	Dados	prazo de conservação	sim/não
4	T000	*ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade*	*ex: cor dos sapatos na festa de Natal*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: hábitos de vida, bom devedor, saudável*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: sim*
5	T001						
6	T002						

... 1-responsável 2-se representante 3-se corresponsável **4-tratamentos** 5-destinatários e trans ...

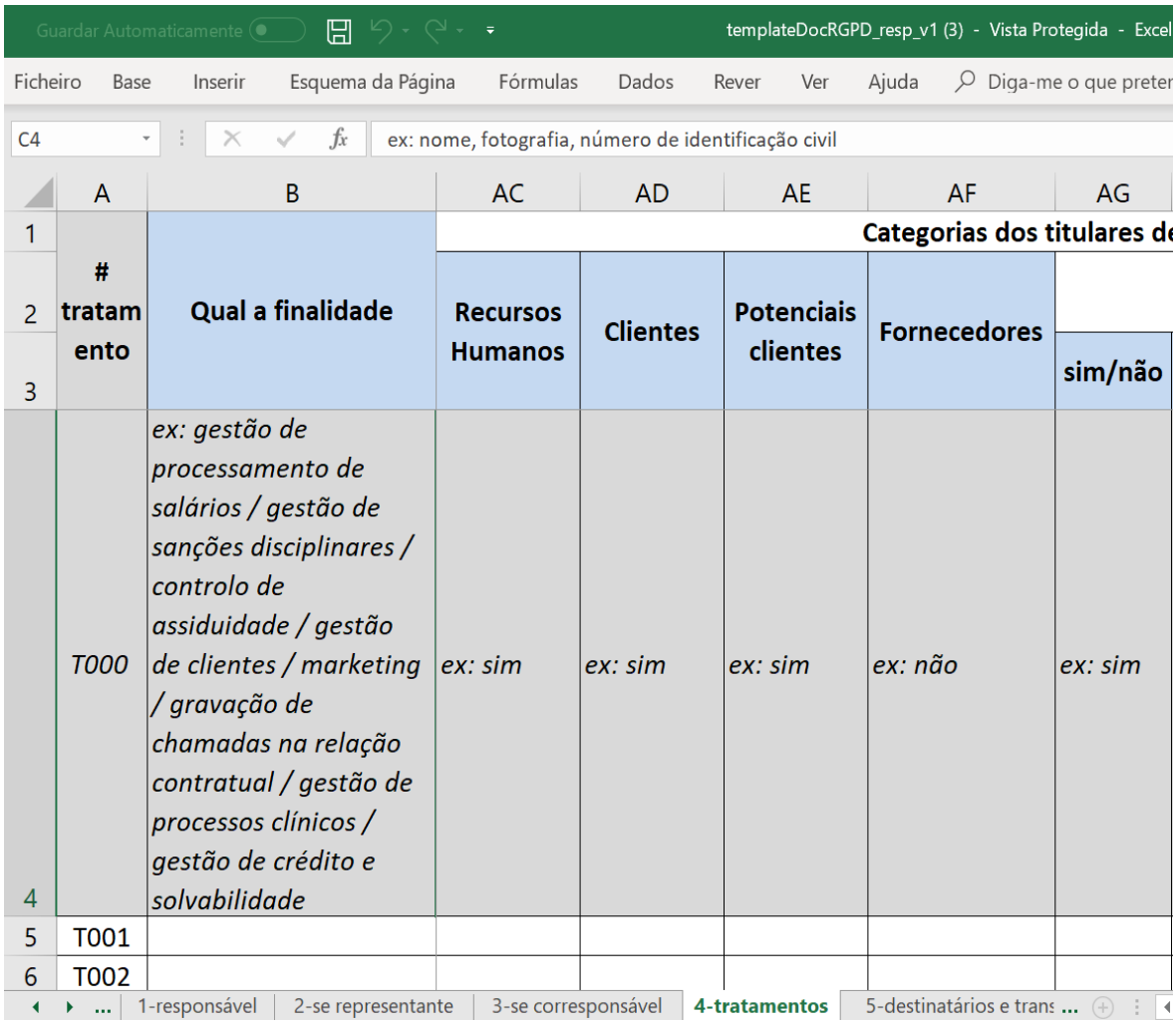


Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

C4 ex: nome, fotografia, número de identificação civil

	A	B	X	Y	Z	AA	AB
1							
2	# tratamento	Qual a finalidade	Art.º 9.º, n.º 1		Art.º 10.º		
3			se sim, quais	prazo de conservação	sim/não	se sim, quais	prazo de conservação
4	*T000*	*ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade*	*ex: origem racial ou étnica, opiniões políticas, convicções religiosas e filosóficas, filiação sindical, dados genéticos, dados biométricos (controlo de acesso físico, controlo de acesso lógico), dados sobre a saúde, a vida sexual e a orientação sexual*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: sim*	*dados relativos às condenações e às infrações penais*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*
5	T001						
6	T002						

... 1-responsável 2-se representante 3-se corresponsável 4-tratamentos 5-destinatários e trans ...



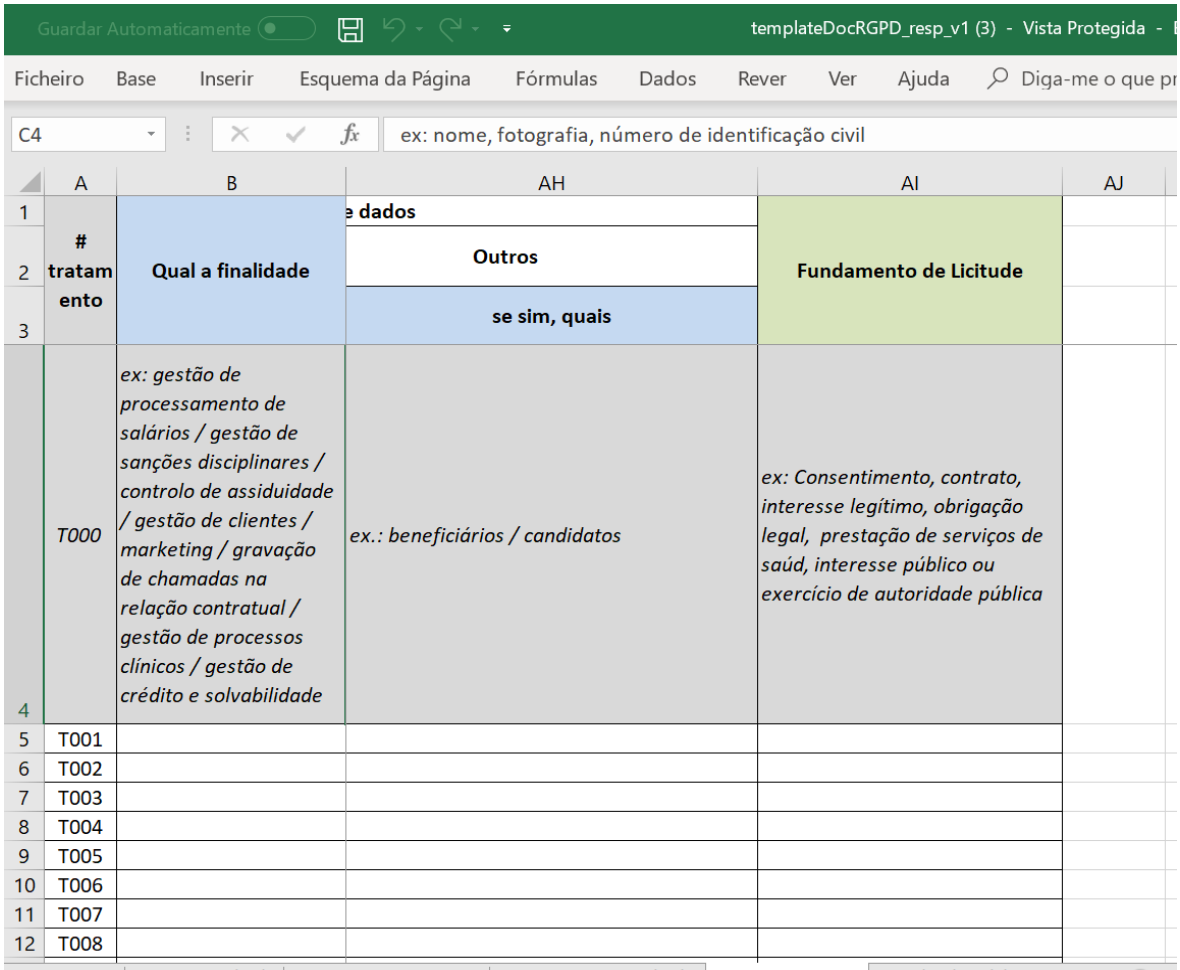
Guardar Automaticamente templateDocRGPD_resp_v1 (3) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que preter

C4 ex: nome, fotografia, número de identificação civil

	A	B	AC	AD	AE	AF	AG
1			Categorias dos titulares de				
2	# tratamento	Qual a finalidade	Recursos Humanos	Clientes	Potenciais clientes	Fornecedores	
3							sim/não
4	*T000*	*ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade*	*ex: sim*	*ex: sim*	*ex: sim*	*ex: não*	*ex: sim*
5	T001						
6	T002						

... 1-responsável 2-se representante 3-se corresponsável 4-tratamentos 5-destinatários e trans ...



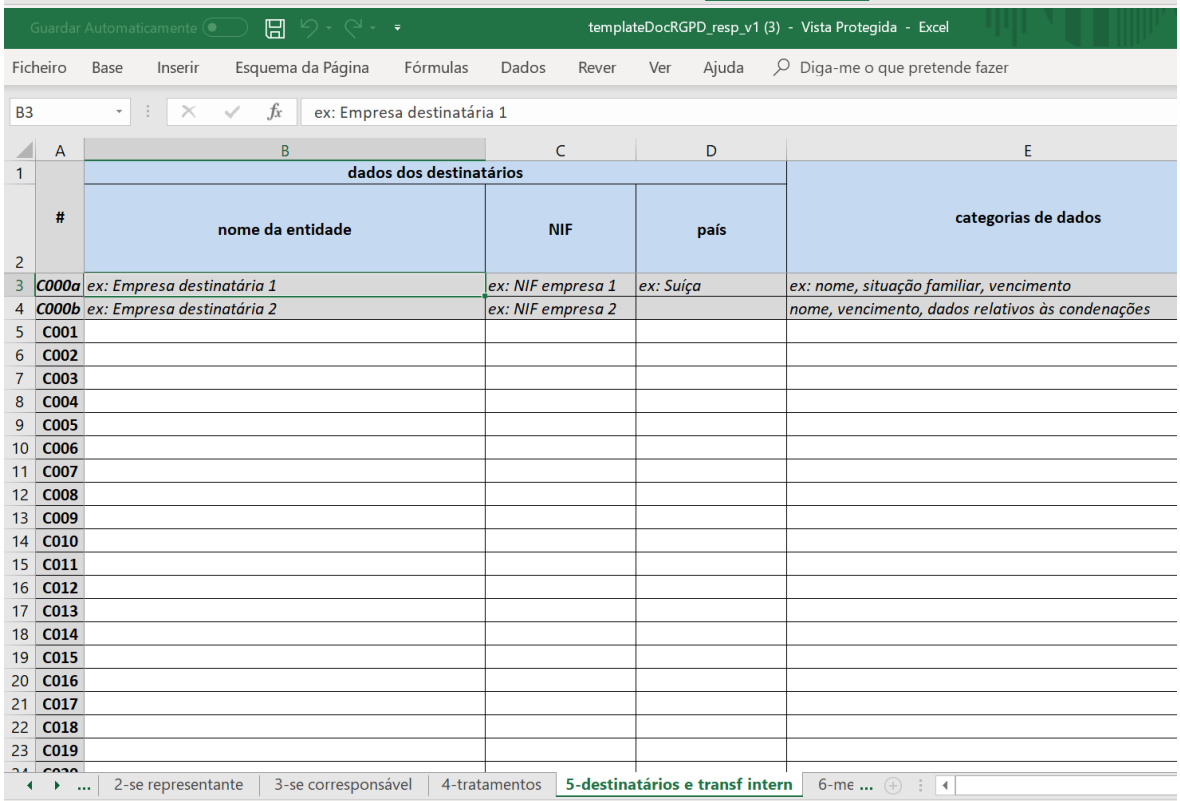
templateDocRGPD_resp_v1 (3) - Vista Protegida

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pr

C4 ex: nome, fotografia, número de identificação civil

	A	B	AH	AI	AJ
1			e dados		
2	# tratamento	Qual a finalidade	Outros	Fundamento de Licitude	
3			se sim, quais		
4	T000	*ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade*	*ex.: beneficiários / candidatos*	*ex: Consentimento, contrato, interesse legítimo, obrigação legal, prestação de serviços de saúd, interesse público ou exercício de autoridade pública*	
5	T001				
6	T002				
7	T003				
8	T004				
9	T005				
10	T006				
11	T007				
12	T008				

... 1-responsável 2-se representante 3-se corresponsável **4-tratamentos** 5-destinatários e trans ...



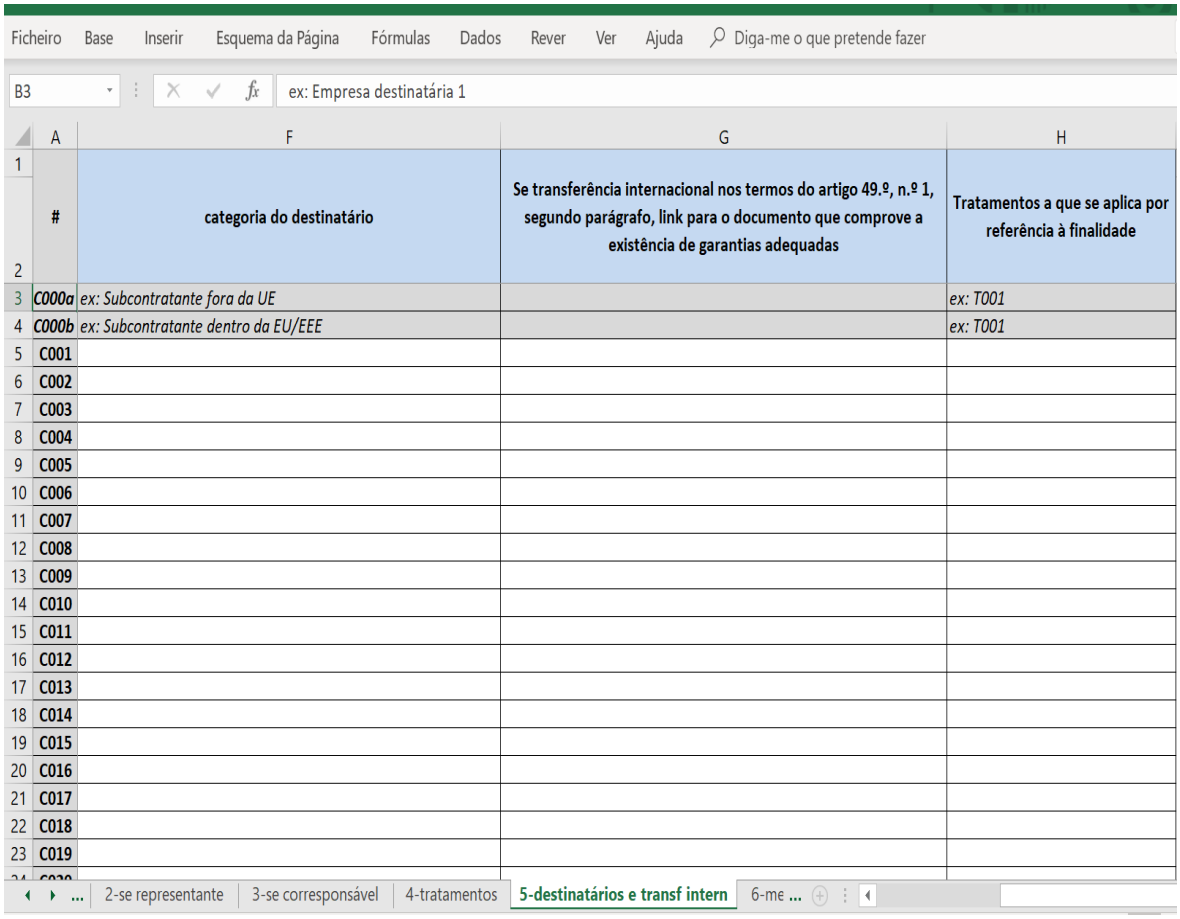
templateDocRGPD_resp_v1 (3) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

B3 ex: Empresa destinatária 1

	A	B	C	D	E
1		dados dos destinatários			
2	#	nome da entidade	NIF	país	categorias de dados
3	C000a	*ex: Empresa destinatária 1*	*ex: NIF empresa 1*	*ex: Suíça*	*ex: nome, situação familiar, vencimento*
4	C000b	*ex: Empresa destinatária 2*	*ex: NIF empresa 2*		*nome, vencimento, dados relativos às condenações*
5	C001				
6	C002				
7	C003				
8	C004				
9	C005				
10	C006				
11	C007				
12	C008				
13	C009				
14	C010				
15	C011				
16	C012				
17	C013				
18	C014				
19	C015				
20	C016				
21	C017				
22	C018				
23	C019				

... 2-se representante 3-se corresponsável 4-tratamentos **5-destinatários e transf intern** 6-me ...

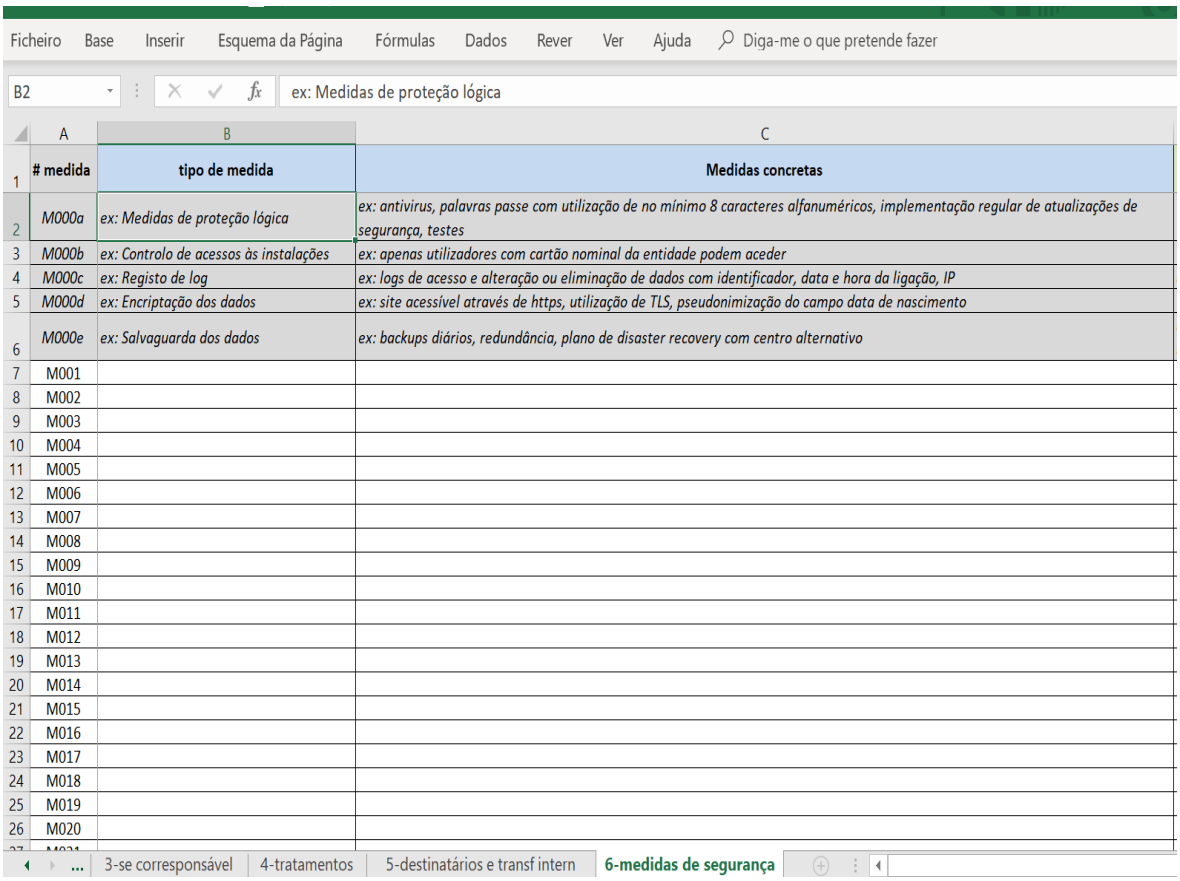


Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

B3 ex: Empresa destinatária 1

	A	F	G	H
1	#	categoria do destinatário	Se transferência internacional nos termos do artigo 49.º, n.º 1, segundo parágrafo, link para o documento que comprove a existência de garantias adequadas	Tratamentos a que se aplica por referência à finalidade
2				
3	*C000a*	*ex: Subcontratante fora da UE*		*ex: T001*
4	*C000b*	*ex: Subcontratante dentro da EU/EEE*		*ex: T001*
5	C001			
6	C002			
7	C003			
8	C004			
9	C005			
10	C006			
11	C007			
12	C008			
13	C009			
14	C010			
15	C011			
16	C012			
17	C013			
18	C014			
19	C015			
20	C016			
21	C017			
22	C018			
23	C019			

... 2-se representante 3-se corresponsável 4-tratamentos 5-destinatários e transf intern 6-me ...

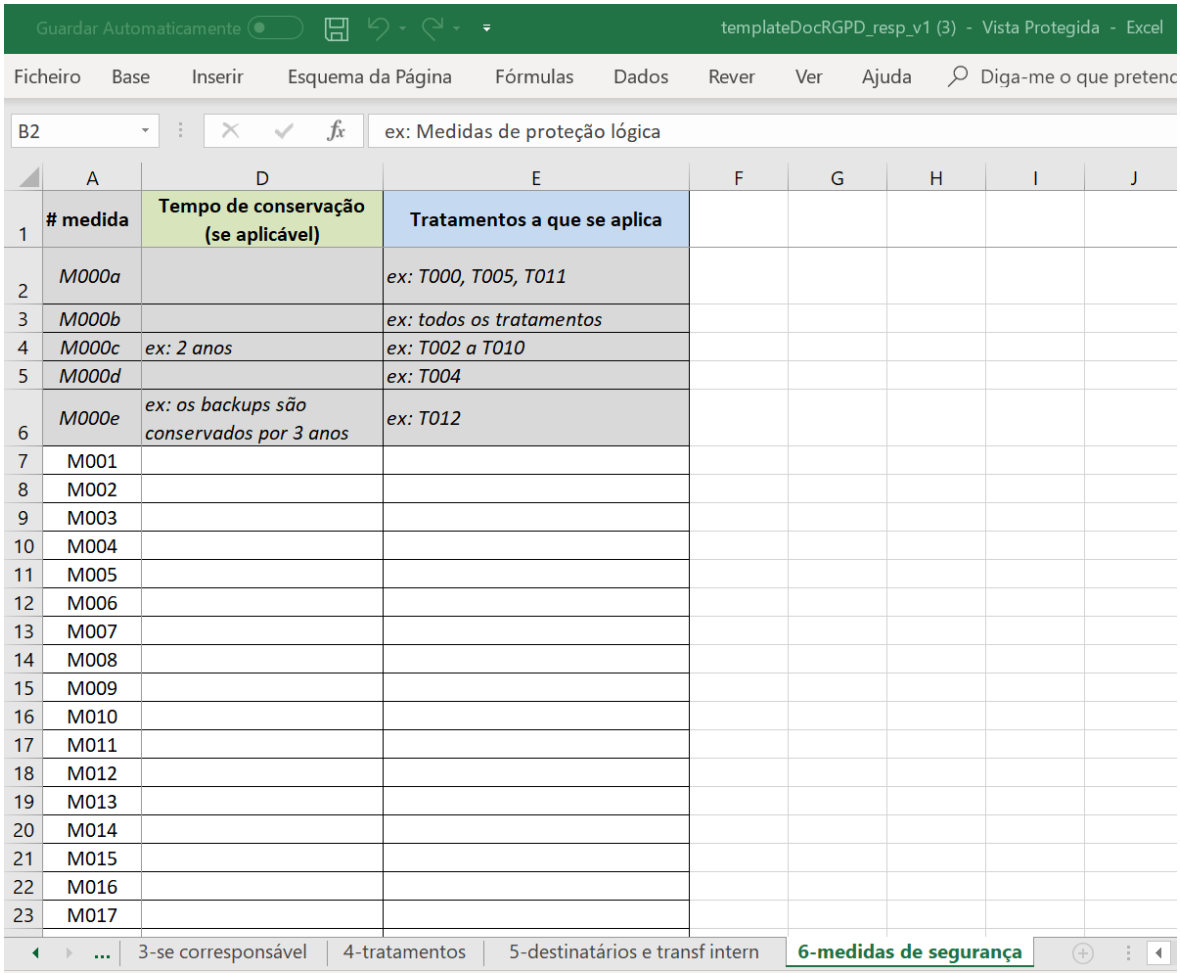


Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

B2 ex: Medidas de proteção lógica

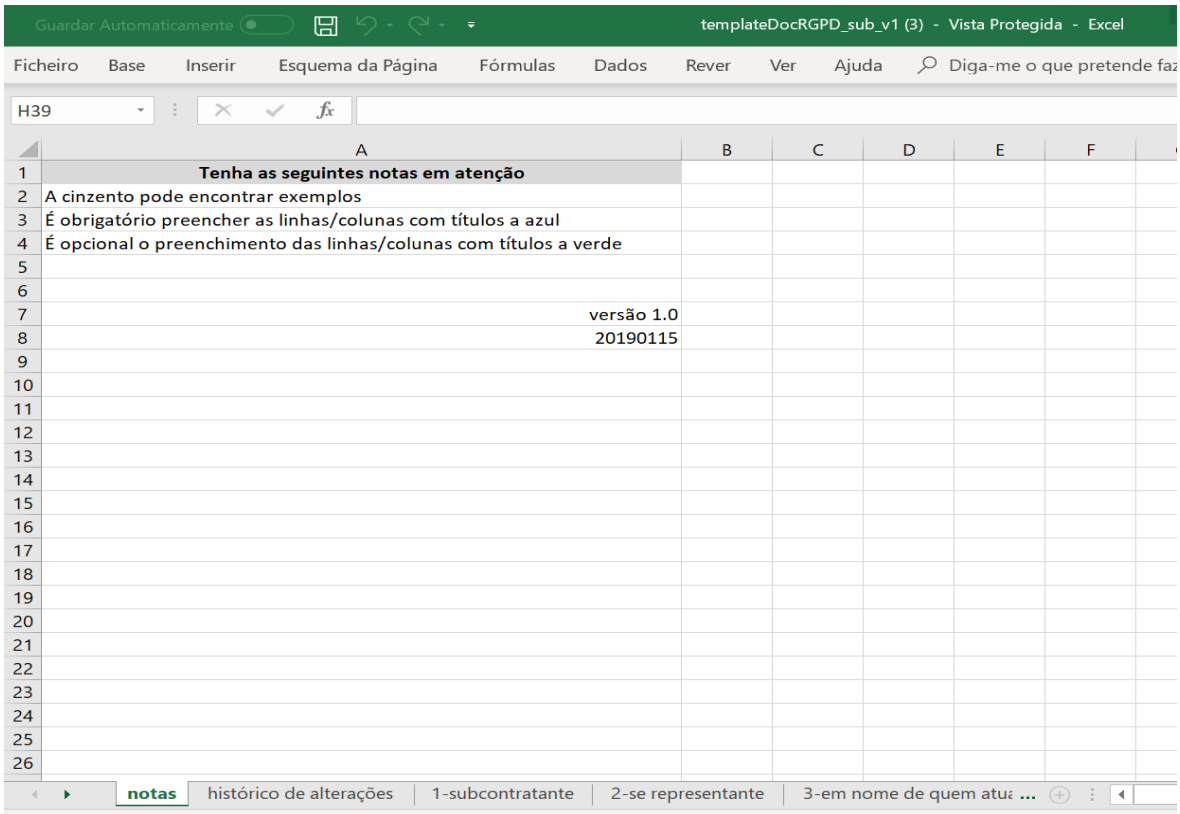
	A	B	C
1	# medida	tipo de medida	Medidas concretas
2	*M000a*	*ex: Medidas de proteção lógica*	*ex: antivirus, palavras passe com utilização de no mínimo 8 caracteres alfanuméricos, implementação regular de atualizações de segurança, testes*
3	*M000b*	*ex: Controlo de acessos às instalações*	*ex: apenas utilizadores com cartão nominal da entidade podem aceder*
4	*M000c*	*ex: Registo de log*	*ex: logs de acesso e alteração ou eliminação de dados com identificador, data e hora da ligação, IP*
5	*M000d*	*ex: Encriptação dos dados*	*ex: site acessível através de https, utilização de TLS, pseudonimização do campo data de nascimento*
6	*M000e*	*ex: Salvaguarda dos dados*	*ex: backups diários, redundância, plano de disaster recovery com centro alternativo*
7	M001		
8	M002		
9	M003		
10	M004		
11	M005		
12	M006		
13	M007		
14	M008		
15	M009		
16	M010		
17	M011		
18	M012		
19	M013		
20	M014		
21	M015		
22	M016		
23	M017		
24	M018		
25	M019		
26	M020		

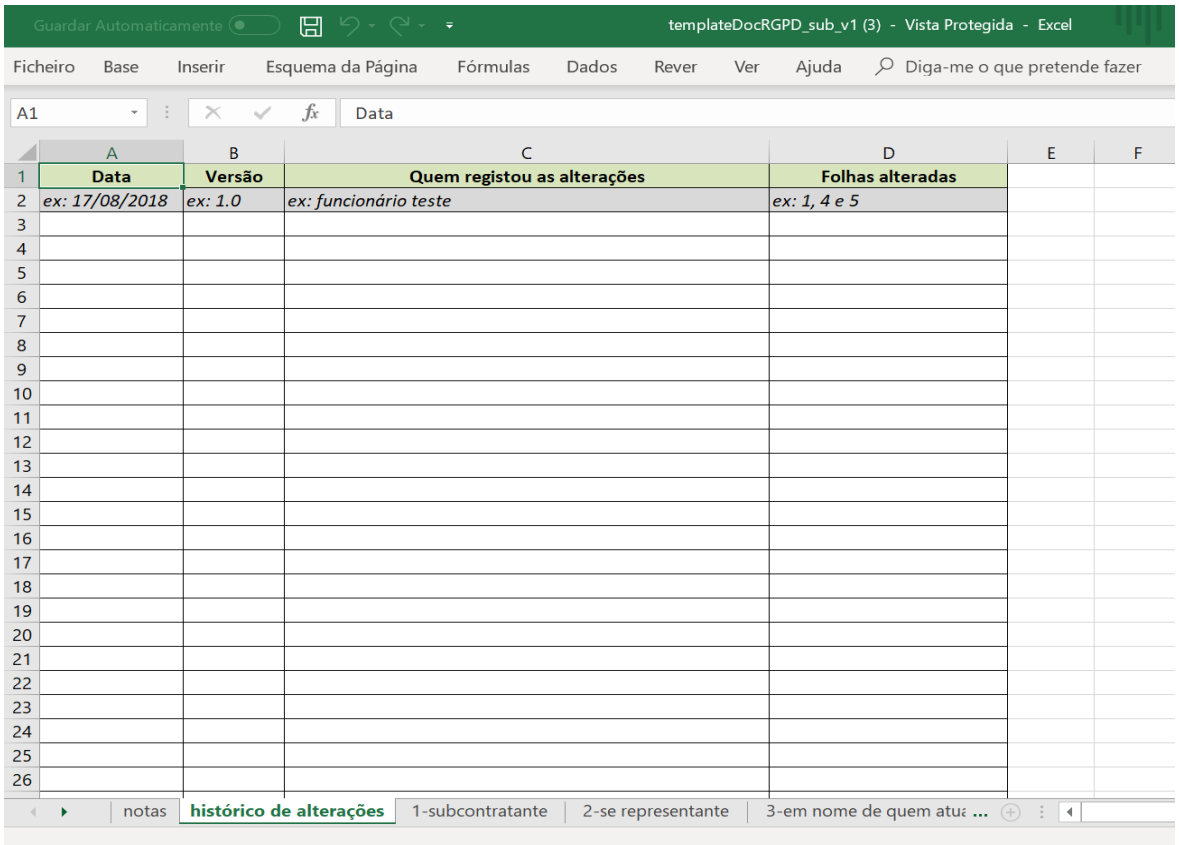
... 3-se corresponsável 4-tratamentos 5-destinatários e transf intern 6-medidas de segurança

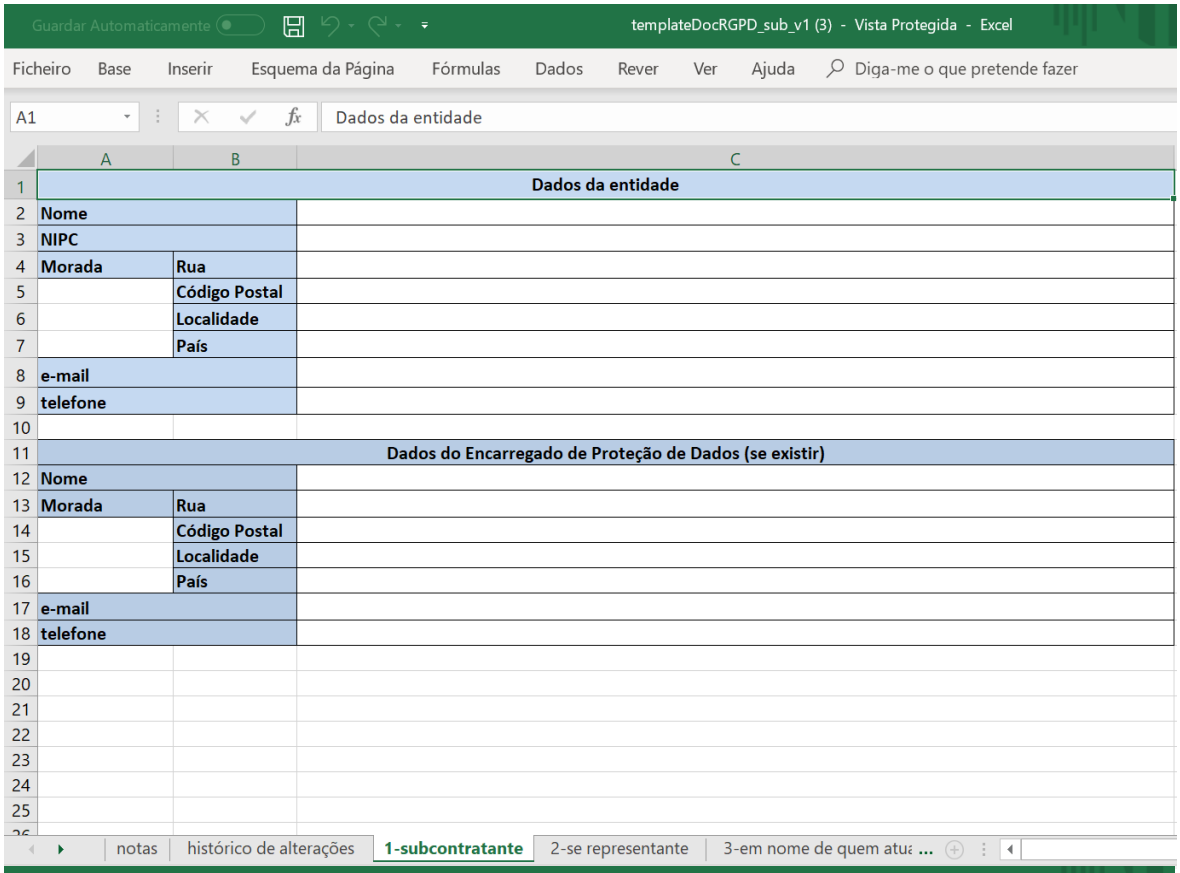


	A	D	E	F	G	H	I	J
1	**# medida**	**Tempo de conservação (se aplicável)**	**Tratamentos a que se aplica**					
2	*M000a*		*ex: T000, T005, T011*					
3	*M000b*		*ex: todos os tratamentos*					
4	*M000c*	*ex: 2 anos*	*ex: T002 a T010*					
5	*M000d*		*ex: T004*					
6	*M000e*	*ex: os backups são conservados por 3 anos*	*ex: T012*					
7	M001							
8	M002							
9	M003							
10	M004							
11	M005							
12	M006							
13	M007							
14	M008							
15	M009							
16	M010							
17	M011							
18	M012							
19	M013							
20	M014							
21	M015							
22	M016							
23	M017							

ANEXO 6: MODELO DE REGISTO PARA O SUBCONTRATANTE







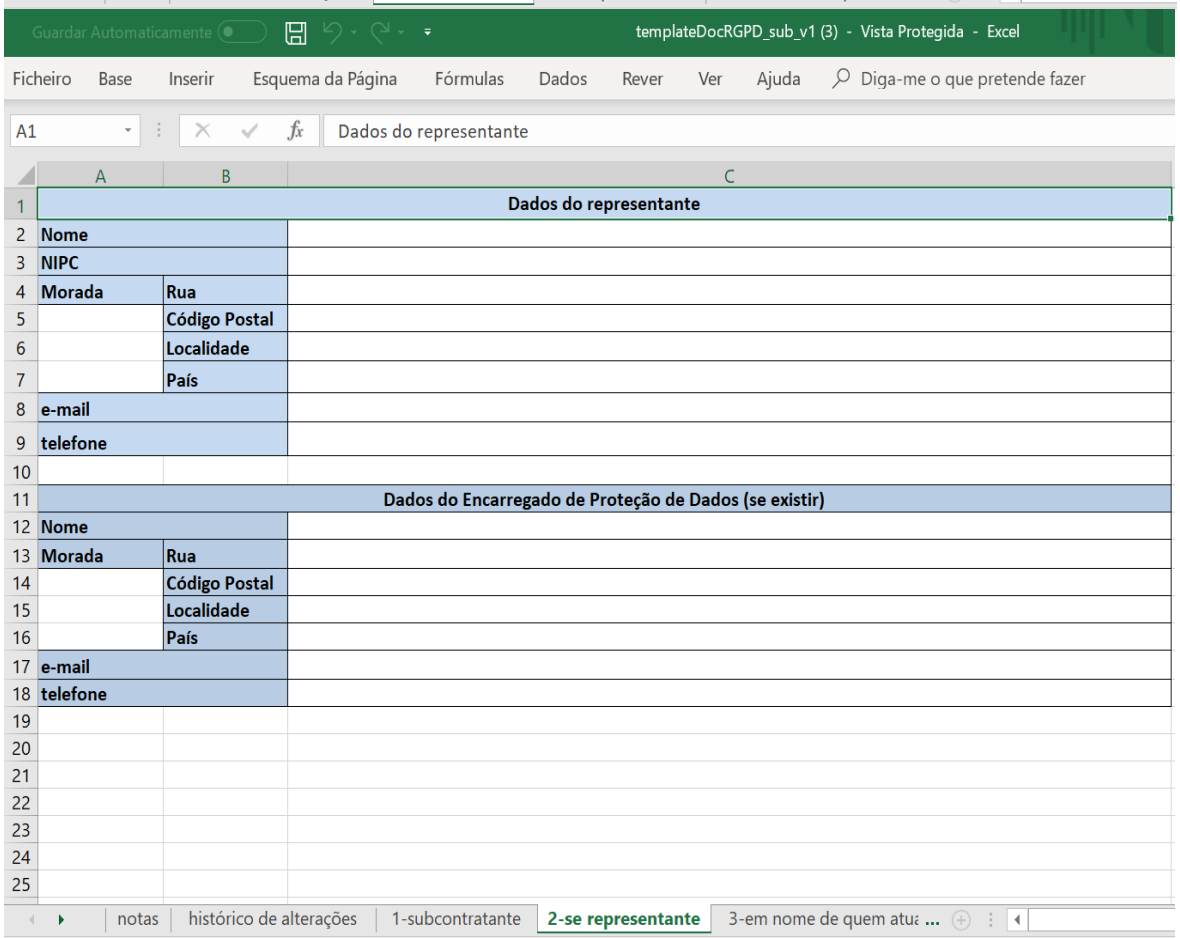
templateDocRGPD_sub_v1 (3) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

A1 Dados da entidade

	A	B	C
1	**Dados da entidade**		
2	**Nome**		
3	**NIPC**		
4	**Morada**	**Rua**	
5		**Código Postal**	
6		**Localidade**	
7		**País**	
8	**e-mail**		
9	**telefone**		
10			
11	**Dados do Encarregado de Proteção de Dados (se existir)**		
12	**Nome**		
13	**Morada**	**Rua**	
14		**Código Postal**	
15		**Localidade**	
16		**País**	
17	**e-mail**		
18	**telefone**		
19			
20			
21			
22			
23			
24			
25			

notas | histórico de alterações | **1-subcontratante** | 2-se representante | 3-em nome de quem atua ...



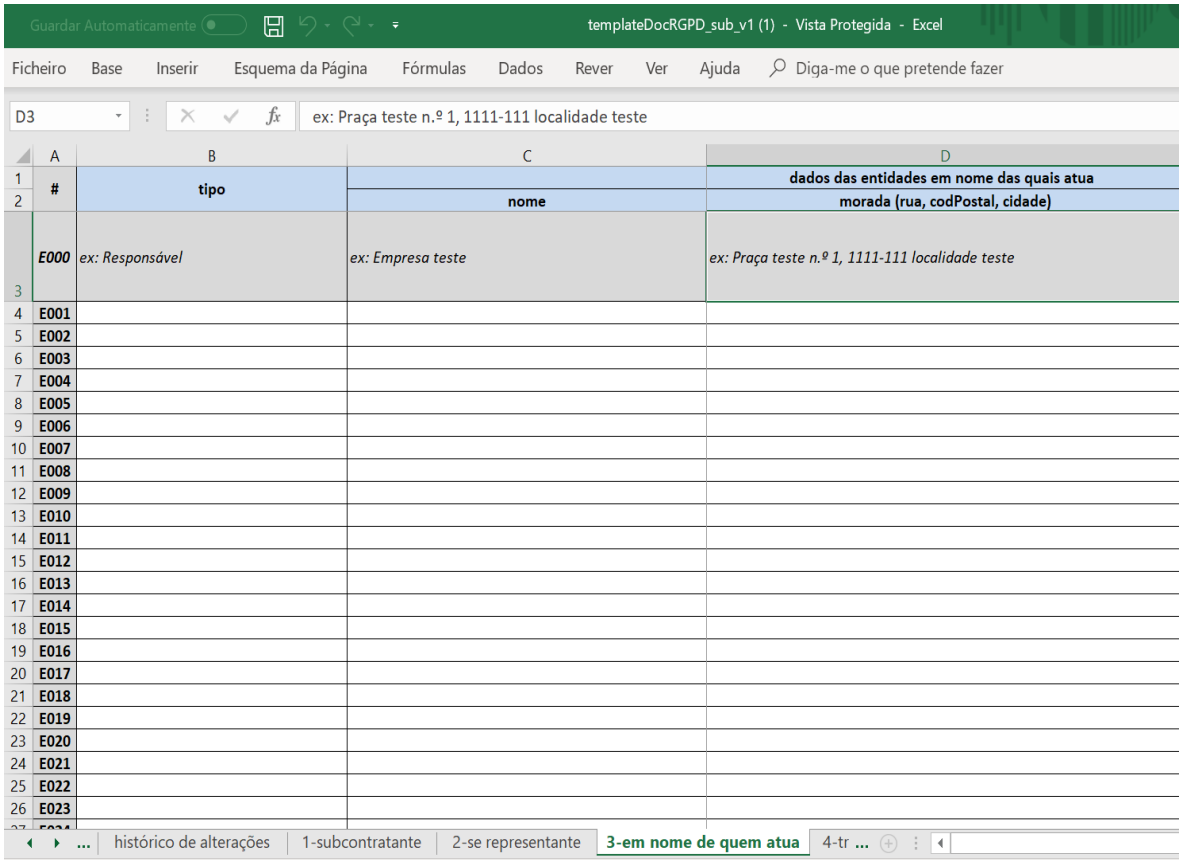
templateDocRGPD_sub_v1 (3) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

A1 Dados do representante

	A	B	C
1	**Dados do representante**		
2	**Nome**		
3	**NIPC**		
4	**Morada**	**Rua**	
5		**Código Postal**	
6		**Localidade**	
7		**País**	
8	**e-mail**		
9	**telefone**		
10			
11	**Dados do Encarregado de Proteção de Dados (se existir)**		
12	**Nome**		
13	**Morada**	**Rua**	
14		**Código Postal**	
15		**Localidade**	
16		**País**	
17	**e-mail**		
18	**telefone**		
19			
20			
21			
22			
23			
24			
25			

notas | histórico de alterações | 1-subcontratante | **2-se representante** | 3-em nome de quem atua ...

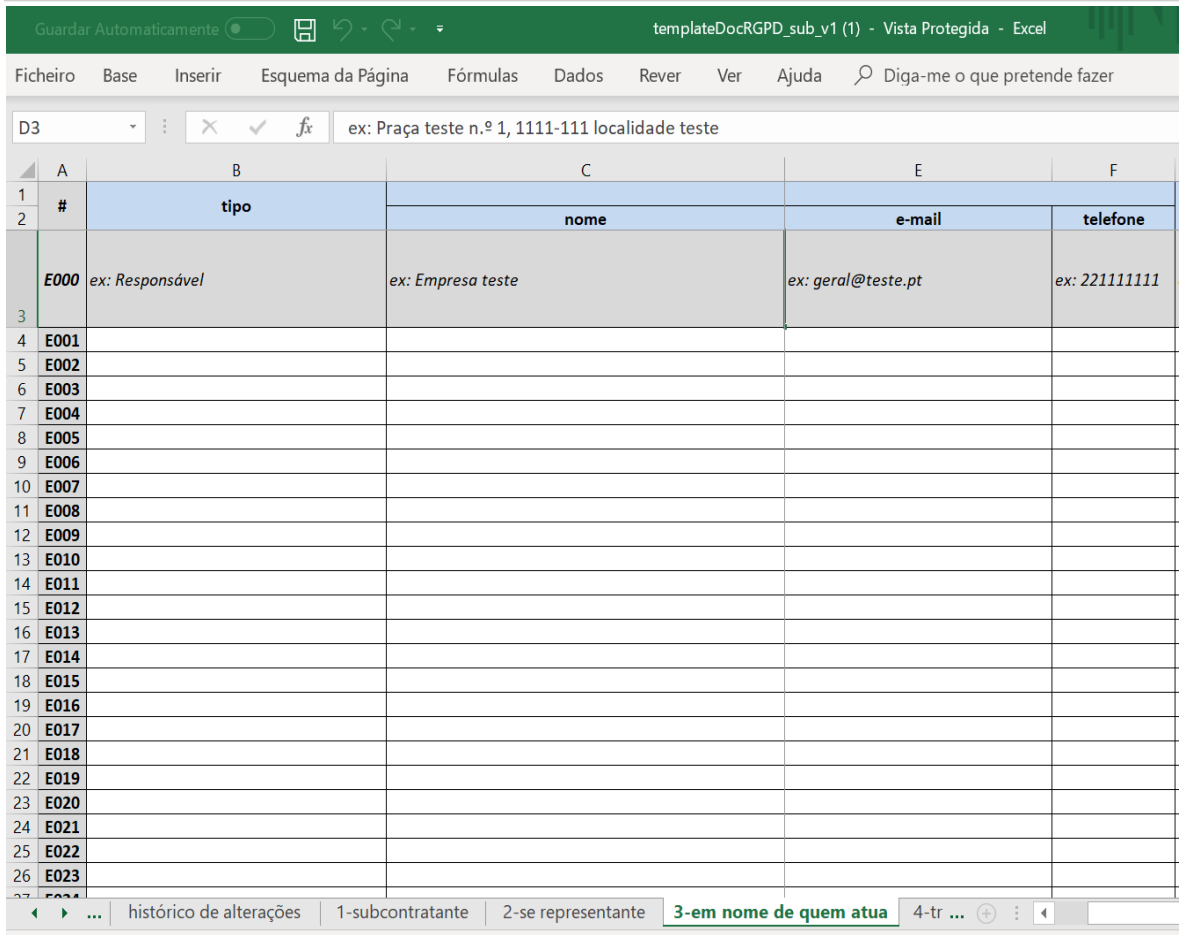

templateDocRGPD_sub_v1 (1) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

D3 ex: Praça teste n.º 1, 1111-111 localidade teste

	A	B	C	D
1	#	tipo		dados das entidades em nome das quais atua
2			nome	morada (rua, codPostal, cidade)
3	***E000***	*ex: Responsável*	*ex: Empresa teste*	*ex: Praça teste n.º 1, 1111-111 localidade teste*
4	**E001**			
5	**E002**			
6	**E003**			
7	**E004**			
8	**E005**			
9	**E006**			
10	**E007**			
11	**E008**			
12	**E009**			
13	**E010**			
14	**E011**			
15	**E012**			
16	**E013**			
17	**E014**			
18	**E015**			
19	**E016**			
20	**E017**			
21	**E018**			
22	**E019**			
23	**E020**			
24	**E021**			
25	**E022**			
26	**E023**			

... histórico de alterações | 1-subcontratante | 2-se representante | **3-em nome de quem atua** | 4-tr ...

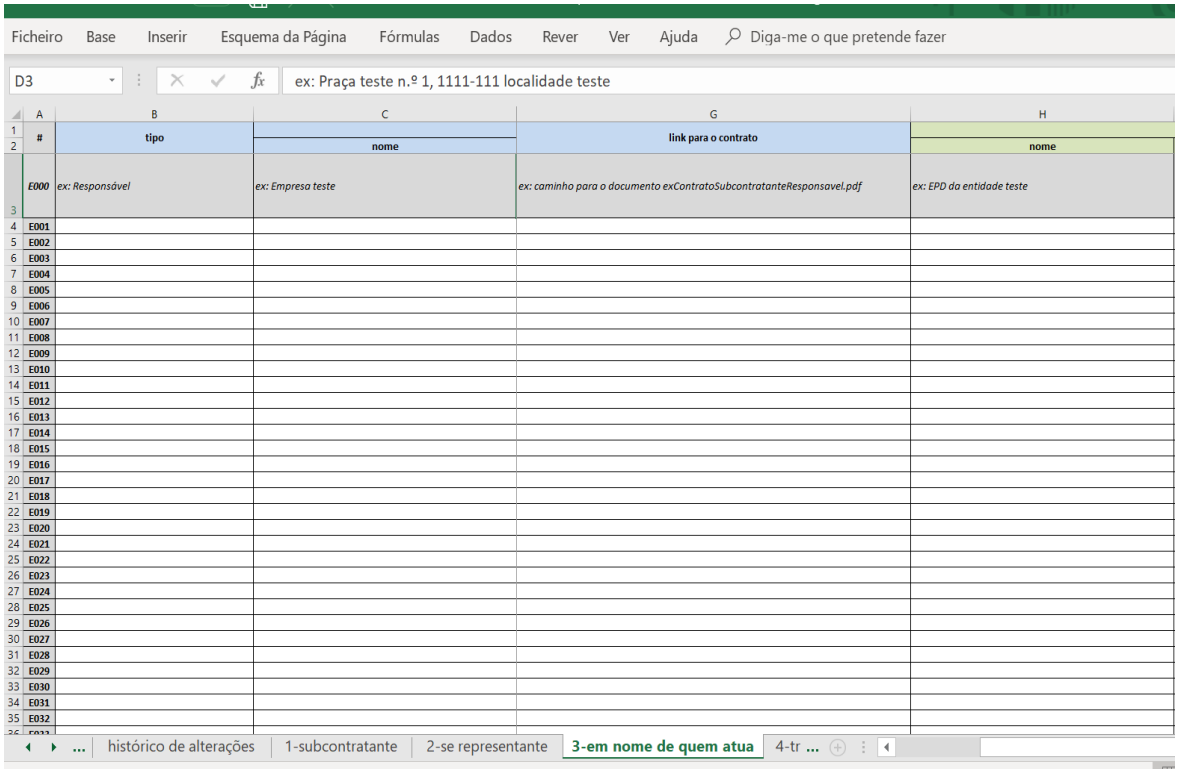

templateDocRGPD_sub_v1 (1) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

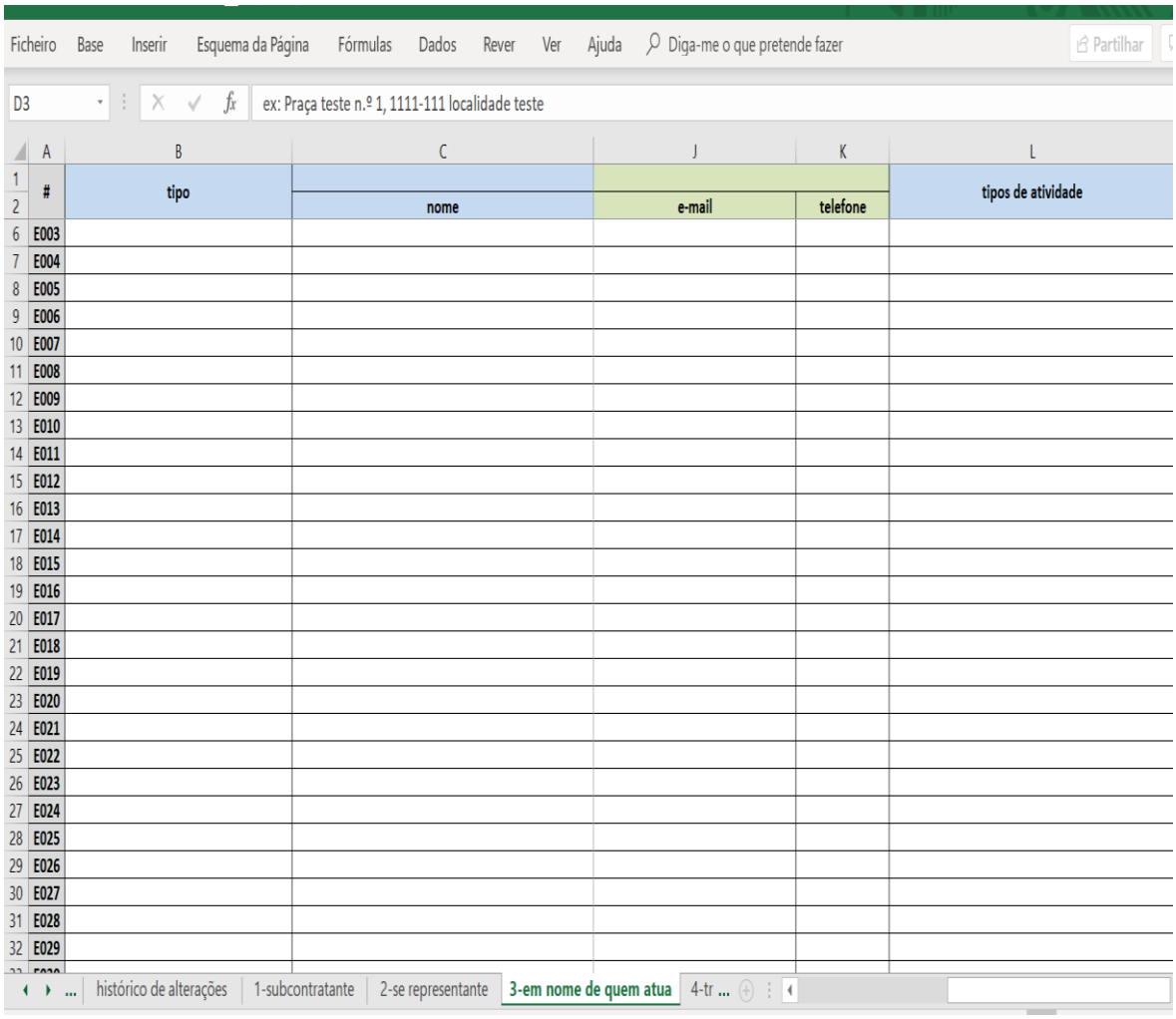
D3 ex: Praça teste n.º 1, 1111-111 localidade teste

	A	B	C	E	F
1	#	tipo			
2			nome	e-mail	telefone
3	***E000***	*ex: Responsável*	*ex: Empresa teste*	*ex: geral@teste.pt*	*ex: 221111111*
4	**E001**				
5	**E002**				
6	**E003**				
7	**E004**				
8	**E005**				
9	**E006**				
10	**E007**				
11	**E008**				
12	**E009**				
13	**E010**				
14	**E011**				
15	**E012**				
16	**E013**				
17	**E014**				
18	**E015**				
19	**E016**				
20	**E017**				
21	**E018**				
22	**E019**				
23	**E020**				
24	**E021**				
25	**E022**				
26	**E023**				

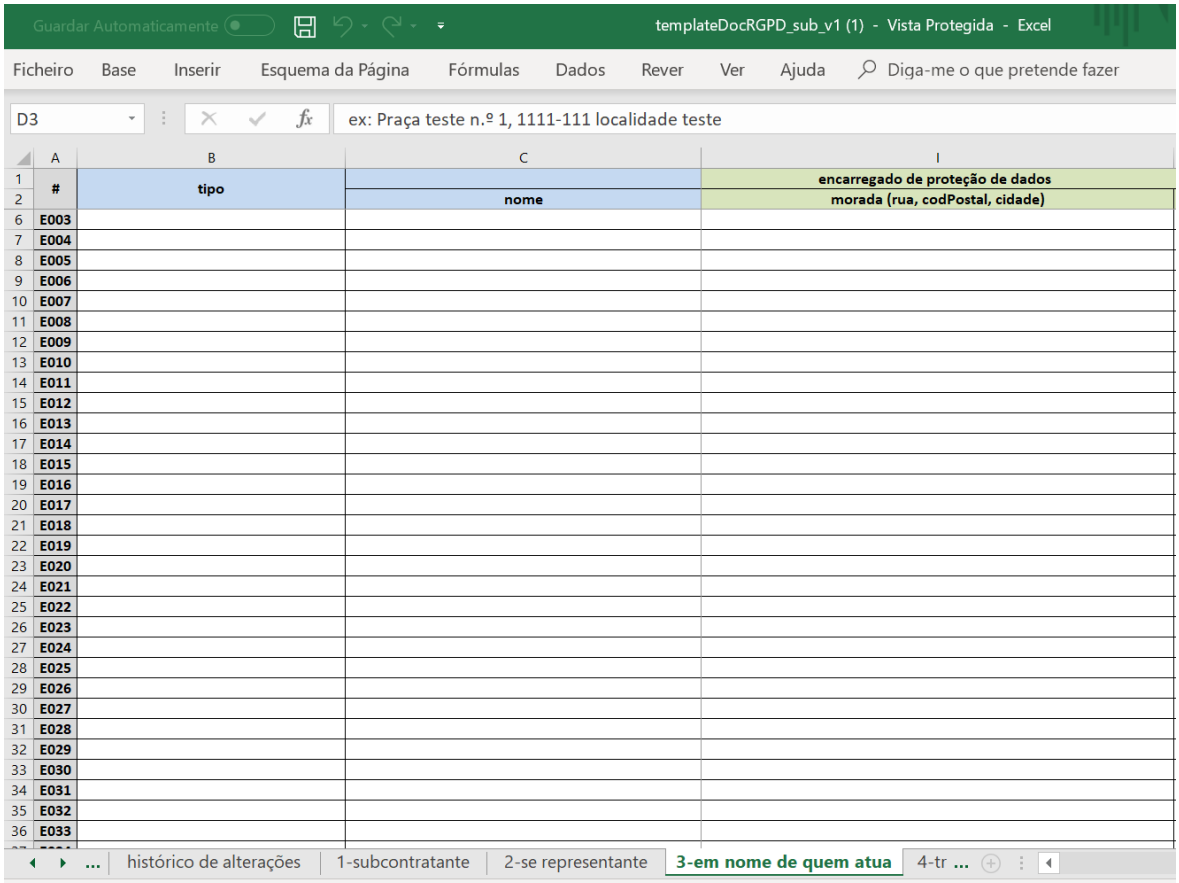
... histórico de alterações | 1-subcontratante | 2-se representante | **3-em nome de quem atua** | 4-tr ...



#	tipo	nome	link para o contrato	nome
E000	ex: Responsável	ex: Empresa teste	ex: caminho para o documento exContratoSubcontratanteResponsavel.pdf	ex: EPD da entidade teste
E001				
E002				
E003				
E004				
E005				
E006				
E007				
E008				
E009				
E010				
E011				
E012				
E013				
E014				
E015				
E016				
E017				
E018				
E019				
E020				
E021				
E022				
E023				
E024				
E025				
E026				
E027				
E028				
E029				
E030				
E031				
E032				



#	tipo	nome	e-mail	telefone	tipos de atividade
E003					
E004					
E005					
E006					
E007					
E008					
E009					
E010					
E011					
E012					
E013					
E014					
E015					
E016					
E017					
E018					
E019					
E020					
E021					
E022					
E023					
E024					
E025					
E026					
E027					
E028					
E029					

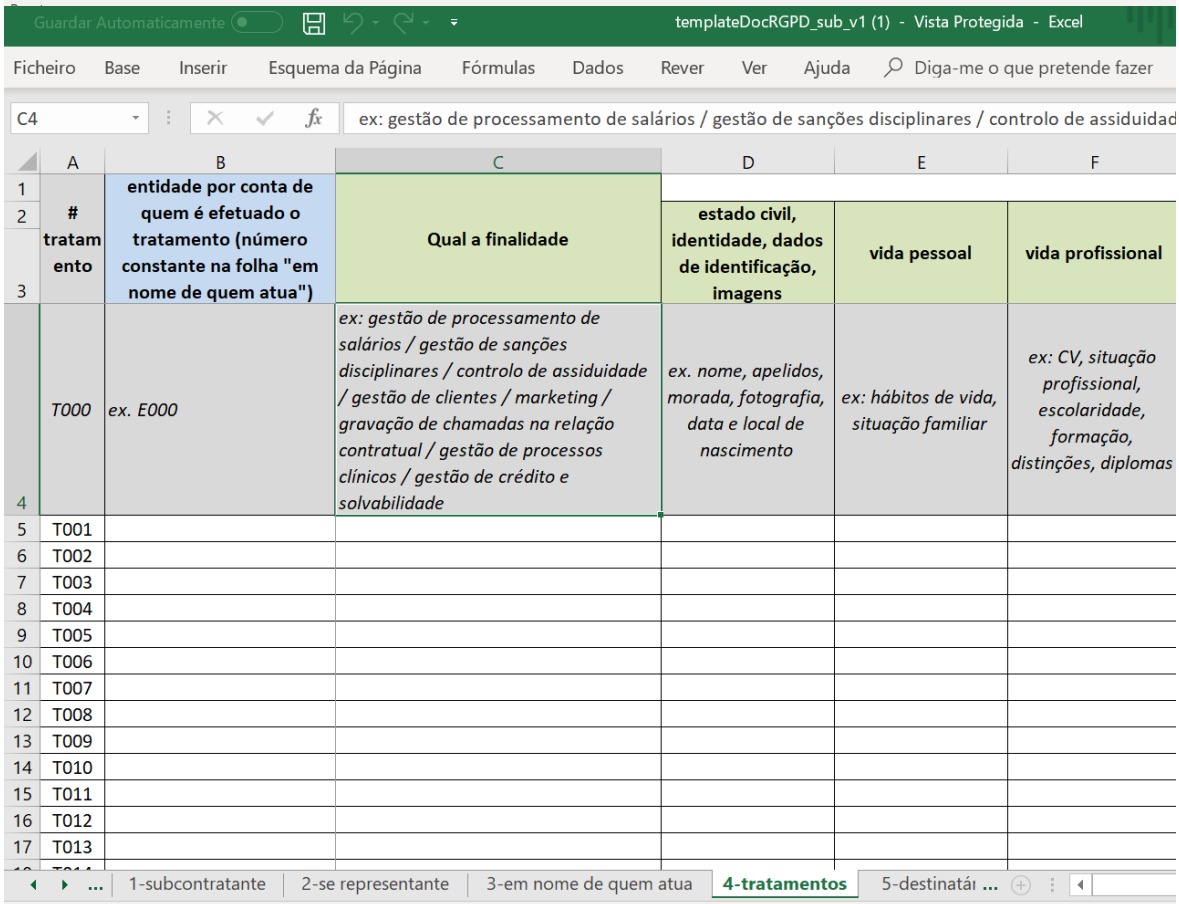

templateDocRGPD_sub_v1 (1) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

D3 ex: Praça teste n.º 1, 1111-111 localidade teste

	A	B	C	I
1	#	tipo		encarregado de proteção de dados
2			nome	morada (rua, codPostal, cidade)
6	E003			
7	E004			
8	E005			
9	E006			
10	E007			
11	E008			
12	E009			
13	E010			
14	E011			
15	E012			
16	E013			
17	E014			
18	E015			
19	E016			
20	E017			
21	E018			
22	E019			
23	E020			
24	E021			
25	E022			
26	E023			
27	E024			
28	E025			
29	E026			
30	E027			
31	E028			
32	E029			
33	E030			
34	E031			
35	E032			
36	E033			

... histórico de alterações | 1-subcontratante | 2-se representante | **3-em nome de quem atua** | 4-tr ...

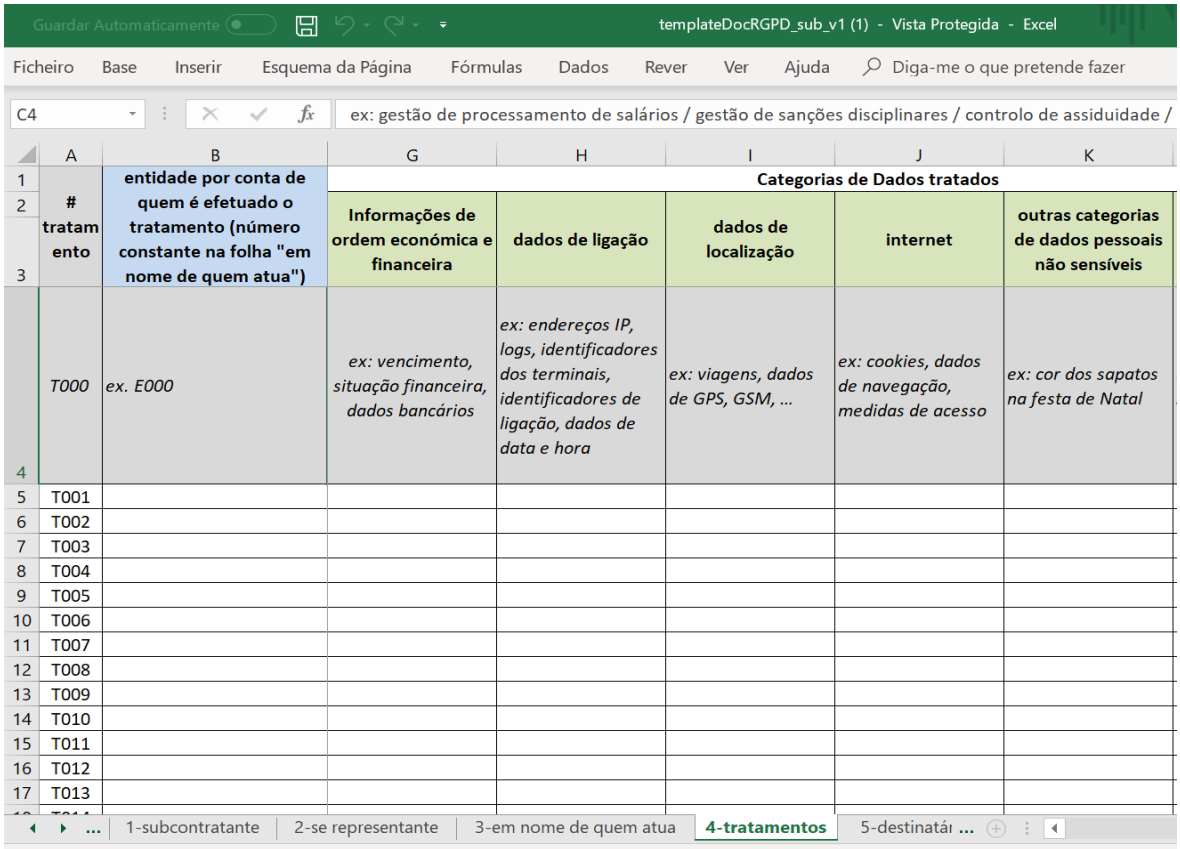

templateDocRGPD_sub_v1 (1) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

C4 ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidad

	A	B	C	D	E	F
1						
2	# tratamento	entidade por conta de quem é efetuado o tratamento (número constante na folha "em nome de quem atua")	Qual a finalidade	estado civil, identidade, dados de identificação, imagens	vida pessoal	vida profissional
3						
4	*T000*	*ex. E000*	*ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade*	*ex. nome, apelidos, morada, fotografia, data e local de nascimento*	*ex: hábitos de vida, situação familiar*	*ex: CV, situação profissional, escolaridade, formação, distinções, diplomas*
5	T001					
6	T002					
7	T003					
8	T004					
9	T005					
10	T006					
11	T007					
12	T008					
13	T009					
14	T010					
15	T011					
16	T012					
17	T013					

... 1-subcontratante | 2-se representante | 3-em nome de quem atua | **4-tratamentos** | 5-destinatái ...



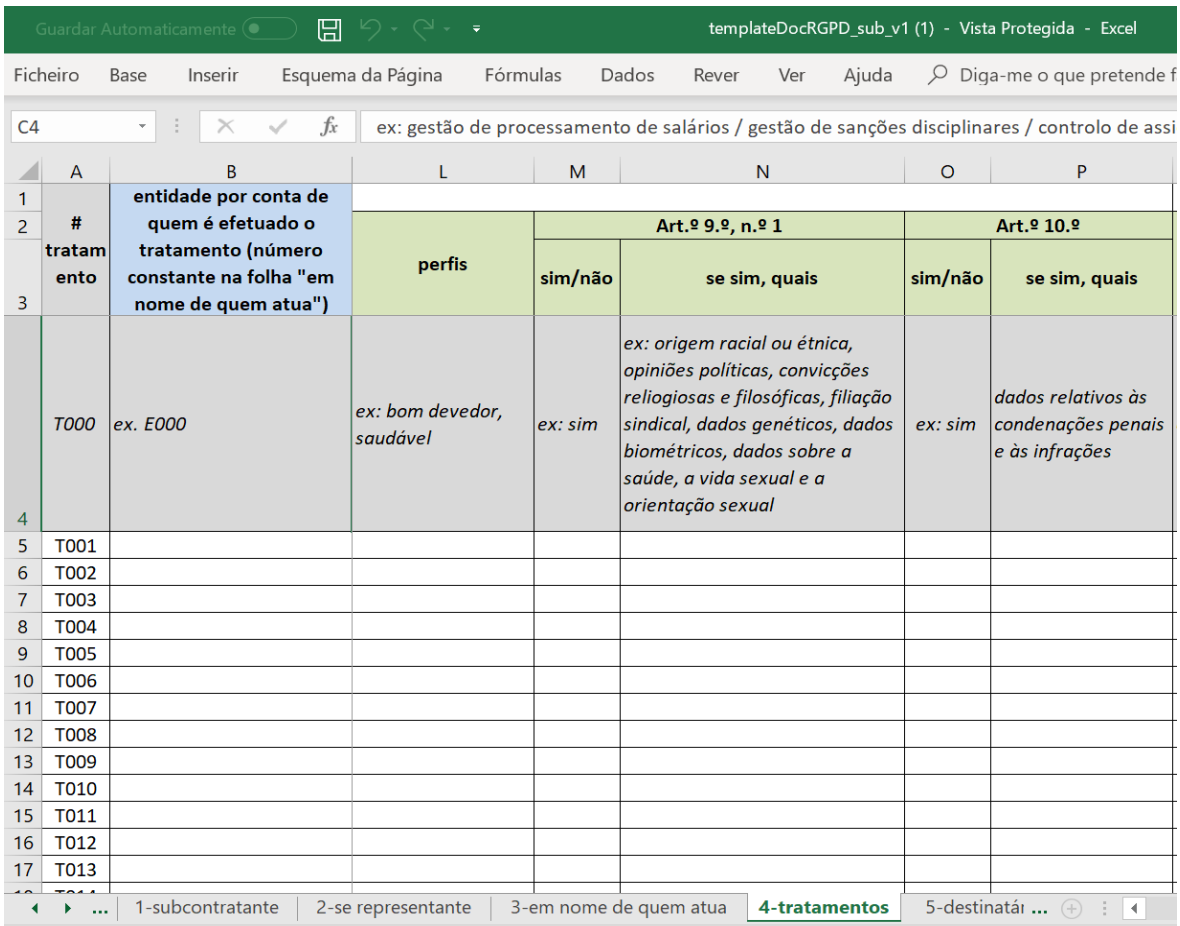
templateDocRGPD_sub_v1 (1) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

C4 ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade /

	A	B	G	H	I	J	K
1			Categorias de Dados tratados				
2	# tratamento	entidade por conta de quem é efetuado o tratamento (número constante na folha "em nome de quem atua")	Informações de ordem económica e financeira	dados de ligação	dados de localização	internet	outras categorias de dados pessoais não sensíveis
3							
4	*T000*	*ex. E000*	*ex: vencimento, situação financeira, dados bancários*	*ex: endereços IP, logs, identificadores dos terminais, identificadores de ligação, dados de data e hora*	*ex: viagens, dados de GPS, GSM, ...*	*ex: cookies, dados de navegação, medidas de acesso*	*ex: cor dos sapatos na festa de Natal*
5	T001						
6	T002						
7	T003						
8	T004						
9	T005						
10	T006						
11	T007						
12	T008						
13	T009						
14	T010						
15	T011						
16	T012						
17	T013						

... 1-subcontratante 2-se representante 3-em nome de quem atua **4-tratamentos** 5-destinatái ...



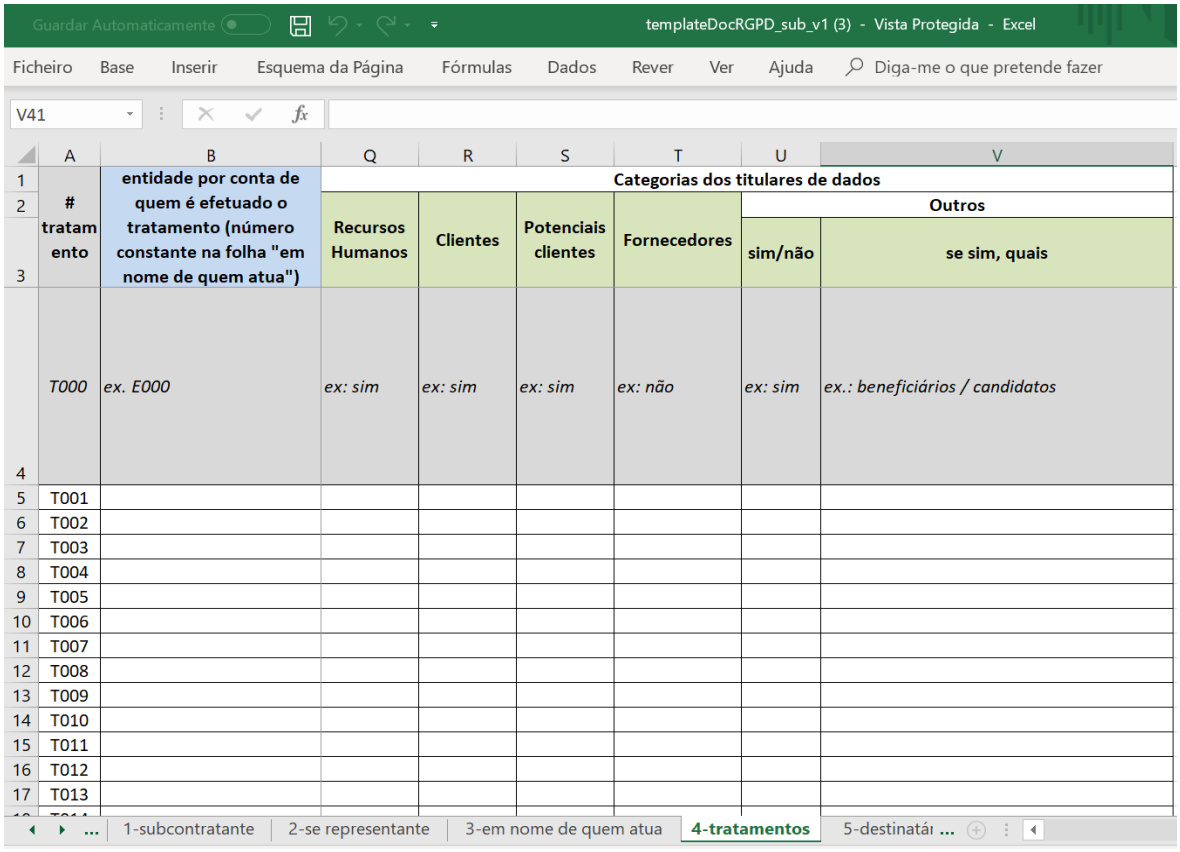
templateDocRGPD_sub_v1 (1) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende f

C4 ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assi

	A	B	L	M	N	O	P
1							
2	# tratamento	entidade por conta de quem é efetuado o tratamento (número constante na folha "em nome de quem atua")	perfis	Art.º 9.º, n.º 1		Art.º 10.º	
3				sim/não	se sim, quais	sim/não	se sim, quais
4	*T000*	*ex. E000*	*ex: bom devedor, saudável*	*ex: sim*	*ex: origem racial ou étnica, opiniões políticas, convicções religiosas e filosóficas, filiação sindical, dados genéticos, dados biométricos, dados sobre a saúde, a vida sexual e a orientação sexual*	*ex: sim*	*dados relativos às condenações penais e às infrações*
5	T001						
6	T002						
7	T003						
8	T004						
9	T005						
10	T006						
11	T007						
12	T008						
13	T009						
14	T010						
15	T011						
16	T012						
17	T013						

... 1-subcontratante 2-se representante 3-em nome de quem atua **4-tratamentos** 5-destinatái ...



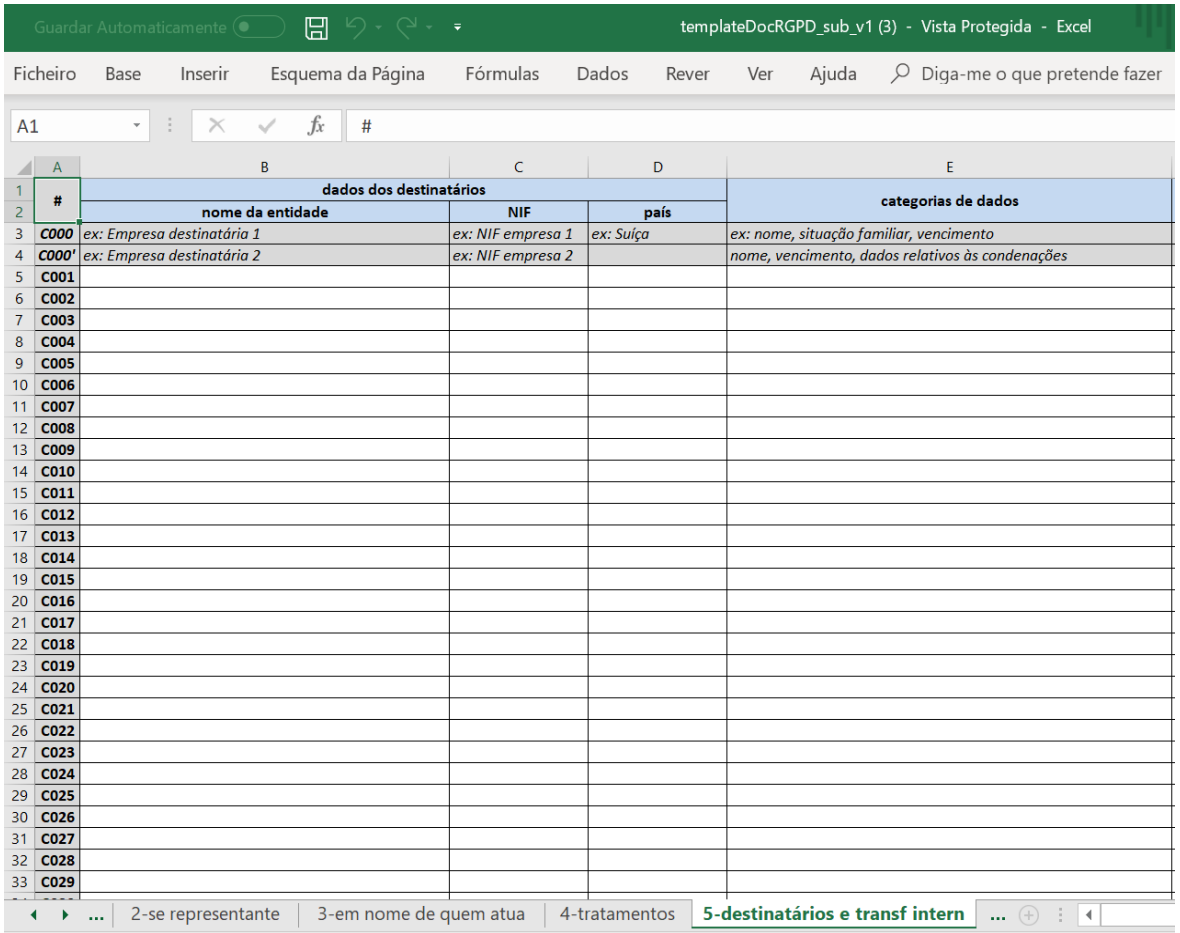
templateDocRGPD_sub_v1 (3) - Vista Protegida - Excel

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

V41

	A	B	Q	R	S	T	U	V
1			Categorias dos titulares de dados					
2	#	entidade por conta de quem é efetuado o tratamento (número constante na folha "em nome de quem atua")					Outros	
3	tratamento		Recursos Humanos	Clientes	Potenciais clientes	Fornecedores	sim/não	se sim, quais
4	*T000*	*ex. E000*	*ex: sim*	*ex: sim*	*ex: sim*	*ex: não*	*ex: sim*	*ex.: beneficiários / candidatos*
5	T001							
6	T002							
7	T003							
8	T004							
9	T005							
10	T006							
11	T007							
12	T008							
13	T009							
14	T010							
15	T011							
16	T012							
17	T013							

... 1-subcontratante 2-se representante 3-em nome de quem atua **4-tratamentos** 5-destinatár ...



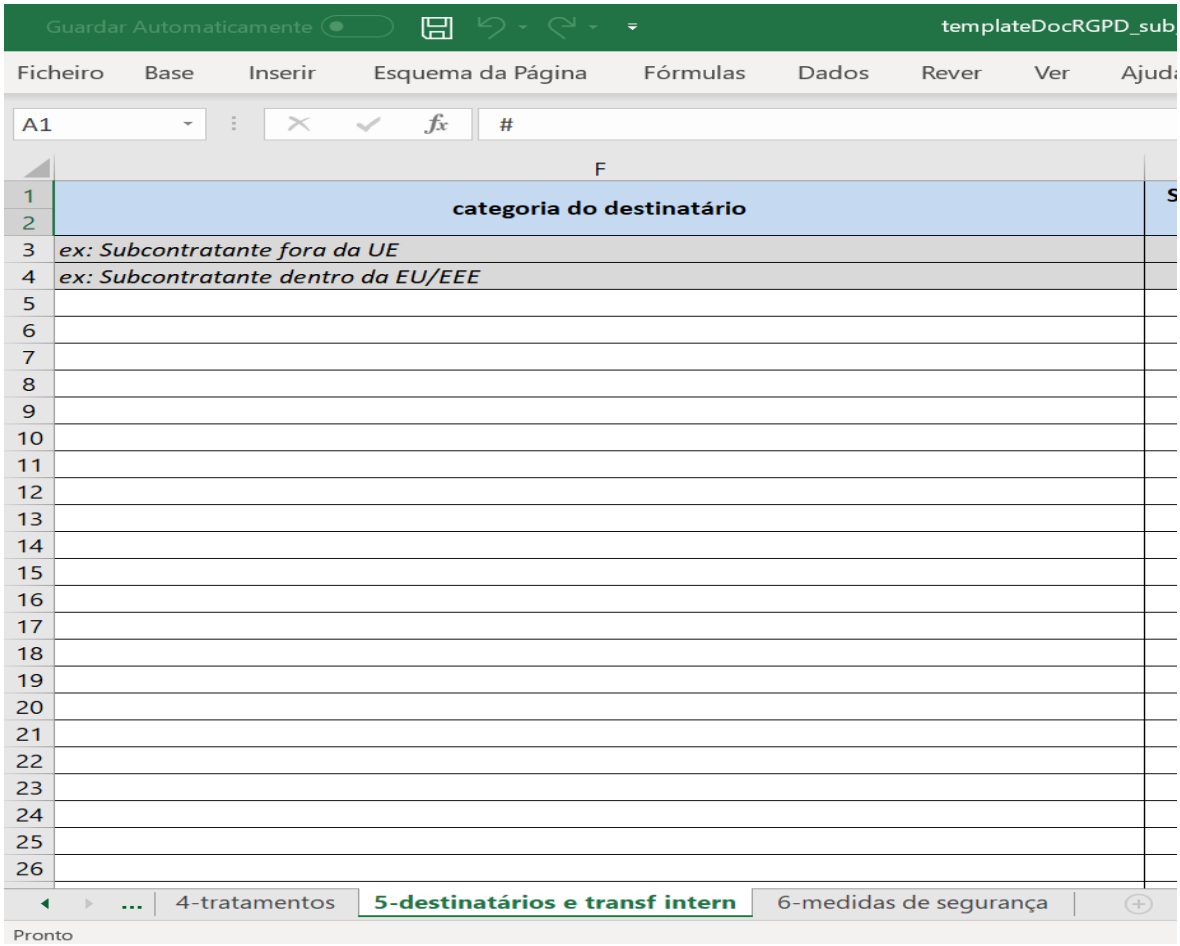
templateDocRGPD_sub_v1 (3) - Vista Protegida - Excel

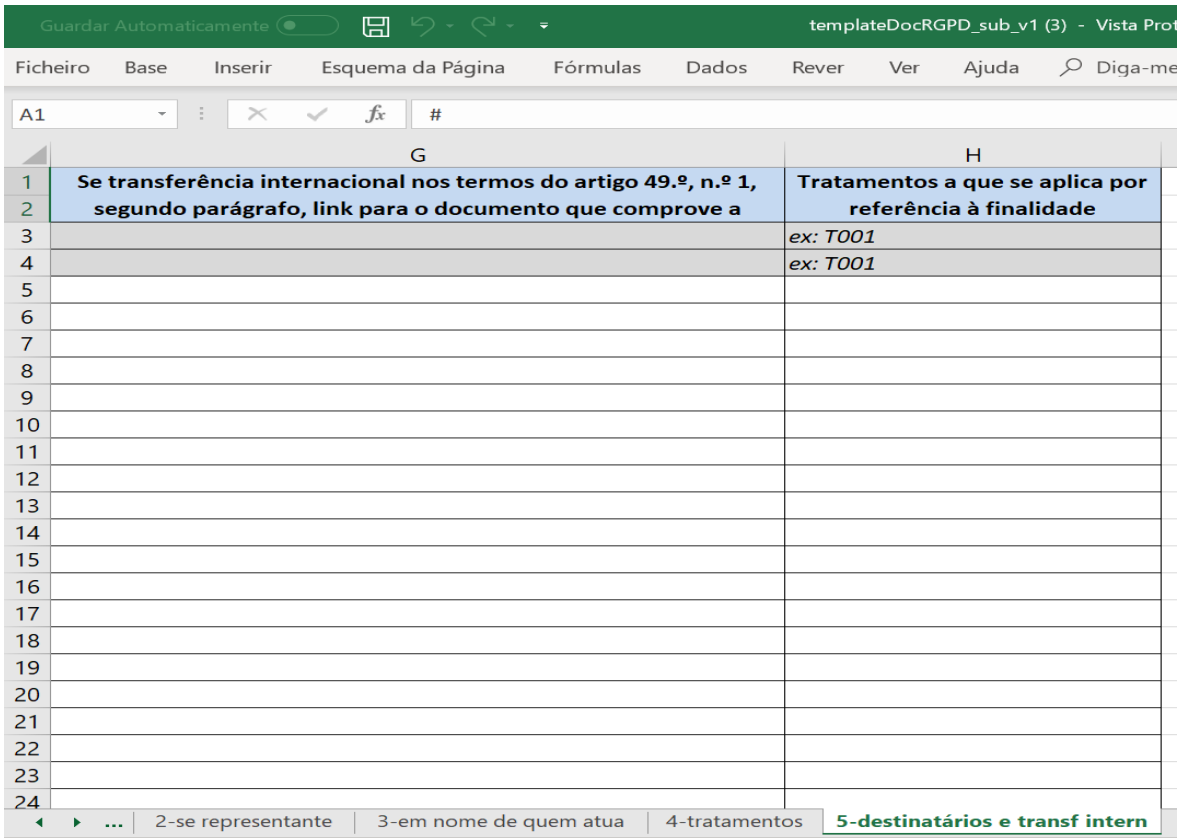
Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

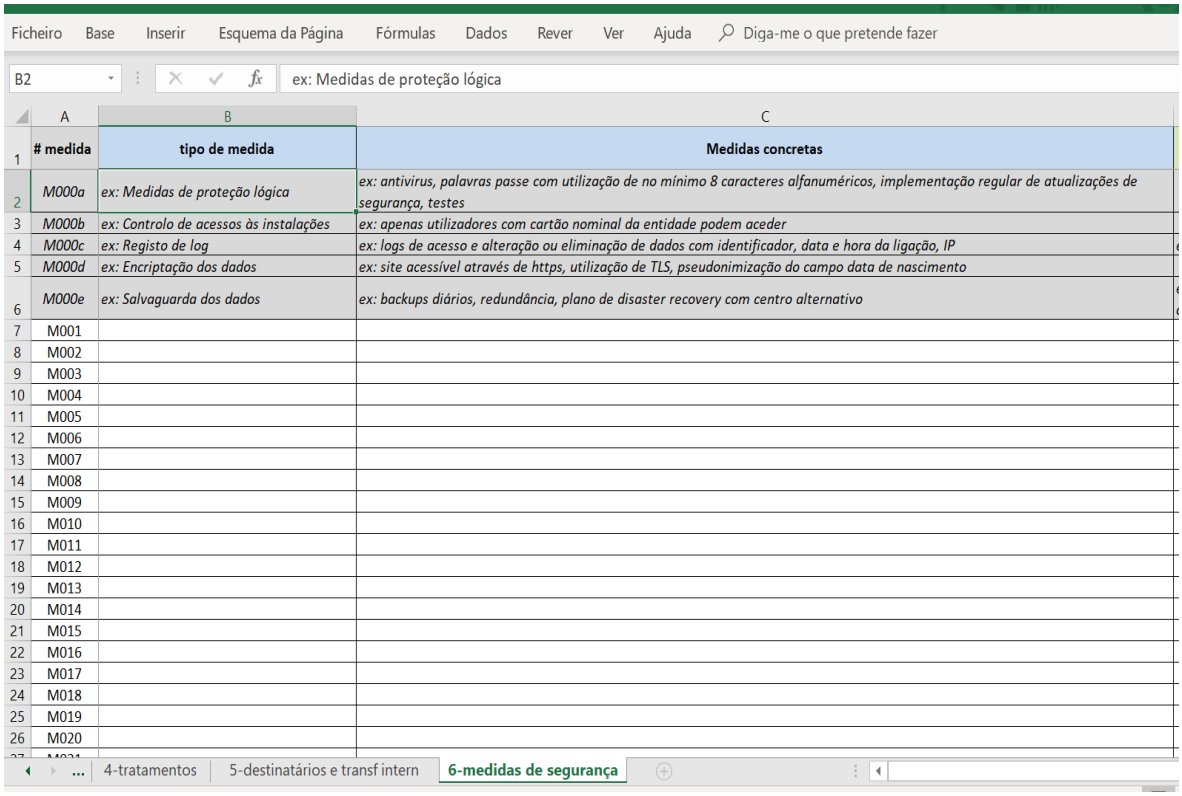
A1 #

	A	B	C	D	E
1	#	dados dos destinatários			categorias de dados
2		nome da entidade	NIF	país	
3	***C000***	*ex: Empresa destinatária 1*	*ex: NIF empresa 1*	*ex: Suíça*	*ex: nome, situação familiar, vencimento*
4	***C000'***	*ex: Empresa destinatária 2*	*ex: NIF empresa 2*		*nome, vencimento, dados relativos às condenações*
5	**C001**				
6	**C002**				
7	**C003**				
8	**C004**				
9	**C005**				
10	**C006**				
11	**C007**				
12	**C008**				
13	**C009**				
14	**C010**				
15	**C011**				
16	**C012**				
17	**C013**				
18	**C014**				
19	**C015**				
20	**C016**				
21	**C017**				
22	**C018**				
23	**C019**				
24	**C020**				
25	**C021**				
26	**C022**				
27	**C023**				
28	**C024**				
29	**C025**				
30	**C026**				
31	**C027**				
32	**C028**				
33	**C029**				

... 2-se representante 3-em nome de quem atua 4-tratamentos **5-destinatários e transf intern** ...


Guardar Automaticamente
templateDocRGPD_sub
Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda
A1
#
F
categoria do destinatário
ex: Subcontratante fora da UE
ex: Subcontratante dentro da EU/EEE
4-tratamentos
5-destinatários e transf intern
6-medidas de segurança
Pronto


Guardar Automaticamente
templateDocRGPD_sub_v1 (3) - Vista Prot
Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me
A1
#
G
Se transferência internacional nos termos do artigo 49.º, n.º 1, segundo parágrafo, link para o documento que comprove a
H
Tratamentos a que se aplica por referência à finalidade
ex: T001
ex: T001
2-se representante
3-em nome de quem atua
4-tratamentos
5-destinatários e transf intern

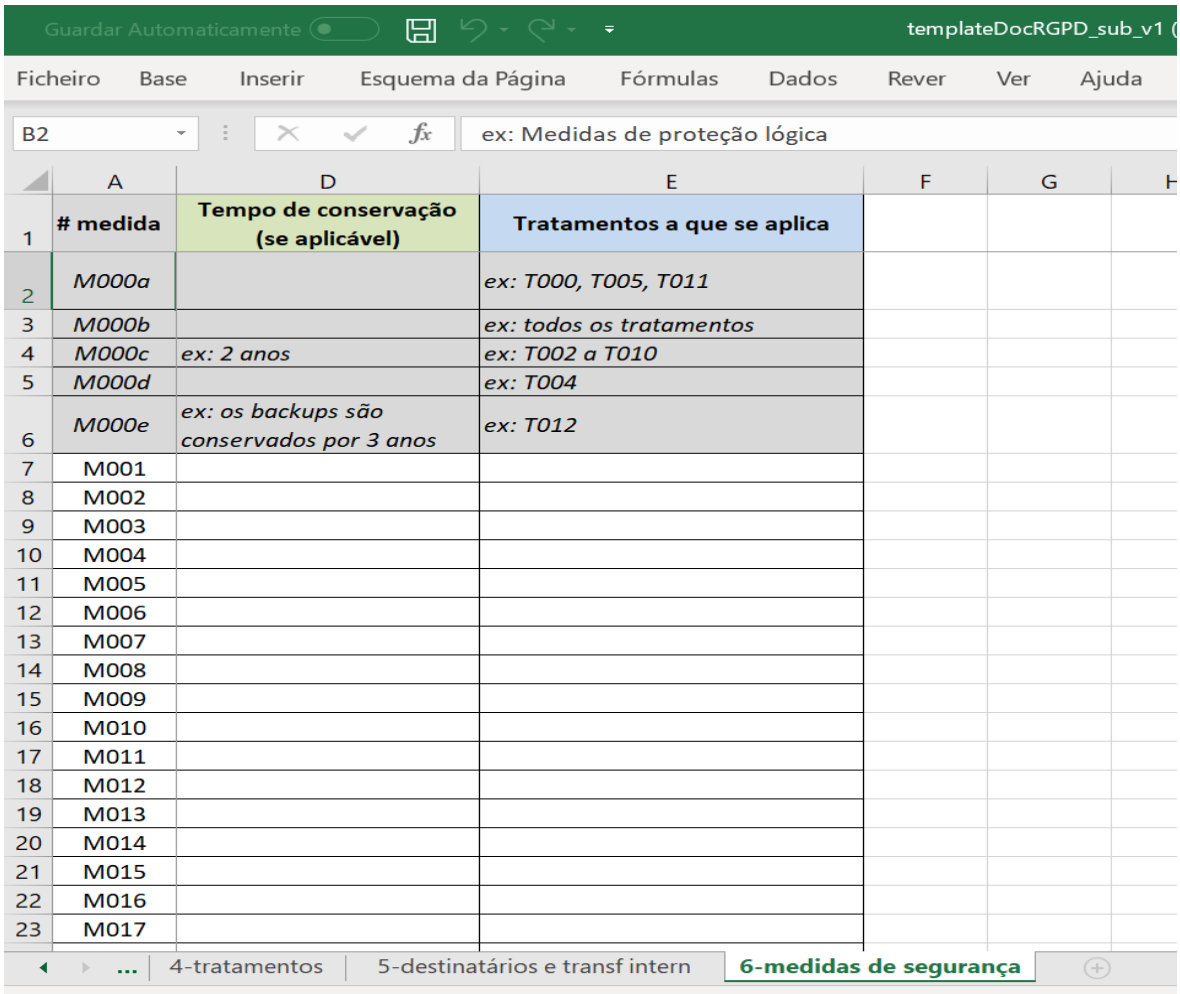


Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda Diga-me o que pretende fazer

B2 ex: Medidas de proteção lógica

# medida	tipo de medida	Medidas concretas
M000a	*ex: Medidas de proteção lógica*	*ex: antivirus, palavras passe com utilização de no mínimo 8 caracteres alfanuméricos, implementação regular de atualizações de segurança, testes*
M000b	*ex: Controlo de acessos às instalações*	*ex: apenas utilizadores com cartão nominal da entidade podem aceder*
M000c	*ex: Registo de log*	*ex: logs de acesso e alteração ou eliminação de dados com identificador, data e hora da ligação, IP*
M000d	*ex: Encriptação dos dados*	*ex: site acessível através de https, utilização de TLS, pseudonimização do campo data de nascimento*
M000e	*ex: Salvaguarda dos dados*	*ex: backups diários, redundância, plano de disaster recovery com centro alternativo*
M001		
M002		
M003		
M004		
M005		
M006		
M007		
M008		
M009		
M010		
M011		
M012		
M013		
M014		
M015		
M016		
M017		
M018		
M019		
M020		

... 4-tratamentos 5-destinatários e transf intern 6-medidas de segurança



Guardar Automaticamente templateDocRGPD_sub_v1

Ficheiro Base Inserir Esquema da Página Fórmulas Dados Rever Ver Ajuda

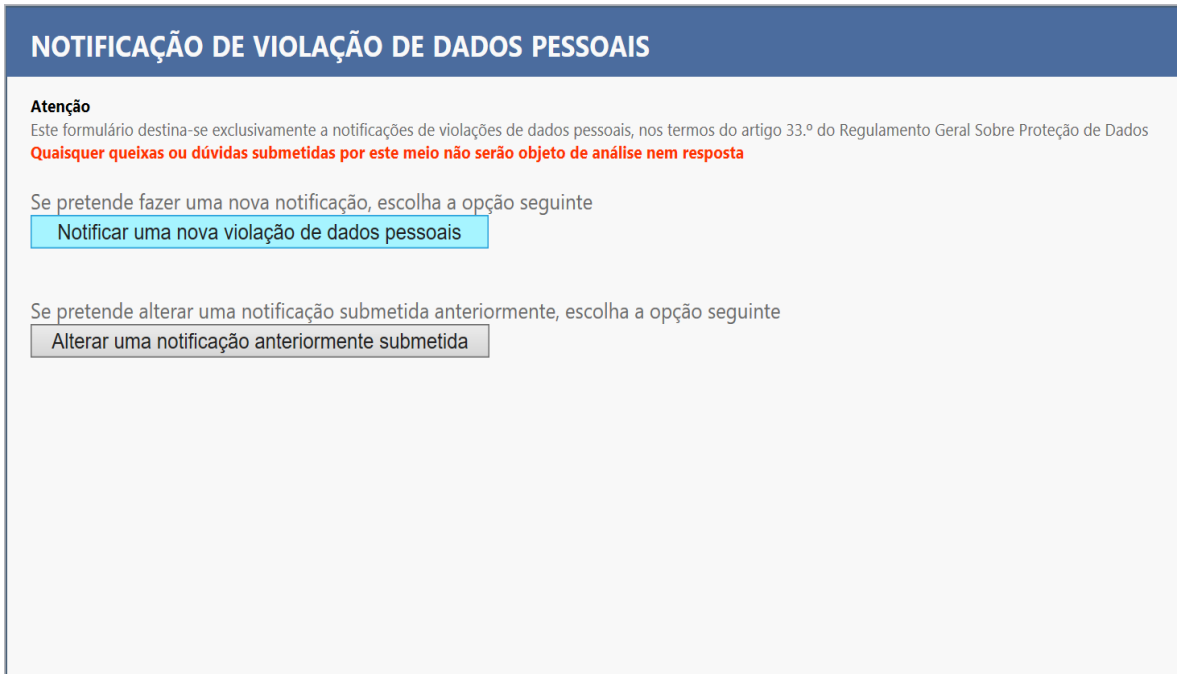
B2 ex: Medidas de proteção lógica

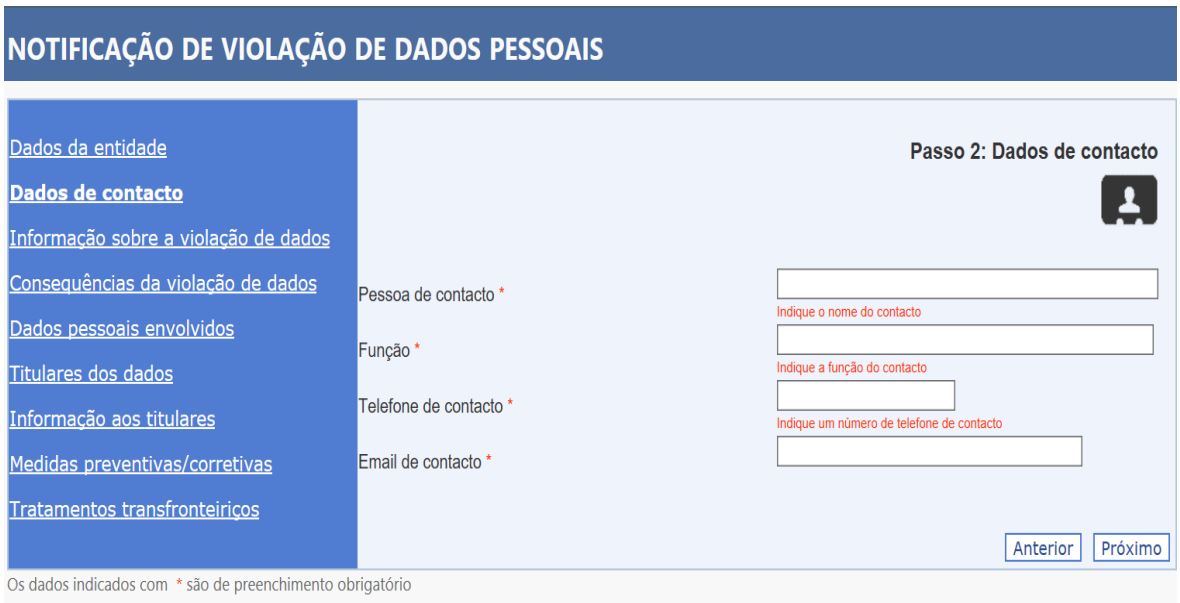
# medida	Tempo de conservação (se aplicável)	Tratamentos a que se aplica
M000a		*ex: T000, T005, T011*
M000b		*ex: todos os tratamentos*
M000c	*ex: 2 anos*	*ex: T002 a T010*
M000d		*ex: T004*
M000e	*ex: os backups são conservados por 3 anos*	*ex: T012*
M001		
M002		
M003		
M004		
M005		
M006		
M007		
M008		
M009		
M010		
M011		
M012		
M013		
M014		
M015		
M016		
M017		

... 4-tratamentos 5-destinatários e transf intern 6-medidas de segurança

ANEXO 7: NOTIFICAÇÃO DA VIOLAÇÃO DE DADOS

CNPD, disponível em: http://www.cnpd.pt/bin/notifica_rgpd/databreach.htm


NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS
Atenção
Este formulário destina-se exclusivamente a notificações de violações de dados pessoais, nos termos do artigo 33.º do Regulamento Geral Sobre Proteção de Dados
Quaisquer queixas ou dúvidas submetidas por este meio não serão objeto de análise nem resposta
Se pretende fazer uma nova notificação, escolha a opção seguinte
Notificar uma nova violação de dados pessoais
Se pretende alterar uma notificação submetida anteriormente, escolha a opção seguinte
Alterar uma notificação anteriormente submetida


NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS
Dados da entidade
Dados de contacto
Informação sobre a violação de dados
Consequências da violação de dados
Dados pessoais envolvidos
Titulares dos dados
Informação aos titulares
Medidas preventivas/corretivas
Tratamentos transfronteiriços
Passo 2: Dados de contacto
Pessoa de contacto *
Indique o nome do contacto
Função *
Indique a função do contacto
Telefone de contacto *
Indique um número de telefone de contacto
Email de contacto *
Anterior
Próximo
Os dados indicados com * são de preenchimento obrigatório


NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS
Dados da entidade
Dados de contacto
Informação sobre a violação de dados
Consequências da violação de dados
Dados pessoais envolvidos
Titulares dos dados
Informação aos titulares
Medidas preventivas/corretivas
Tratamentos transfronteiriços
Passo 3: Informação sobre a violação de dados
Descrição da violação *
Hora/data início da violação *
Hora/data fim da violação *
Janeiro de 2019
Hora/data em que teve conhecimento da violação *
Forma como a violação foi identificada *
Tipo de violação *
(assinale pelo menos uma opção)
Integridade
Confidencialidade
Disponibilidade
Natureza da violação *
Equipamento perdido ou roubado
Documentos perdidos ou roubados
Correio perdido ou acedido indevidamente
Hacking
Malware
Phishing
Outra
Causa da violação *
Ato interno não malicioso
Ato interno malicioso
Ato externo não malicioso
Ato externo malicioso
Outra
Anterior
Próximo

NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS

Dados da entidade
Dados de contacto
Informação sobre a violação de dados
Consequências da violação de dados
Dados pessoais envolvidos
Titulares dos dados
Informação aos titulares
Medidas preventivas/corretivas
Tratamentos transfronteiriços

4. Consequências da violação de dados

Integridade

A alteração/corrupção dos dados pode ter consequências para os titulares? (•) Sim ( ) Não

Indique quais:

A alteração/corrupção dos dados é passível de ser revertida para o estado original? (•) Sim ( ) Não

Os dados foram cifrados? ( ) Sim (•) Não

Grau de impacto nos utilizadores: Médio

Anterior | Próximo

Os dados indicados com * são de preenchimento obrigatório

NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS

Dados da entidade
Dados de contacto
Informação sobre a violação de dados
Consequências da violação de dados
Dados pessoais envolvidos
Titulares dos dados
Informação aos titulares
Medidas preventivas/corretivas
Tratamentos transfronteiriços

5. Dados pessoais envolvidos

Indique o(s) tipo(s) de dados pessoais envolvido(s)
(assinale, pelo menos, uma opção)

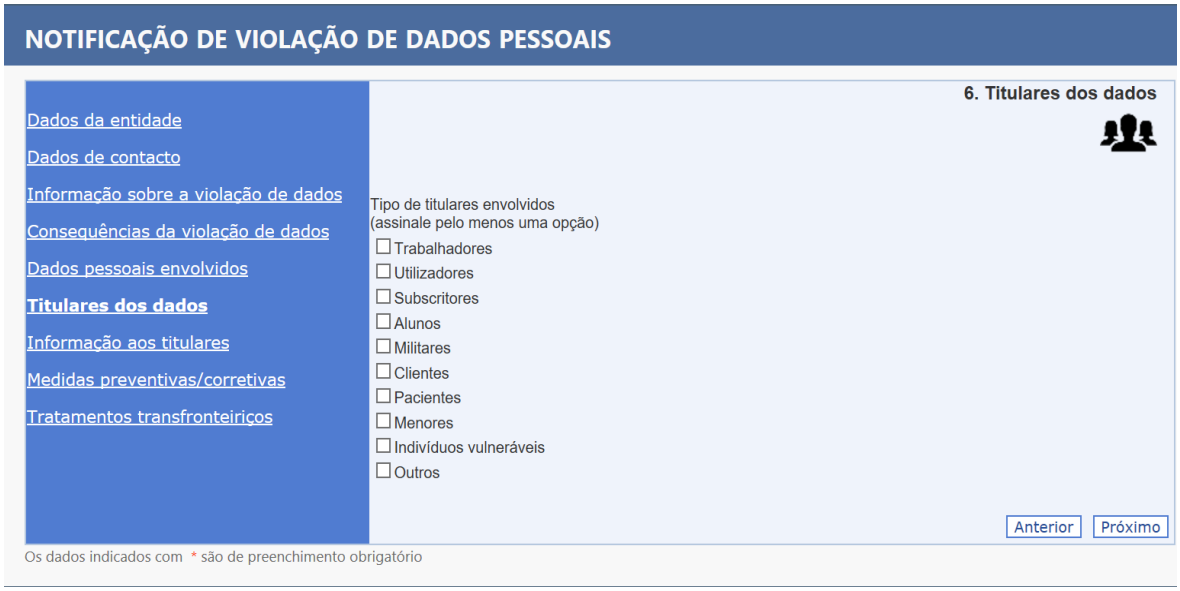
- [ ] Nome do titular
- [ ] Número de identificação
- [ ] Dados de morada
- [ ] Dados de contacto
- [ ] Dados de perfil
- [ ] Dados comportamentais
- [ ] Dados de saúde
- [ ] Dados genéticos
- [ ] Dados de localização
- [ ] Dados biométricos
- [ ] Dados relativos a crédito e solvabilidade
- [ ] Dados bancários
- [ ] Dados de recursos humanos
- [ ] Dados de faturação
- [ ] Dados relativos à atividade letiva
- [ ] Dados relativos a convicções filosóficas
- [ ] Dados relativos à filiação partidária
- [ ] Dados relativos às orientações sexuais
- [ ] Imagem
- [ ] Voz
- [ ] Outros

Foi possível determinar o número de titulares afetados? (•) Sim ( ) Não

Indique o número de titulares afetados:

Anterior | Próximo

Os dados indicados com * são de preenchimento obrigatório


NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS
Dados da entidade
Dados de contacto
Informação sobre a violação de dados
Consequências da violação de dados
Dados pessoais envolvidos
Titulares dos dados
Informação aos titulares
Medidas preventivas/corretivas
Tratamentos transfronteiriços
6. Titulares dos dados
Tipo de titulares envolvidos
(assinale pelo menos uma opção)
Trabalhadores
Utilizadores
Subscritores
Alunos
Militares
Clientes
Pacientes
Menores
Indivíduos vulneráveis
Outros
Anterior
Próximo
Os dados indicados com * são de preenchimento obrigatório


NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS
Dados da entidade
Dados de contacto
Informação sobre a violação de dados
Consequências da violação de dados
Dados pessoais envolvidos
Titulares dos dados
Informação aos titulares
Medidas preventivas/corretivas
Tratamentos transfronteiriços
7. Informação aos titulares
Os titulares foram informados da violação?
Sim
Não
00 00
Janeiro de 2019
S T Q Q S S D
Data da comunicação da violação
Forma de comunicação da violação
Número de titulares contactados
Mensagem que foi remetida aos titulares (max 500 carateres)
Anterior
Próximo
Os dados indicados com * são de preenchimento obrigatório

NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS

Dados da entidade
Dados de contacto
Informação sobre a violação de dados
Consequências da violação de dados
Dados pessoais envolvidos
Titulares dos dados
Informação aos titulares
Medidas preventivas/corretivas
Tratamentos transfronteiriços

8. Medidas preventivas/corretivas

Que mecanismos de segurança existiam ANTES da violação?

Que medidas foram aplicadas para corrigir/mitigar a violação?

Anterior | Próximo

Os dados indicados com * são de preenchimento obrigatório

NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS

Dados da entidade
Dados de contacto
Informação sobre a violação de dados
Consequências da violação de dados
Dados pessoais envolvidos
Titulares dos dados
Informação aos titulares
Medidas preventivas/corretivas
Tratamentos transfronteiriços

9.Tratamentos transfronteiriços

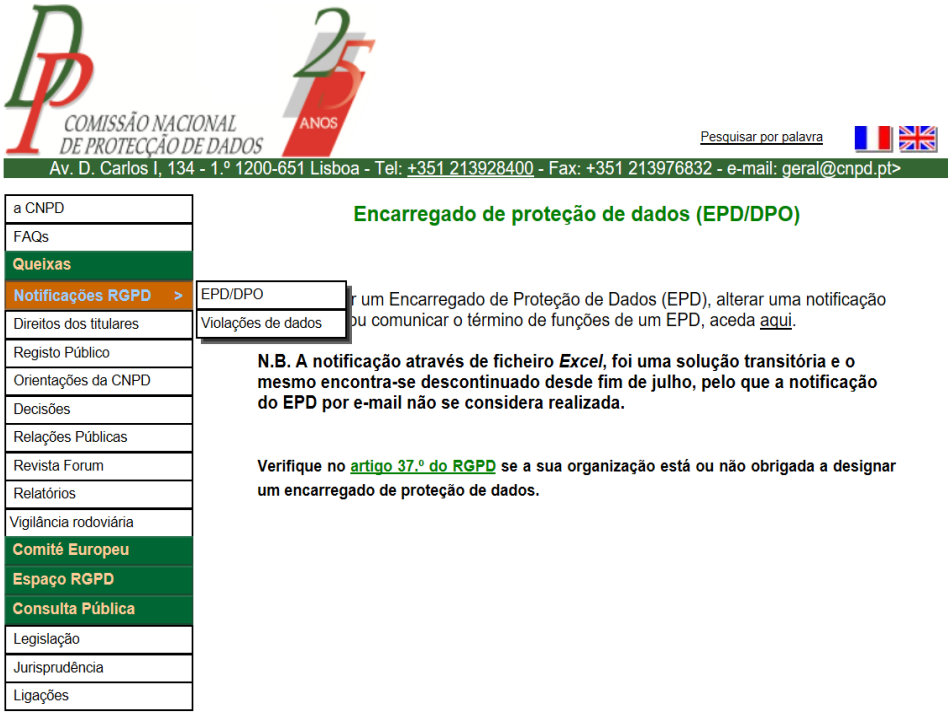
Existe tratamento de dados transfronteiriço?	○ Sim ◉ Não
A violação vai ser notificada diretamente a outra autoridade de controlo da UE?	○ Sim ◉ Não
A violação vai ser notificada diretamente a outra autoridade de controlo da fora da UE?	○ Sim ◉ Não
A violação será notificada a outros reguladores europeus, por razões legais?	○ Sim ◉ Não

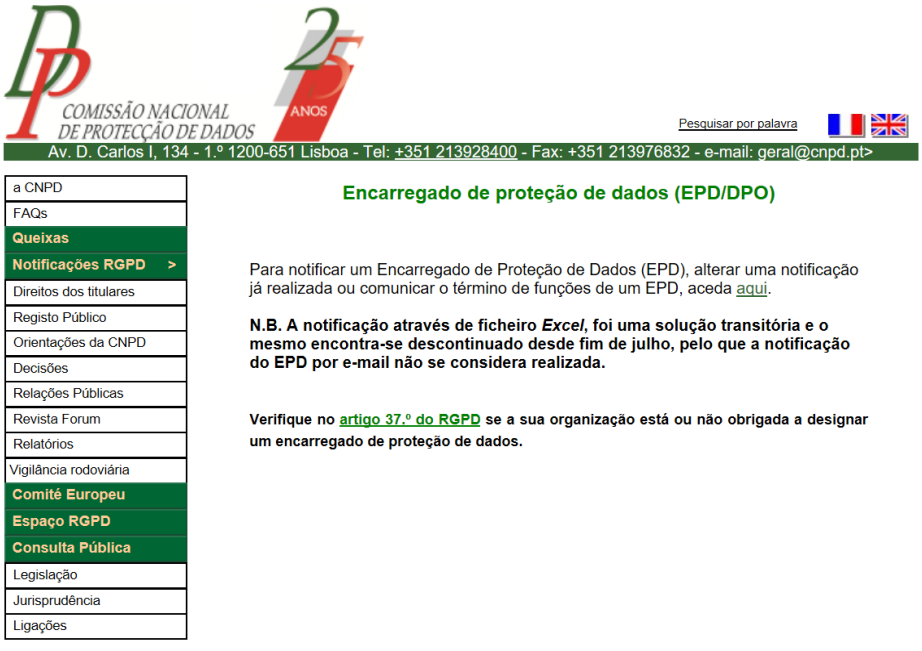
Anterior | Terminar

Os dados indicados com * são de preenchimento obrigatório

ANEXO 8: NOTIFICAÇÃO DA NOMEAÇÃO DO EDP

CNPD, disponível em http://www.cnpd.pt/bin/notifica_rgpd/epd_dpo.htm





Encarregado de Proteção de dados

Escolha a opção que melhor se aplica

Fazer notificação de Encarregado de Proteção de Dados

Alterar notificação (dados do EPD)

Alterar notificação (dados da entidade)

Comunicar término de Encarregado de Proteção de Dados

Notificação do Encarregado de Proteção de dados

Preâmbulo (Passo 1 de 4)

Antes de proceder ao preenchimento do formulário, tenha por favor em atenção o seguinte:

- Este formulário destina-se a entidades com estabelecimento no território nacional
- O EPD/DPO tem que ser uma pessoa singular (mesmo que pertença a uma empresa que forneça serviços de EPD)
- É necessário preencher um formulário por cada entidade, independentemente de serem do mesmo grupo ou partilharem o EPD

Informação quanto ao tratamento de dados pessoais
Os dados pessoais recolhidos através deste formulário são tratados pela CNPD para fins de gestão dos contactos dos encarregados de proteção de dados, na sequência do exigível pelo n.º 7 do artigo 37.º do Regulamento (UE) 2016/679 (RGPD). A prestação de informação prevista no artigo 14.º do RGPD será dada diretamente aos encarregados de proteção de dados enquanto titulares dos dados.

Atenção: Independentemente da possibilidade de submissão do formulário, só se consideram válidas as notificações que cumpram todas as regras.

☑ **Confirmo que li as condições de utilização do formulário de notificação de EPD/DPO**

Next

Voltar ao menu

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

Notificação do Encarregado de Proteção de dados

Dados da entidade (Passo 2 de 4)

Nome da entidade que notifica o encarregado de proteção de dados *

Designação comercial

NIF/NIPC da entidade *

Morada

País * Portugal

Via (Rua, Avenida, Praça, Largo, etc), n.º de porta e andar *

Código postal * -

Localidade *

Contactos

Telefone *

Email (será remetido um PDF da notificação e a referência da mesma para este endereço)

Qual o setor da entidade? * ◉ Setor público ○ Setor privado

Responsável pelo tratamento de dados? * ◉ Sim ○ Não

Subcontratante? * ◉ Sim ○ Não

Previous Next

Encarregado de Proteção de Dados (EPD / DPO) (Passo 3 de 4)

Nome Completo *

País em que se encontra * Portugal

Contactos *

Email *

Telefone * ◉ Fixo ○ Móvel

Portugal (+351) número

extensão (opcional)

Contactos alternativos

Email

Telefone ◉ Fixo ○ Móvel

Portugal (+351) número

extensão (opcional)

Relação de trabalho com a entidade * ◉ Quadro da organização ○ Quadro do grupo empresarial ○ Externo

A quem reporta o EPD dentro da organização

Administração / Departamento / Divisão *

Qual o regime de trabalho * ◉ tempo inteiro ○ tempo parcial

Exerce outras funções dentro da organização? * ○ Sim ◉ Não

Exerce funções de EPD para mais entidades? * ○ Sim ◉ Não

Data de início de funções (AAAA-MM-DD) *

Previous Next

Voltar ao menu

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

Notificação do Encarregado de Proteção de dados

Revisão dos dados e submissão (Passo 4 de 4)

Valide por favor a informação introduzida:

Dados da entidade

Nome da entidade que notifica	
Designação comercial	
NIF/NIPC da entidade	
Morada	
País	Portugal
Via (Rua, Avenida, Praça, Largo, etc), n.º de porta e andar	
Código postal	
Localidade	
Contactos	
Telefone	
Email	*não fornecido*
Setor da entidade	Setor público
Responsável pelo tratamento de dados?	Sim
Subcontratante?	Sim

Encarregado de Proteção de Dados (EPD / DPO)

Nome Completo	
País em que se encontra	
Contactos	
Email	
Telefone	
Contactos alternativos	
Email	*não fornecido*
Telefone	*não fornecido*
Relação de trabalho com a entidade	Quadro da organização
A quem reporta o EPD dentro da organização	
Administração / Departamento / Divisão	Administração
Qual o regime de trabalho	tempo inteiro
Exerce outras funções dentro da organização?	Não
Exerce funções de EPD para mais entidades?	Não
Data de início de funções (AAAA-MM-DD)	

Atenção: Não se considera cumprida a obrigação de notificação prevista no n.º 7 do Art.º 37 do RGPD se o formulário não estiver devidamente preenchido.

Nome da pessoa que preencheu a notificação *

☐ **Declaro que estou mandatado pela entidade notificante para proceder a esta notificação e que as informações prestadas correspondem à verdade.**

Escreva os caracteres que vê na imagem:

Previous Finish

Voltar ao menu

ANEXO 9: QUEIXA PERANTE A CNPD

CNPD, disponível em http://www.cnpd.pt/bin/queixas/queixas.htm