



Regulamento Europeu de Proteção de Dados (UE) 2016/679 + Lei Nacional 58/2019

Fernando Ferreira Batista



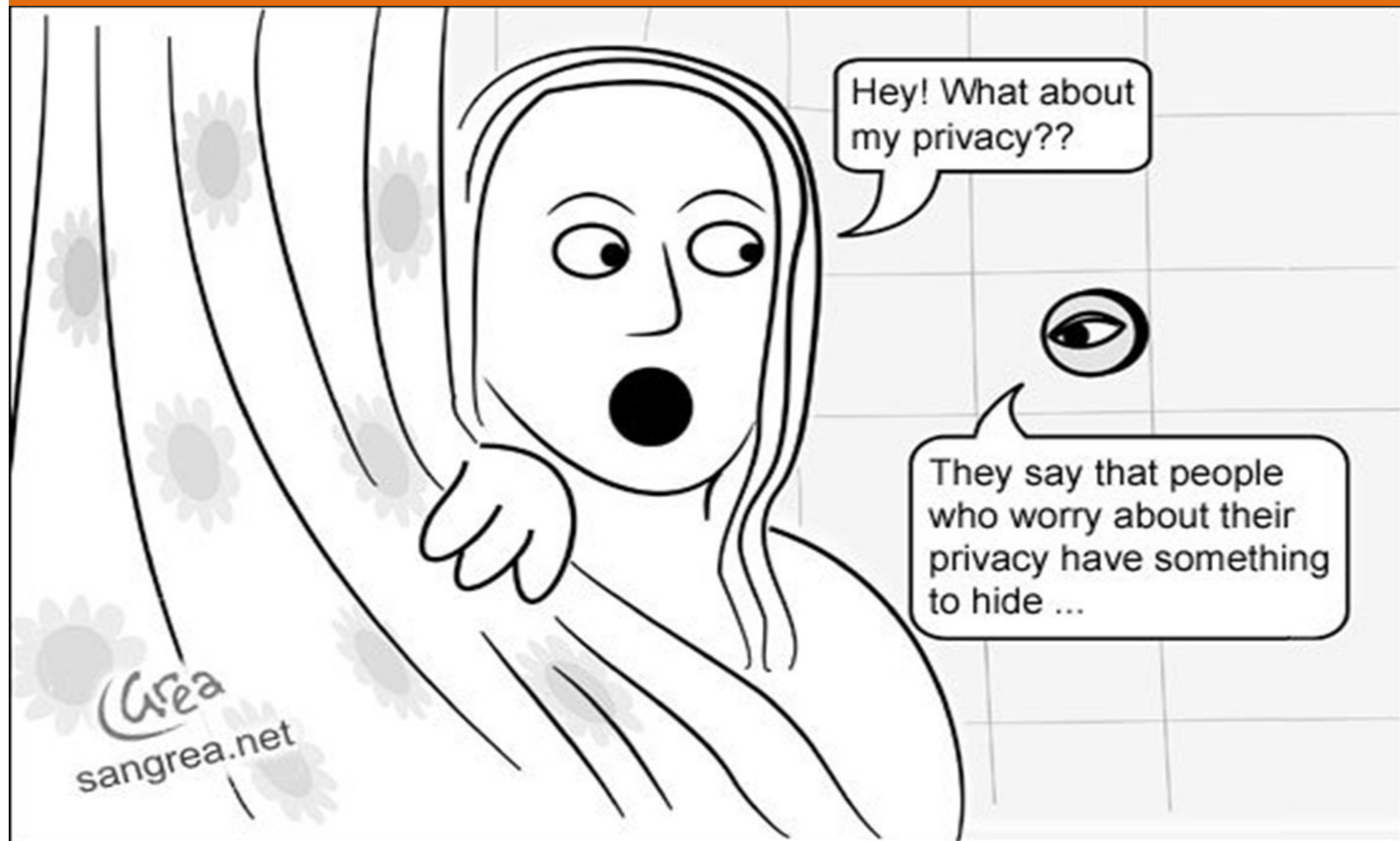
universidade
de aveiro

encarregado de proteção de dados | data protection officer



Contacto:

epd@ua.pt



Privacidade: valor intrínseco ou instrumental?

- Permite estabelecer laços com outras pessoas, impossíveis de estabelecer de outra forma?
- Essencial para a *autonomia* (Johnson)
- *Valores nucleares*? Embora em expressões diferentes, partilhados e presentes de alguma forma em culturas diversas
- Como expressão do valor nuclear da **segurança**, representa um *bem intrínseco* numa sociedade informatizada e ligada em rede
- Cidadãos têm o direito de ser *protegidos*, o que inclui a **proteção da privacidade e dos seus dados de carácter pessoal**



Privacidade e proteção de dados como direitos

Carta dos direitos fundamentais da UE, Artigo 8ª

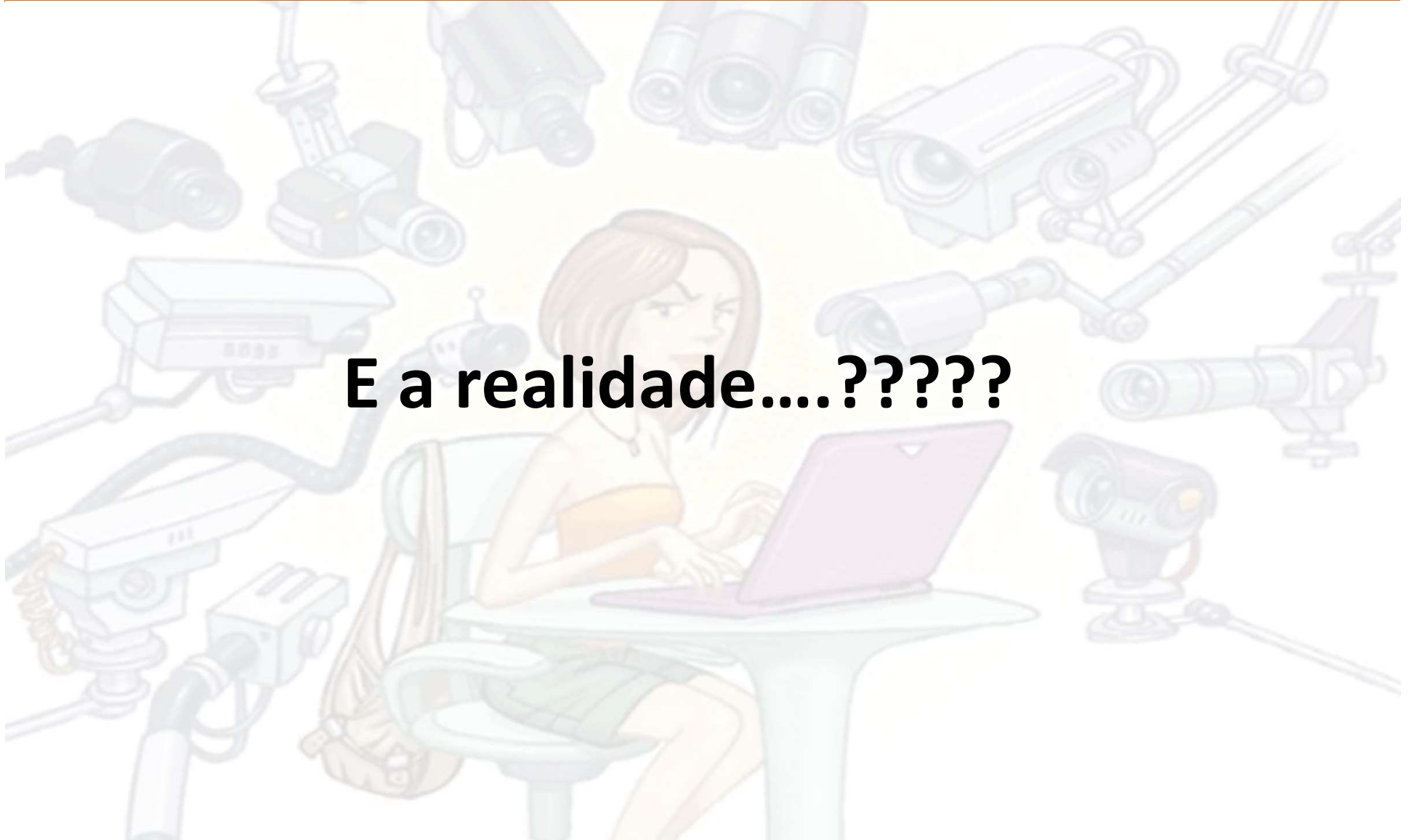
1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, **para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo** previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

Constituição da República Portuguesa, Artigo 35º

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a **finalidade** a que se destinam, nos termos previstos na lei.
2. A lei define o conceito de **dados pessoais**, bem como as condições aplicáveis ao seu tratamento (...), e garante a sua proteção, designadamente através de entidade administrativa independente.

Privacidade e proteção de dados como direitos

E a realidade....?????



Amazing mind reader reveals his 'gift'

de acordo com a realização:

- é um “clip” de uma encenação “vidente” para um suposto “novo programa de televisão”, realizada no centro de Bruxelas com pessoas aleatoriamente escolhidas para que lhes fosse “lida a mente”, mas tendo em vista, afinal, alertar utilizadores de serviços bancários online, numa campanha com o título Sejam Vigilantes!

PORTUGAL



EXCLUSIVOS

“Soube que tinha sido roubada quando o WiZink me ligou a comunicar que tinha uma dívida para pagar e me disse que tinha validado três transações através de autenticação forte feita na ‘app’ e que teria fornecido os meus dados pessoais”, disse ao ‘CM’ uma das clientes que foi burlada em cerca de cinco mil euros, garantindo que nunca fez nada disso



Contudo, a instituição garante que não houve falhas de segurança, assegurando que tem um sistema antifraude robusto e que todas as transações bancárias que estão em causa, “seguiram processos rigorosos de autenticação”.

O banco, adiantou ainda, é “totalmente alheio a atividades de ‘phishing’ no mercado português e não pode responsabilizar-se pela cedência de dados por parte de clientes a terceiros”.

Brexit: uma guerra descortês

“Brexit, the uncivil war” (excerto editado)



de acordo com a realização:

- é um filme baseado em eventos reais e entrevistas com pessoas que estiveram presentes;
- alguns aspetos de diálogo, personagens e cenas foram concebidos para efeitos de dramatização.

O último referendo para o Brexit foi realizado em 2016!

Brexit

uma guerra descortês

“Brexit, the uncivil war”



Dominic Cummings, diretor da campanha [Leave.EU](#) divulgou **mil milhões** de anúncios personalizados a eleitores através da [AggregateIQ](#) antes do referendo.

Arron Banks admitiu que o [Stay.EU](#) também contratou uma empresa especialista em personalização de anúncios para eleitores, a [Cambridge Analytica](#).

Tanto a [Cambridge Analytica](#) como a [AgregateIQ](#) estão ligadas ao empresário Robert Mercer*, que se tornou o maior doador da campanha de **Donald Trump**.

*R. Mercer, o mesmo que disse: **“Dinheiro é uma coisa, mas dados são poder!”**

(em 2018 a campanha “vote leave” foi considerada culpada de violar a lei eleitoral. O assunto ainda hoje está em aberto nos tribunais!)

A Proteção de dados na UE e em Portugal: RGPD

Regulamento (EU) 2016/79 do Parlamento Europeu e do Conselho – **Regulamento Geral de Proteção de Dados**

- Defender os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção de dados, 1.º/2; e
- **Promover a livre circulação dos dados pessoais, 1.º/3.**

A Proteção de dados na UE e em Portugal: RGPD

Regulamento (EU) 2016/79 do Parlamento Europeu e do Conselho – **Regulamento Geral de Proteção de Dados**

- Em vigor desde Maio de 2018
- Regulamento do Direito Europeu: não necessita transposição, aplica-se diretamente a todos os estados membros
- Deixa algumas cláusulas abertas, reguladas por legislação nacional – Lei 58/2019, de Execução do RGPD

A close-up photograph of a hand holding a pair of glasses. The hand and the glasses are outlined with a vibrant, multi-colored neon effect in shades of red, green, blue, and yellow, set against a dark, textured background. The text "O RGPD na sua essência ..." is overlaid in the center in a bold, yellow font.

O RGPD na sua essência ...

- 1. Introdução ao Regulamento (EU) 2016/679**
2. Direitos do titular dos dados
3. Obrigações dos responsáveis pelo tratamento
4. Legislação Nacional vs Regulamento
5. Impacto do novo regulamento na UA: resumo

Regulamento Europeu Proteção de Dados

Proteção de dados como direito fundamental

A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um **direito fundamental**.

- artigo 8.º, n.º 1, da **Carta dos Direitos Fundamentais da União Europeia** («Carta»)

- artigo 16.º, n.º 1, do **Tratado sobre o Funcionamento da União Europeia** (TFUE)

“Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito”

Regulamento Europeu Proteção de Dados

Introdução ao Regulamento (EU) 2016/679

Desde o dia 04 de Maio de 2016 que a União Europeia tem um novo quadro normativo para a Proteção de dados, estabelecendo as regras relativas à proteção das pessoas singulares no que diz respeito ao **tratamento de dados pessoais** e à **livre circulação desses dados**. O Regulamento* entrou em vigor no dia 25 de Maio de 2018.

O regulamento aplica-se:

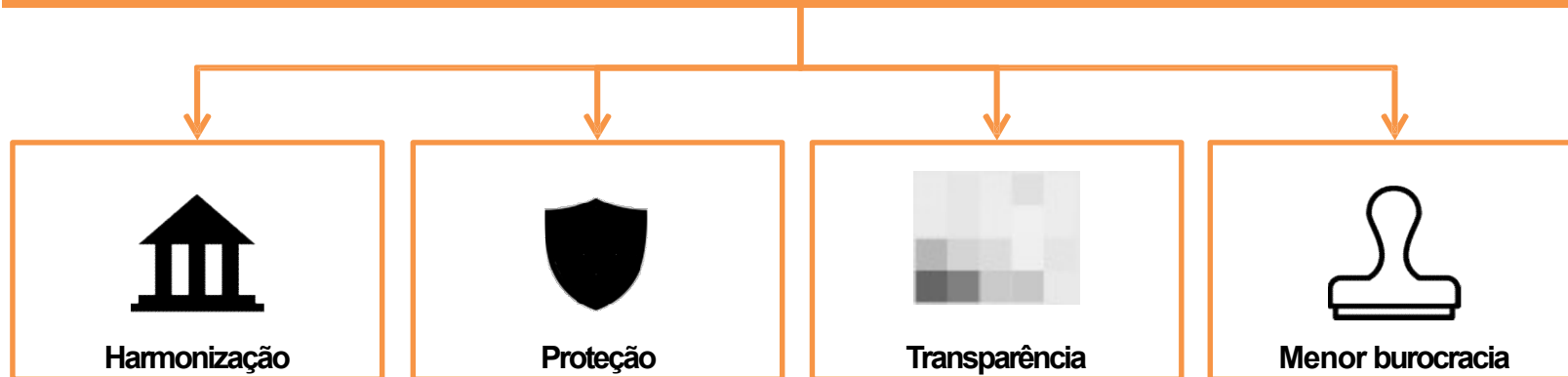
- em todo o território da **União Europeia**.
- a todas as empresas e entidades públicas que tratem dados pessoais.
- ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados.
- ao tratamento de dados, de residentes no território da União, efetuado por um responsável não estabelecido na União. -> ([edpb guidelines 3 2018 territorial scope pt.pdf](#))
- **entidades subcontratadas**.

* (deriva da anterior Diretiva Europeia 95/46 CE de 1995)

Regulamento Europeu Proteção de Dados

Introdução ao Regulamento (EU) 2016/679

REGULAMENTO GERAL PROTEÇÃO DE DADOS (UE) 2016/679



Regulamento Europeu Proteção de Dados

Definições

Para efeitos do presente regulamento, entende-se por:



**Responsável
pelo
tratamento**

Pessoa singular ou coletiva **que**, individualmente ou em conjunto com outras, **determina as finalidades e os meios de tratamento de dados pessoais.**



Subcontratante

Uma **pessoa singular ou coletiva**, a autoridade pública, agência ou outro organismo **que trate os dados pessoais por conta do responsável pelo tratamento destes**



**Art. 4º Regulamento
(UE) 2016/679**



**Violação de
dados pessoais**

Uma **violação que provoque**, de modo acidental ou ilícito **a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.**



**Autoridade de
Controlo**

Uma autoridade pública independente criada por um Estado-Membro.

CNPD em Portugal;
CNIL na França
ICO na Inglaterra – fora da UE, mas existe uma decisão de adequação;

Etc ...

Regulamento Europeu Proteção de Dados

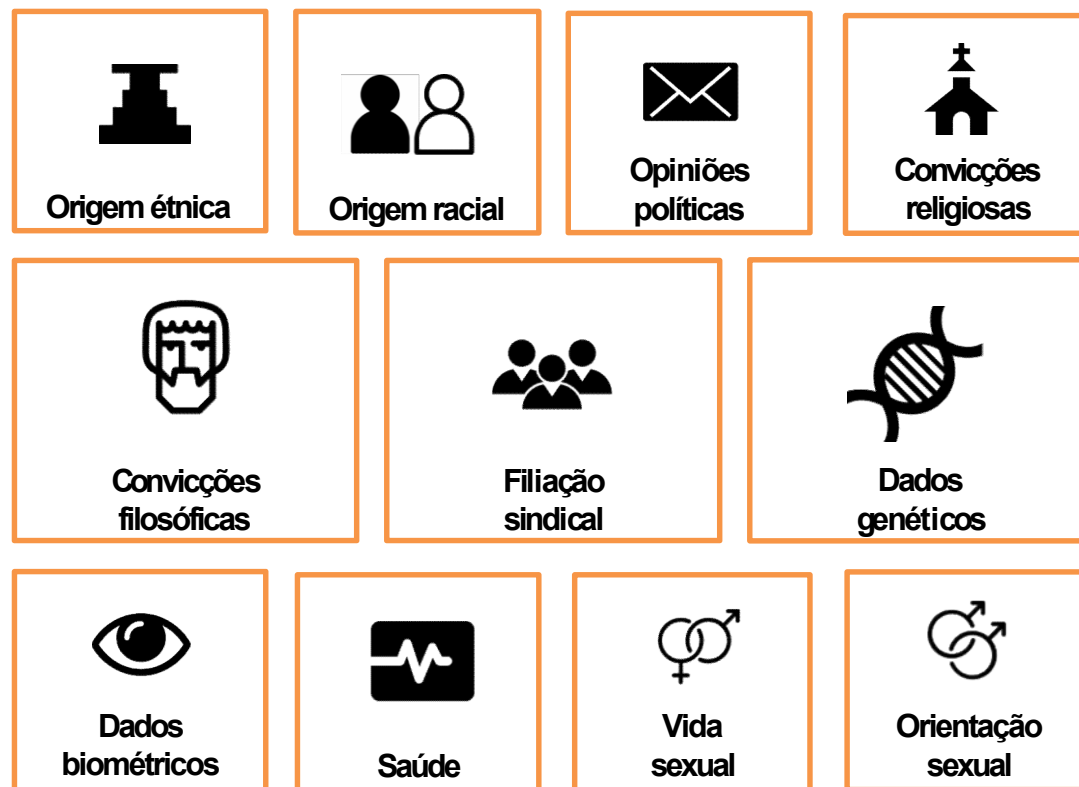
O que são dados pessoais?

Todos e quaisquer dados relativos a pessoas **singulares** identificadas ou identificáveis, direta ou indiretamente, como por exemplo o nome, morada, e-mail, idade, estado civil, dados de localização, genéticos, fisiológicos, económicos, culturais, sociais ou identificadores por via eletrónica.



Regulamento Europeu Proteção de Dados

Categorias Especiais de Dados Pessoais (sensíveis)



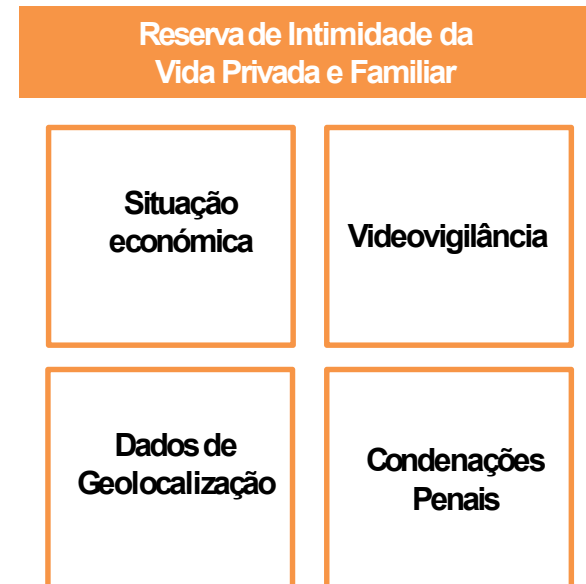
Art. 9º Regulamento (UE)2016/679



Constituição
Republica Portuguesa

Regulamento Europeu Proteção de Dados

Categorias Especiais de Dados Pessoais



Art. 9º Regulamento (UE)2016/679

proibição de tratamento dados especiais



**Constituição
Republica Portuguesa**

Regulamento Europeu Proteção de Dados

Princípios do Regulamento -> Categorias de dados especiais

Aproibição não se aplica quando se verificar um dos seguintes casos:

Se o titular dos dados tiver dado o seu consentimento explícito (exceto a lei proibir)

Cumprimento de obrigações/exercício de direitos específicos de RdT ou do titular

Proteger os interesses vitais do titular dos dados

Por um organismo sem fins lucrativos e com fins políticos, filosóficos, religiosos ou sindicais (aos seus elementos)

Adados pessoais que tenham sido manifestamente tornados públicos

Necessário à declaração, ao exercício ou à defesa de um direito

Necessário por motivos de interesse público

Necessário para efeitos de medicina preventiva ou do trabalho

Interesse público no domínio da saúde pública

Necessário para fins de arquivo de interesse público, estatístico, científico ou histórico

Regulamento Europeu Proteção de Dados

O que são dados pessoais?

- O retrato físico de uma pessoa (fotografia ou outro) e registos de voz ou vídeo **são dados pessoais**
- Assunção a partir de um retrato físico de características possivelmente categorizáveis como dados especiais (e.g. a etnia a partir da cor), implica de tais assunções estar-se perante tratamento de dados sensíveis?

➤ **Não**, salvo se houver tratamento de informação

E.g. Tratamento de fotografias por meios tecnológicos e que permitam a identificação inequívoca ou a autenticação de pessoa, corresponde a tratamento de dados biométricos, e bem assim dados sensíveis.

Regulamento Europeu Proteção de Dados

Anonimização

- Aplicação de técnicas de conversão de dados pessoais em dados anónimos, e.g. a supressão de atributos, a codificação, a generalização ou introdução de ruído.
- Se a finalidade de tratamento é possível com dados anonimizados, os dados têm que ser anonimizados.

Se *adequadamente* anonimizados, ficam fora do âmbito do RGPD!

- Se investigador recolher dados pessoais e só posteriormente os anonimizar, os dados brutos iniciais ainda são pessoais e devem ser tratados como tal.

e.g. dados de transcrição de entrevistas gravadas, ainda que subtraída de informações de identificação pessoal, não se traduz em anonimização, até que os dados brutos sejam destruídos.

Regulamento Europeu Proteção de Dados

Anonimização e re-identificação

- O RGPD aplica-se a dados pessoais; se os dados estão (adequadamente) anonimizados o quadro legal não se aplica.
- Mas... com a emergência do *big data* estudos mostram que pessoas podem ser re-identificadas a partir de dados anónimos e.g. usando apenas o código postal, data de nascimento e sexo, com 87% de precisão (Gumbus e Grodzinsky 2016)

<https://www.kdnuggets.com/2016/03/netflix-prize-analyzed-movie-ratings-recommender-systems.html>

- caso Netflix Prize Dataset

[HTTPS://www.kdnuggets.com/2016/03/netflix-prize-analyzed-movie-ratings-recommender-systems.html](https://www.kdnuggets.com/2016/03/netflix-prize-analyzed-movie-ratings-recommender-systems.html)

- ~500.000 registos anónimos de classificações de filmes
- Objetivo era fomentar investigação científica...
- ... e fomentar propostas de algoritmos capazes de prever o rating atribuído por utilizadores a filmes
- Dois investigadores - Arvind Narayanan e Vitaly Shmatikov – cruzaram informações com perfis públicos no IMBD (The Internet Movie Database)
- Apenas algumas preferências ($2 \leq \text{filmes} < 8$) mostraram ser suficientes para realizar re-identificação
- Outras informações pessoais sensíveis foram inferidas, tais como orientação política...



Regulamento Europeu Proteção de Dados

Pseudonimização

Tratamento de dados de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a **informações suplementares**, e desde que essas **informações suplementares** sejam mantidas separadamente e sujeitas a medidas para assegurar que os dados não possam ser atribuídos a uma pessoa singular:

- Projetos onde a anonimização compromete finalidades, sendo necessário manter um vínculo entre os sujeitos da investigação e os dados pessoais.
- **Não remove o carácter pessoal dos dados.**

Regulamento Europeu Proteção de Dados

Actividades de Tratamento

Operação ou um conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados:

Recolha

Adaptação ou Alteração

Registo

Recuperação

Organização

Consulta

Estruturação

Utilização

Conservação

Divulgação por transmissão

Comparação ou Interconexão

Apagamento ou Destruição

Regulamento Europeu Proteção de Dados

“Direito” ao consentimento

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

Condições aplicáveis ao consentimento



- Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.
- Há que verificar se a execução está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato
- O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado.
- Caso a criança tenha menos de 16 anos (em Portugal e por via da Lei 58/2019 a idade mínima foi estabelecida nos 13 anos), o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança.

Regulamento Europeu Proteção de Dados

“Direito” ao consentimento

Normalmente obtido sob a forma de declaração escrita, com referência à Informação ao Titular, e pode ser recolhido por meios eletrónicos, por exemplo:

(1) Consinto em que os meus dados pessoais sejam utilizados no âmbito do projeto de investigação *[identificar qual o projeto de investigação]* de acordo com a finalidade e demais informações que me foram disponibilizadas na Informação supra:

Sim ☐ Não ☐



Somente após a disponibilização da Informação ao Titular e obtida a sua manifestação positiva de consentimento podem os dados ser tratados (incluindo a recolha).

Consentimento nos planos legal e ético

Plano Legal: Consentimento do titular de dados (livre, específico, informado e explícito)

versus

Plano Ético: Consentimento informado de participantes na investigação.

O primeiro refere-se ao **consentimento para tratamento de dados pessoais** nos planos legais do RGPD.

O último ao **consentimento do sujeito de investigação para participar no projeto**, nos planos da ética e boas práticas na investigação científica.

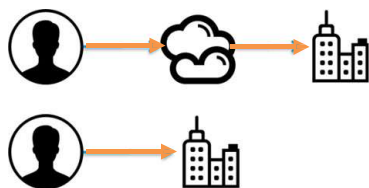
→ Necessário, mesmo com dados anonimizados, no plano ético.

→ **Não se referirá** ao tratamento de dados pessoais, mas apenas à participação no projeto e/ou a outras circunstâncias do projeto no plano ético.

1. Introdução ao Regulamento (EU) 2016/679
2. **Direitos do titular dos dados**
3. Obrigações dos responsáveis pelo tratamento
4. Legislação Nacional vs Regulamento
5. Impacto do novo regulamento na UA: resumo

Regulamento Europeu Proteção de Dados

Direitos do titular dos dados



Informação



Acesso



Retificação



Eliminação



Limitação



Portabilidade



Oposição

**Direitos
ARCO**



**Decisões
Automatizadas**

Regulamento Europeu Proteção de Dados

Direitos do titular dos dados

Informação ao Titular...

- A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
- Os contactos do encarregado da proteção de dados.
- As finalidades do tratamento .
- O fundamento jurídico para o tratamento
- Os destinatários ou categorias de destinatários dos dados pessoais.
- Transferências para países terceiros, existência de decisão da Comissão, ou garantias adequadas.
- Prazo de conservação dos dados pessoais (ou critérios).
- Direitos ARCO.
- Direito de retirar o consentimento.
- O direito de apresentar reclamação a uma autoridade de controlo .
- Existência de decisões automatizadas, lógica aplicada, importância e consequências.



**Momento da
recolha**



Informação ao Titular...



Informação ao Titular \neq Consentimento

Informação a facultar é
obrigatória
independentemente do
fundamento legal

**Momento da
recolha**



Regulamento Europeu Proteção de Dados

Direitos do titular dos dados



- Não ficar sujeito a nenhuma decisão com base no tratamento automatizado.
 - Incluindo a definição de perfis.
 - Que produza efeitos na esfera jurídica ou que o afecte significativamente.



Se a decisão...



- Necessária para elaboração/execução de **contrato** entre Responsável pelo tratamento e o interessado.
- Base **legal**.
- **Consentimento** explícito do interessado.

Não se basear em **categorias especiais** de dados

- Obter intervenção humana
- Expressar seu ponto de vista
- Impugnar a decisão

1. Introdução ao Regulamento (EU) 2016/679
2. Direitos do titular dos dados
3. **Obrigações dos responsáveis pelo tratamento**
4. Legislação Nacional vs Regulamento
5. Impacto do novo regulamento na UA: resumo

Regulamento Europeu Proteção de Dados

Regras e Responsabilidades

O **regulamento** vem definir um **conjunto de novas obrigações** em matérias de proteção de dados e privacidade. O responsável pelo tratamento deverá garantir:



Regras
e
Responsabilidades

- **licitude, lealdade e transparência:** **objeto de um tratamento lícito**, leal e transparente em relação ao titular dos dados;
- **limitação das finalidades:** **recolhidos para finalidades determinadas**, explícitas e legítimas e **não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades**;
- **minimização dos dados:** adequados, pertinentes e **limitados ao que é necessário** relativamente às finalidades ;
- **exatidão:** **exatos e atualizados** sempre que necessário . Os dados inexatos devem ser apagados ou retificados sem demora;
- **limitação da conservação:** **conservados** apenas **durante o período necessário** para as finalidades para as quais são tratados;
- **integridade e confidencialidade:** **tratados de uma forma que garanta a proteção** contra o tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental;

Adequação
Regl. Europeu



Regulamento Europeu Proteção de Dados

Princípios do Regulamento -> Licitude

O tratamento só será lícito se cumprir:



Consentimento do interessado



Execução de contrato/ medidas pré-contratuais



Cumprimento da obrigação legal do Responsável pelo Tratamento



Proteção de interesses vitais



Cumprimento de missão de interesse público / Exercício poderes públicos



Interesse legítimo do Responsável pelo Tratamento ou terceiros, se não prevalecem os direitos do interessado

Fundamento legal baseado em *Interesses legítimos* - Exemplo

Uma instituição de ensino superior (IES), pública ou privada, tem interesse em investigar os fatores socioeconómicos que influenciam a retenção de alunos e o seu percurso académico na instituição.

A IES tem bases de dados disponíveis fruto dos concursos de ingresso, incluindo diversas variáveis de descrição socioeconómica dos candidatos, bem como dados sobre o percurso académico dos alunos.

É do interesse legítimo da IES realizar a investigação, que tem aliás grande interesse público.

Exercício de ponderação: IES deve assegurar garantias (e.g. pseudonomização) e medidas de mitigação de risco, e demonstrar que os interesses, direitos e liberdades e garantias dos participantes não prevalecem sobre os interesses legítimos da IES.

Fundamento legal baseado em *Interesses legítimos* - Exemplo

- Em qualquer caso, o dever legal de informação ao titular mantém-se.
- O titular dos dados pode exercer o Direito de Oposição, mas o *opt-out* não é automático.
- Opcionalmente e como garantia adicional, a IES pode aplicar consentimento informado de participação.

Regulamento Europeu Proteção de Dados

...minimização dos dados

Proteção de Dados manda eliminar número de contribuinte do livro reclamações digital

minimização dos dados:

adequados, pertinentes e

limitados ao que é necessário
relativamente às finalidades ;

"O número de identificação fiscal só é necessário para efeitos de identificação dos cidadãos perante a administração fiscal", lembra a CNPD no seu parecer, da passada quarta-feira, dois dias antes de ter sido publicado o regime que criou a plataforma de queixas digital.

"Não estando aqui em causa uma operação sujeita a tributação, seja sob a forma de imposto seja sob a forma de taxa a pagar pelo reclamante, não se verifica nem a adequação, nem a necessidade de tal dado pessoal, já que os dados nome e o número do documento de identificação civil são mais do que suficientes para o efeito da identificação", defende a comissão.

Adequação
Regl. Europeu



Notícia de 16 de Julho 2017

Regulamento Europeu Proteção de Dados

...limitação da conservação

limitação da conservação:
conservados apenas **durante**
o período necessário para as
finalidades para as quais são
tratados;

.....

A CNPD recomenda a "reponderação" daquele prazo de conservação, "por forma a reduzir o mesmo ao período estritamente necessário", e lembra que tornar a informação anónima pode, depois de resolvido o problema que deu origem à reclamação, ser uma solução de conservação sem conhecer a identidade dos reclamantes.

Adequação
Regl. Europeu



Notícia de 16 de Julho 2017

Regulamento Europeu Proteção de Dados

...Segurança da Informação

.....

Segurança da Informação:

avaliar o nível de segurança adequado, 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.

Protecção de dados avisa: chave móvel digital tem inseguranças

Faltam regras mínimas de segurança na definição de palavras-passe e o sistema não garante que não seja possível que as mesmas sejam deduzíveis. As críticas são da CNPD, mas o Governo desvaloriza e garante que os níveis de segurança são os adequados.

Adequação
Regl. Europeu



Notícia de 13 de Fevereiro 2018

Regulamento Europeu Proteção de Dados

Registos das Atividades de Tratamento

Registos das atividades de tratamento

Cada **responsável pelo tratamento** e, sendo caso disso, o seu representante deverá conservar um registo de todas as atividades sob a sua responsabilidade:

- O nome e os contactos do responsável pelo tratamento;
- As finalidades do tratamento;
- A descrição das categorias de dados pessoais;
- As categorias de destinatários a quem os dados pessoais foram ou serão divulgados;
- Identificação dos países terceiros ou organizações internacionais para onde os dados serão enviados
- Identificação dos prazos para o apagamento das diferentes categorias de dados;
- Descrição geral das medidas técnicas e organizativas no domínio da segurança

Regulamento Europeu Proteção de Dados

Transferência Internacional de dados

Decisão de adequação

Decisão da Comissão que garante um **nível adequado** de proteção

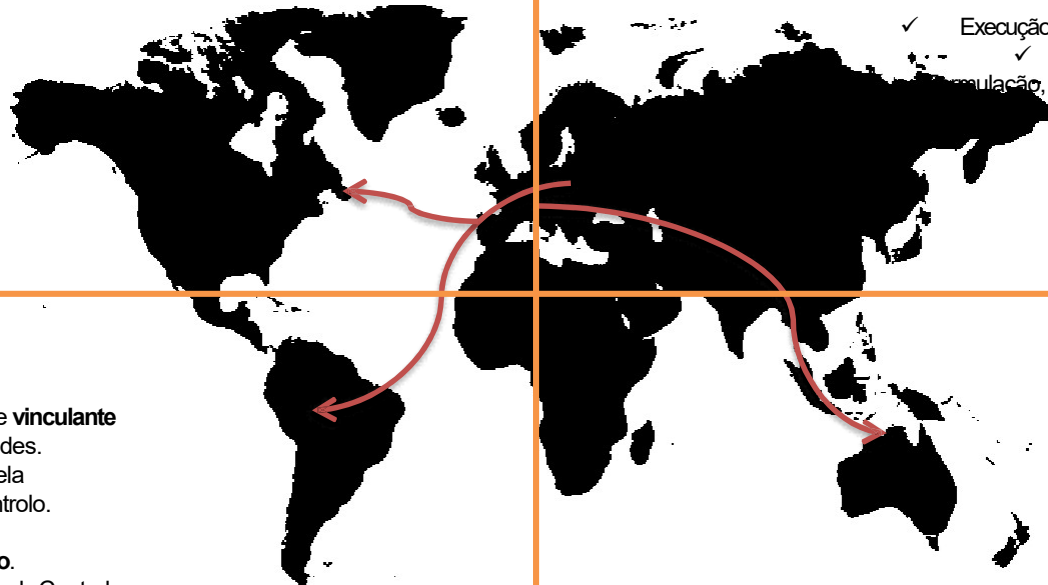
- ✓ Instrumento juridicamente **vinculante** e exigível entre as autoridades.
- ✓ **Cláusulas tipo** adotadas pela Comissão/Autoridade Controladora.
- ✓ Código de **conduta**.
- ✓ Mecanismo de **certificação**.
- ✓ **Autorização** da Autoridade de Controlo.

Garantias adequadas

Exceções

- ✓ Consentimento do afetado.
- ✓ Execução contrato/medidas pré-contractuais.
- ✓ Contrato no interesse do afetado.
- ✓ Exercício ou defesa de reclamações.
- ✓ Razões de interesse público.
- ✓ Proteção interesse vital.
- ✓ Desde registro público.

Normas Corp. Vinculantes



Tratamento de dados



1. Verificação **prévia** de **garantias** reunidas pelos Terceiros.
2. Formalização de **contratos**.
3. Autorização **prévia** para subcontratar.
4. Verificação das **garantias** ao longo da prestação.

Operação realizada por um **Terceiro**, por conta do Responsável pelo tratamento.

Parte da operação realizada por outro **Terceiro**, por conta do Responsável pelo tratamento.



Risco de que o Subcontratante seja considerado como Responsável pelo Tratamento.

Regulamento Europeu Proteção de Dados

Entidades subcontratadas -> Contrato



O contrato

Poderá basear-se, total ou parcialmente, em **cláusulas contratuais-tipo**

- **Estabelece** (geral):
 - Objeto.
 - Duração.
 - Natureza do tratamento.
 - Finalidade do tratamento.
 - Tipo de dados.
 - Categorias de interessados.
 - Obrigações e Direitos.

- **Em particular:**

Tratar os dados seguindo instruções **documentadas** do Responsável pelo tratamento

Compromisso de **confidencialidade** das pessoas autorizadas do Subcontratante

Adoção de **medidas** de **segurança** adequadas

Assistir o responsável pelo tratamento na resposta a solicitudes de direitos **ARCO**

Ajuda ao Responsável pelo tratamento no cumprimento de medidas de segurança, **falhas** de segurança e **PIAs**

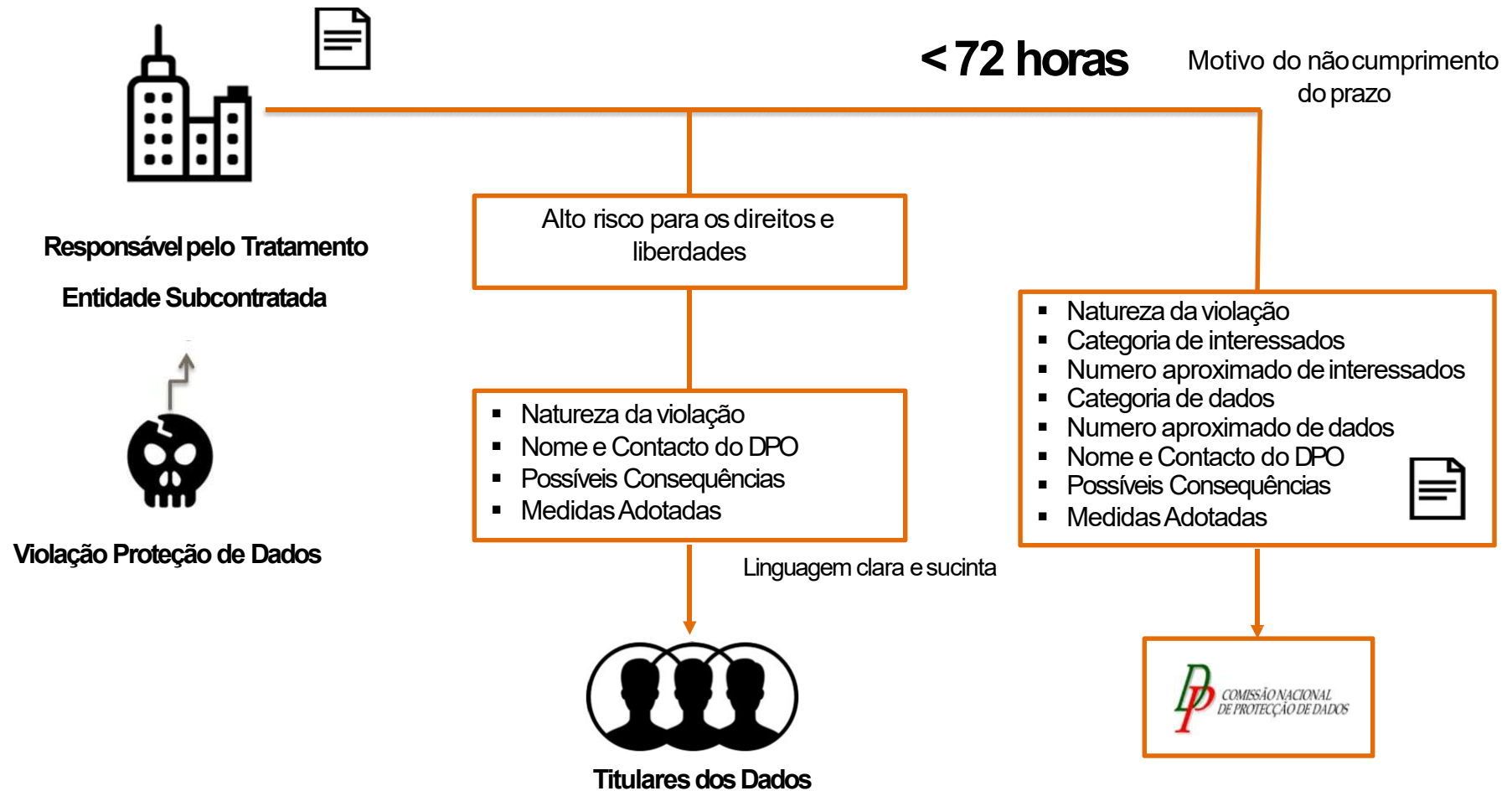
Suprimir/devolver os dados no termo da prestação

Disponibilizar ao responsável pelo tratamento **as evidências** de cumprimento da suas obrigações

Código de conduta

Regulamento Europeu Proteção de Dados

Comunicação de Incidentes – Art. 33º



Nem todas as violações devem ser reportadas à autoridade de controlo

Todas as violações devem ser devidamente documentadas

Regulamento Europeu Proteção de Dados

Privacy By Design and Privacy By Default

- ❑ A adopção de medidas que respeitem os princípios da proteção de dados desde a concepção (*privacy by design*) e da protecção de dados por defeito (*privacy by default*).
- ❑ O responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a concepção e da proteção de dados por defeito, podendo tais medidas incluir a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais, encriptação, etc.

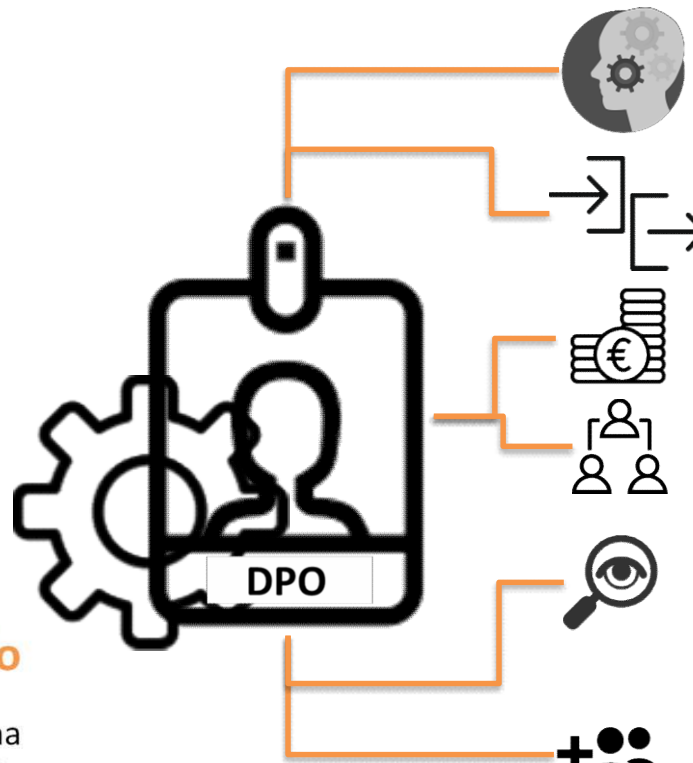
Regulamento Europeu Proteção de Dados

Encarregado Proteção de Dados



Art. 39º Regulamento (UE) 2016/679

Data Privacy
Officer (DPO)



conhecimento especializado no domínio do **direito** e das práticas de **Proteção de dados**

interno | **externo**

dotação de **recursos suficientes** para o adequado desempenho da função

dependência hierárquica ao **mais alto nível**

absoluta independência no desempenho das suas funções

Aplicável a grupos empresariais
| organismos públicos

função

Informa e aconselha
Controla a conformidade
Presta aconselhamento
Coopera
Ponto de contacto

Regulamento Europeu Proteção de Dados

Avaliação de Impacto sobre a Privacidade (PIA)



Art. 35 Regulamento (UE) 2016/679

Avaliação de
Impacto sobre a
Proteção de dados
(PIA)



- ❑ A **avaliação de impacto sobre a proteção de dados** deve ser realizado quando o tratamento de dados "...for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares".
- ❑ A realização da avaliação é obrigatória nomeadamente em caso de:
 - Avaliação sistemática e completa dos aspetos pessoais, baseada no tratamento automatizado e na definição de perfis;
 - Operações de tratamento em grande escala de categorias especiais de dados;
 - Controlo sistemático de zonas acessíveis ao público em grande escala;
- ❑ As avaliações devem ser revistas a cada três anos, exceto nas situações em que o tratamento seja objeto de alterações.
- ❑ Apenas estão sujeitos à obrigação da realização de um PIA os tratamentos de dados iniciados após 25 de Maio de 2018. Os tratamentos iniciados em data anterior, será obrigatório caso sejam inseridas alterações ao tratamento dos dados após a aplicação do RGPD.

Regulamento Europeu Proteção de Dados

Limitações

Artigo 23.º do RGPD

Limitações

O direito da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento ou o seu subcontratante pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 12.º a 22.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar, designadamente:

- ☐ A segurança do Estado;
- ☐ A defesa;
- ☐ A segurança pública;
- ☐ A prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública; ...
- ☐ A defesa do titular dos dados ou dos direitos e liberdades de outrem; ...

1. Introdução ao Regulamento (EU) 2016/679
2. Direitos do titular dos dados
3. Obrigações dos responsáveis pelo tratamento
4. **Legislação Nacional vs Regulamento**
5. Impacto do novo regulamento na UA: resumo

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – Investigação/Saúde

DELIBERAÇÃO Nº 1704 /2015 (CNPd)

Aplicável aos tratamentos de dados pessoais efetuados no âmbito de investigação clínica

Lei da Investigação Clínica

“os estudos clínicos devem ser realizados no estrito respeito pelo princípio da dignidade da pessoa humana e dos seus direitos fundamentais, reforçando-se que os direitos dos participantes prevalecem sobre os interesses da ciência e da sociedade . . .na realização da investigação devem ser tomadas todas as precauções no sentido do respeito da privacidade e dos direitos de personalidade”

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – Investigação/Saúde

Legislação

- ☐ A Convenção 108.º do Conselho da Europa, de 28 de janeiro de 1981;
- ☐ A Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro;
- ☐ O n.º 1 do artigo 26.º, o artigo 35.º e o n.º 4 do artigo 73.º da Constituição da República Portuguesa (doravante, CRP);
- ☐ **A Lei n.º 58/2019, de 08 de Agosto;**
- ☐ Lei n.º 21/2014, de 16 de abril, alterada pela Lei n.º 73/2015, de 27 de julho (LIC – Lei Investigação Clínica);
- ☐ A Lei n.º 12/2005, de 26 de janeiro, relativa à Informação genética pessoal e informação de saúde;
- ☐ A Lei n.º 48/90, de 24 de agosto (Lei de Bases da Saúde);
- ☐ A Lei n.º 125/99, de 20 de abril, relativa ao Regime Jurídico das Instituições de Investigação Científica;
- ☐ O Código Deontológico da Ordem dos Médicos;
- ☐ A Declaração de Helsínquia da Associação Médica Mundial;

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – Investigação/Saúde

Deliberação N° 1704 /2015 (CNPd)

- ☐ Os investigadores, na avaliação prévia, devem ponderar os riscos previsíveis não apenas para a vida ou integridade física das pessoas, mas também para a privacidade e para a proteção dos dados pessoais.


- ☐ **A lei de investigação clínica, distingue as seguintes formas de investigação:**
 - ensaios clínicos;
 - estudos clínicos sem intervenção;
 - estudos clínicos com intervenção;
 - estudos clínicos de dispositivo médico;
 - estudos clínicos de produtos cosméticos e de higiene corporal.

- ☐ Os tratamentos de dados pessoais com a finalidade de realizar investigação clínica incidem necessariamente sobre dados sensíveis, designadamente dados pessoais relativos à saúde, relativos à vida privada e dados genéticos.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – Investigação/Saúde

Princípios de Protecção de Dados

- Adequados, pertinentes e não excessivos relativamente à finalidade da recolha;
 - ❑ a adequação, pertinência, bem como a necessidade e não excessividade dos dados são aferidas pela avaliação das categorias de dados recolhidos em função da finalidade do estudo de investigação.
- Tratados de forma lícita e com respeito pelos princípios da boa-fé;
- Tratados e conservados apenas durante o tempo necessário ao cumprimento da finalidade, não podendo os dados ser utilizados para outras finalidades;
- Princípios da transparência  Prestação do direito de informação;
- Obtenção do consentimento

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – Investigação/Saúde

Princípio da proporcionalidade

- ❑ Terá de verificar se o tratamento se revela como o meio adequado para o fim visado.
- ❑ Salvaguardando, por um lado,
 - ✓ o direito à proteção dos dados pessoais e outros direitos fundamentais dos titulares e,
 - ✓ por outro, o interesse do responsável, o qual se consubstancia também num direito que não pode ser comprimido para além do necessário, devendo ser atingido um justo equilíbrio que não afecte o conteúdo essencial dos direitos em presença.
- Esta ponderação exige:
 - ✓ o direito à privacidade e à proteção dos dados pessoais de todas as pessoas;
 - ✓ *a investigação para a saúde, devendo procurar-se envolver os serviços, os profissionais e a comunidade*

Exceções

Há casos em que a **condição de legitimidade para tratamento de dados pessoais de saúde— para fins de investigação científica se preenche**, na ausência de consentimento livre, específico, informado e expresso, **com a verificação rigorosa da importância do concreto e efectivo interesse público da investigação**, que conduza a outras condições de legitimidade

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – Investigação/Saúde

Analisar as características gerais dos estudos:

1. designadamente se os mesmos são prospectivos ou retrospectivos;
 2. se obrigam à recolha de dados identificados;
 3. se o estudo pode ser efectuado com dados identificáveis ou, ainda, se poderá decorrer com dados não identificáveis.
 4. sempre que um estudo possa ser efectuado sem o tratamento de dados pessoais, deve ser essa a opção do investigador.
 5. Sempre que o estudo puder ser feito com dados anonimizados, em que não se identifica nem permite identificar os titulares dos dados, deve ser esta a opção tomada para a investigação.
 6. No caso de não se poder efectuar o estudo com dados anónimos, deve privilegiar-se a utilização de dados codificados, ainda que estes possam ser, mediante a aplicação de uma chave de descodificação, convertidos em dados pessoais.
- Só em último caso e perante a estrita necessidade se admite a utilização de dados pessoais de saúde para efeitos de investigação científica. A entidade responsável deve justificar a necessidade de efectuar o estudo de forma identificada ou identificável.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – Investigação/Saúde

Recolha dos dados

Os dados podem ser recolhidos **directamente do titular**, **por resposta** directa **a inquéritos/questionários**, que lhe serão disponibilizados pelo investigador ou por profissionais de saúde que colaboram no estudo.

No caso da recolha de amostras, devem ser adoptadas técnicas pouco intrusivas e meios que preservem a dignidade da pessoa humana e a integridade física e moral das pessoas.

Podem, também, **no âmbito de estudos retrospectivos**, **ser recolhidos indirectamente pelo médico assistente**, que os transmitirá ao investigador. Nesta situação poderá não haver necessidade de identificar o dados, **situação em que as informações deverão ser disponibilizadas de forma anónima.**

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – Investigação/Saúde

Condições de legitimidade

- ❑ Tendo a natureza de sensíveis os dados abrangidos pelos estudos em causa, por serem dados de saúde, dados genéticos, dados da vida privada e/ou dados relativos à raça ou etnia, aplica-se o princípio, quer constitucional quer legal, da proibição do seu tratamento.
- ❑ Existem algumas exceções expressamente previstas na lei, sendo permitido o seu tratamento quando se verifiquem as condições de legitimidade:
 - lei (formal) habilitante;
 - consentimento livre, específico, informado, expresso do titular e escrito;
 - autorização da CNPD, em virtude de interesse público importante e desde que o tratamento seja indispensável ao exercício de atribuições legais ou estatutárias do seu responsável, desde que sejam asseguradas garantias de não discriminação.

As unidades do sistema de saúde só podem utilizar os dados pessoais de saúde para fins de investigação científica nos termos constantes da autorização escrita do titular.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – Investigação/Saúde

Condições de legitimidade

- ❑ Quando se tratar de investigação científica retrospectiva de informação de saúde extraída de outros dados pessoais que não as amostras (fichas clínicas, por exemplo), no caso de ausência de consentimento, a autorização para o tratamento de dados pessoais deve revestir-se de uma ponderação minuciosa.
 - Em primeiro lugar, devem estar cabalmente circunstanciadas e demonstradas as “*situações especiais*”.
 - deve ser demonstrada de forma inequívoca a existência e a importância do interesse público do estudo ou da investigação em causa;

- ❑ **A importância do interesse público da investigação** a efectuar com o tratamento de dados pessoais de saúde **sem o consentimento dos titulares deve ser declarada pela entidade** independente **que acompanha e avalia cientificamente estas instituições**, quer internamente, quer pelo Ministério responsável pela tutela das áreas da Ciência e da Tecnologia

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – Investigação/Saúde

Condições de legitimidade

- ❑ **Utilização de dados pessoais de saúde**, sem consentimento dos titulares, para fins de investigação científica, **efetuados no âmbito de teses académicas**.
 - em princípio **não deve ser admitida a utilização desses dados sem o consentimento dos titulares**.
 - os tratamentos de dados pessoais para fins de investigação científica sem consentimento dos titulares, além de ser uma realidade absolutamente excepcional dificilmente compaginável com finalidades individuais ou privadas, **deve revestir-se de garantias de capacidade técnica, de dotação de meios, de suficiência organizacional, de adopção de medidas de segurança** que muito raramente se verificam numa pessoa individual.
 - Tal não obsta a que os **Comités de Ética das Universidades**, acompanhados pelos Comités de Ética Hospitalares, motivando e fundamentando a **importância do interesse público na investigação, se responsabilizem pelo acompanhamento e avaliação dos estudos em causa, assumindo a responsabilidade efectiva pela dotação de meios adequados à pessoa singular em causa.**

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – Investigação/Saúde

Responsável do Tratamento

- ☐ O responsável pelo tratamento é a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais.
- ☐ A LIC considera responsáveis pela realização do estudo clínico o promotor, o investigador e o monitor. No entanto, a responsabilidade pela realização do estudo não é necessariamente coincidente com a responsabilidade pelo tratamento de dados pessoais no contexto do estudo.
- ☐ **O promotor é o responsável pela conceção e realização do estudo, competindo-lhe assegurar que o estudo é realizado em conformidade com as exigências legais e regulamentares aplicáveis.**
- ☐ **O promotor é a entidade que determina a finalidade e os meios do tratamento de dados pessoais.** O promotor é o responsável pelo tratamento de dados pessoais, a quem incumbe cumprir as obrigações decorrentes da LPDP.
- ☐ Pela própria natureza da investigação clínica o investigador pratica atos materiais típicos do responsável, como seja a obrigação de informar, a obrigação de obter consentimento prévio, dos participantes titulares dos dados, a obrigação de assegurar o processamento dos dados pessoais e garantir a confidencialidade do estudo.

NOTA: Por vezes existem as situações em que pode haver coincidência entre o promotor e o investigador, podendo suceder em estudos clínicos efetuados para obtenção de graus académicos.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – Investigação/Saúde

Subcontratantes

- ☐ O investigador é um subcontratante do promotor que se responsabiliza pela realização do estudo no centro de estudo clínico, cabendo-lhe, em representação e em nome do promotor, cumprir o previsto no artigo 10.º da LIC
- ☐ Entre o promotor e o subcontratante deve haver um contrato, ou outro ato jurídico, que vincule o subcontratante ao responsável pelo tratamento.
- ☐ Nesse contrato ou ato jurídico, o qual revestirá a forma escrita, com valor probatório legalmente reconhecido, deve constar que o subcontratante apenas atua mediante instruções do responsável pelo tratamento.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – Investigação/Saúde

Medidas de Segurança

- ☐ O sistema deve garantir uma separação lógica entre os dados referentes à saúde e os restantes dados pessoais, de natureza administrativa;
- ☐ permitir o acesso à informação de acordo com os diferentes perfis de utilizador, com níveis de acesso diferenciados e privilégios de manuseamento da informação distintos
- ☐ adoptadas medidas de segurança que impeçam o acesso à informação a pessoas não autorizadas.
- ☐ sempre que haja circulação da informação de saúde em rede, a transmissão dos dados deve ser cifrada
- ☐ manter um registo de acesso à informação sensível para controlo das operações e para a realização auditorias internas e externas.

Independentemente das medidas de segurança adoptadas pela entidade responsável pelo tratamento, é a esta que cabe assegurar o resultado da efectiva segurança da informação e dos dados tratados.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento

Caso especial: Dados pessoais tratados por alunos

Dados pessoais tratados por alunos

Os alunos usam/tratam dados pessoais essencialmente por três razões:

- 1 . **Por razões pessoais**, por exemplo para comunicar com a família e amigos com a sua conta email institucional;
2. **Para prosseguir estudos**, por exemplo fazendo pesquisas e escrevendo um ensaio, relatório ou tese;
3. Em processos de investigação, **enquanto membros de uma equipa de investigação** estabelecida na Universidade.

O tratamento de dados pessoais existe em variadas formas, tais como a manutenção de um livro de registo de endereços, uma base de dados com informação variada, dossiers ou listas em papel também com informação pessoal, ou apenas um mero registo de uma conta de email pessoal, entre outros.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento

Caso especial: Dados pessoais tratados por alunos

Dados pessoais tratados por alunos

cenário Um

Um aluno processa dados pessoais das suas relações e vida pessoal, por exemplo escrevendo um e-mail (usando a conta de email que a universidade lhe forneceu) para a família sobre o recente aniversário de um colega.

A Universidade não é o responsável pelo tratamento de dados de dados pessoais tratados pelo aluno no curso da sua vida pessoal, pois a Universidade não determina a finalidade do tratamento. O facto do aluno poder usar a sua conta de mail institucional não torna a Universidade responsável pelo tratamento de dados pessoais para esse efeito. Nesta situação o responsável pelo tratamento de dados é o próprio aluno, que responde pessoalmente, podendo sustentar a sua atuação nas relações também pessoais, não abrangidas pelo RGPD.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento

Caso especial: Dados pessoais tratados por alunos

Dados pessoais tratados por alunos

cenário dois

Um aluno processa dados pessoais tendo em vista a prossecução dos seus estudos, por exemplo num trabalho de dissertação incluído no curso, ainda que orientado por um supervisor, que terá mesmo sugerido a realização de entrevistas para a sua concretização.

Nestas circunstâncias a universidade não é o responsável/controlador de dados. Os alunos frequentam a universidade tendo em vista benefícios pessoais, materializados no conhecimento e qualificações obtidos, não sendo funcionários ou agentes da universidade, nem podendo atuar em nome desta. O aluno decide, ainda que aconselhado, o trabalho que vai fazer e a forma como o vai realizar, devendo tomar essas decisões por si próprio, demonstrando as suas capacidades em ordem à obtenção do grau pretendido.

O eventual facto do aluno ter sido recomendado para realizar entrevistas pelo seu supervisor não torna a universidade responsável pelo tratamento de dados pessoais dos entrevistados. **O papel do supervisor é ensinar e aconselhar o aluno, aqui se incluindo conselhos sobre proteção de dados pessoais, como parte da sua formação em boas prática de pesquisa**, mas é o aluno, em seu benefício, quem realiza as entrevistas.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento

Caso especial: Dados pessoais tratados por alunos

Dados pessoais tratados por alunos

cenário três

Um estudante submete à Universidade, para avaliação, um trabalho (ex. um ensaio, relatório ou tese) que envolve – inclui- dados pessoais.

Nessa situação, a Universidade, por via de um ou mais dos seus elementos, é responsável pelo tratamento de dados, relativamente aos dados pessoais contidos no trabalho, a partir do momento em que o mesmo é entregue.

- Mesmo que o tratamento de dados envolvido possa ser apenas materializado na leitura do documento com o único propósito de o avaliar, sendo essa uma das funções da Universidade.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento

Caso especial: Dados pessoais tratados por alunos

Dados pessoais tratados por alunos

cenário quatro

Um aluno/bolseiro processa dados pessoais no âmbito de um projeto em que trabalha, incluído numa equipa de projeto da Universidade.

Nestas circunstâncias a Universidade é responsável/controlador de dados para dados pessoais tratados por esse aluno. O aluno/bolseiro processa os dados pessoais para os fins previstos no projeto, sendo mandatado/decidido pela Universidade (através de um ou vários seus elementos) a forma como tais dados serão tratados, e não pelo aluno. Os resultados do processamento pertencem à Universidade e não ao aluno, portanto a Universidade é o responsável/controlador de dados e o aluno atua como um agente da Universidade. Este é por exemplo o caso de um aluno financiado por um projeto de investigação. Normalmente apenas alunos de pós-graduação se encontram neste tipo de cenário.

No entanto nem todas as Investigações/pesquisas realizadas por alunos de pós-graduação são da responsabilidade da universidade.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – área Administrativa

- ❑ CRP– artigos 35.º e 268.º, n.º 2
- ❑ **Lei nº 58/2019, de 08 de Agosto**
- ❑ Lei n.º 26/2016, de 22 de Agosto (LADA- Lei de Acesso aos Documentos Administrativos)

Privacidade e proteção de dados pessoais na relação de trabalho – atual quadro legislativo:

- ❑ arts. 18.º, 26.º, 32.º, n.º 8, 34.º, 35.º, 40.º da CRP
- ❑ arts. 14.º a 22.º do CT
- ❑ arts. 23.º a 29.º do CT
- ❑ art. 170.º do CT
- ❑ arts. 70.º a 81.º do CC
- ❑ art. 13.º da Lei n.º 12/2005, de 26 de Janeiro sobre Informação genética pessoal e informação de saúde
- ❑ Lei n.º 34/2013, de 16 de Maio - Estabelece o regime do exercício da atividade de segurança privada–sobretudo art. 31.º
- ❑ Portaria n.º 273/2013, de 20 de Agosto
- ❑ Recomendação CM/Rec(2015)5, de 1 de Abril, do Comité de Ministros do Conselho da Europa sobre o tratamento de dados de natureza pessoal no contexto do emprego

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – área Administrativa

Artigo 35º CRP

Utilização da informática

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, 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 proteção, designadamente através de **entidade administrativa independente**

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – área Administrativa

Artigo 17.º LADA

Princípio da administração aberta

- 1- **Todas as pessoas têm o direito de acesso aos arquivos e registos administrativos**, mesmo quando nenhum procedimento que lhes diga diretamente respeito esteja em curso, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal, ao sigilo fiscal e à privacidade das pessoas.
- 2 - **O acesso aos arquivos e registos administrativos é regulado por lei.**

Artigo 268º CRP

Direitos e garantias dos administrados

- 2 - **Os cidadãos têm também o direito de acesso aos arquivos e registos administrativos**, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal e à intimidade das pessoas.

Nr. 1 do Artigo 1.º Lei 58/2019

Âmbito de aplicação

A presente Lei aplica-se aos tratamentos de dados pessoais realizados no território Nacional, independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante, mesmo que o tratamento de dados pessoais seja efetuado em cumprimento de obrigações legais ou no âmbito da prossecução de missões de interesse público, aplicando-se todas as exclusões previstas no Artº 2º do RGPD.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – área Administrativa

Artigo 83.º CPA

Consulta do processo e passagem de certidões

1- Os interessados têm o direito de consultar o processo que não contenha documentos classificados ou que revelem segredo comercial ou industrial ou segredo relativo à propriedade literária, artística ou científica.

2- O direito referido no número anterior abrange os documentos relativos a terceiros, sem prejuízo da proteção dos dados pessoais nos termos da lei.

(...)"

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – área Administrativa

Artigo 6.º Restrições ao direito de acesso (...)

5 - Um terceiro só tem direito de acesso a **documentos nominativos**:

- a) Se estiver munido de autorização escrita do titular dos dados que seja explícita e específica quanto à sua finalidade e quanto ao tipo de dados a que quer aceder;
- b) Se demonstrar fundamentadamente ser titular de um interesse direto, pessoal, legítimo e **constitucionalmente protegido** suficientemente relevante, após ponderação, no quadro do **princípio da proporcionalidade**, de **todos os direitos fundamentais em presença** e do **princípio da administração aberta**, que justifique o acesso à informação.

- Todos os “direitos fundamentais” em presença implica necessariamente considerar o artigo 35.º da CRP e acompanhar as imposições do princípio da finalidade.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – área Administrativa

Artigo 268º CRP

Direitos e garantias dos administrados

1. Os cidadãos têm o direito de ser informados pela Administração, sempre que o requeiram, sobre o andamento dos processos em que sejam diretamente interessados, bem como o de conhecer as resoluções definitivas que sobre eles forem tomadas.

2. Os cidadãos têm também o direito de acesso aos arquivos e registos administrativos, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal e à intimidade das pessoas.

Princípio geral é o do acesso, mas tem que existir uma interpretação efetuada em harmonia com o artigo 35.º da CRP.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento – área Administrativa

Artigo 86.º RGD

Tratamento e acesso do público aos documentos oficiais

- Os dados pessoais que constem de documentos oficiais na posse de uma autoridade pública ou de um organismo público ou privado para a prossecução de atribuições de interesse público podem ser divulgados pela autoridade ou organismo nos termos do direito da União ou do Estado-Membro que for aplicável à autoridade ou organismo público, a fim de conciliar o acesso do público a documentos oficiais com o direito à proteção dos dados pessoais nos termos do presente regulamento.
- O presente regulamento permite tomar em consideração o princípio do direito de acesso do público aos documentos oficiais na aplicação do mesmo. O acesso do público aos documentos oficiais pode ser considerado de interesse público. Os dados pessoais que constem de documentos na posse dessas autoridades públicas ou organismos públicos deverão poder ser divulgados publicamente por tais autoridades ou organismos, se a divulgação estiver prevista no direito da União ou do Estado-Membro que lhes for aplicável.
- Essas legislações deverão conciliar o acesso do público aos documentos oficiais e a reutilização da informação do setor público com o direito à proteção dos dados pessoais e podem pois prever a necessária conciliação com esse mesmo direito nos termos do presente regulamento. A referência a autoridades e organismos públicos deverá incluir, nesse contexto, todas as autoridades ou outros organismos abrangidos pelo direito do Estado-Membro relativo ao acesso do público aos documentos.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento

Lei - 58/2019

A peça do puzzle que faltava para completar o regime nacional de proteção de dados

Dia 8 de agosto - publicada a Lei n.º 58/2019 que assegurou a execução, na ordem jurídica nacional, do Regulamento

(UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento

Lei - 58/2019

Destacamos, de forma simplificada, as principais disposições da Lei n.º 58/2019:

1 . Entidades Competentes

- a CNPD foi nomeada a autoridade de controlo nacional para efeitos do RGPD;
- a autoridade designada para a acreditação dos organismos de certificação em matéria de proteção de dados é o IPAC, I. P.;

2 . Entidades Públicas

- as entidades públicas poderão ficar isentas de coimas por três anos com um pedido prévio de dispensa, que depende da aprovação da CNPD;
- admite-se que o tratamento possa ser realizado para finalidades diferentes das que justificam a recolha de dados, desde que esteja em causa o interesse público;

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento

Lei - 58/2019

3. Menores

- a idade considerada para o consentimento de menores é de 13 anos para efeitos de consentimento livre, específico, informado e explícito para tratamento de dados pessoais;
- caso a criança tenha idade inferior a 13 anos, o tratamento só é lícito se o consentimento for dado pelos seus representantes legais, preferencialmente através de meios de autenticação segura;

4. Relação laboral

- a recolha de dados biométricos apenas poderá ser efetuada para fins de controlo de assiduidade e acesso às instalações e a sua utilização obedece a regras específicas e definidas;
- as imagens gravadas em vídeo ou outros meios tecnológicos de vigilância só podem ser utilizadas no âmbito de processo penal;

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento

Lei - 58/2019

5 - Titulares falecidos

- os dados pessoais de pessoas falecidas são protegidos quando se integrem nas categorias especiais de dados pessoais ou quando se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações;

6 - Saúde

- os dados de saúde e genéticos apenas podem ser acedidos por profissionais devidamente abrangidos pela obrigação de sigilo e exclusivamente através de meios eletrónicos, sendo que o acesso a estes dados deve ser comunicado ao titular;

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento

Lei - 58/2019

7 - Encarregado de Proteção de Dados (DPO)

- são definidas funções adicionais para o DPO, nomeadamente: a) assegurar a realização de auditorias, quer periódicas, quer não programadas; b) sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança; c) assegurar as relações com os titulares dos dados;

8 - Coimas

- no caso das grandes empresas, as contra-ordenações muito graves terão um valor mínimo de coimas de 5.000€ e as graves, de 2.500€. Para as PME, os valores mínimos variam entre os 1.000€ e os 2.000€;

- para a determinação da medida de coima, deve ser considerado o volume de negócios e o balanço anual da empresa, o carácter continuado da infração e a dimensão da entidade;

- são tipificados crimes referentes a dados pessoais, nomeadamente a utilização de dados com uma finalidade diferente da recolha, o acesso indevido, o desvio de dados, a violação do dever de sigilo e a desobediência, puníveis com pena de prisão até dois anos ou com pena de multa até 240 dias.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento

Lei - 58/2019

8 – Coimas (Cont.)

- Não há qualquer isenção ou dispensa prevista para as entidades públicas,
- Mas as entidades públicas podem, mediante pedido devidamente fundamentado, solicitar à CNPD a dispensa da aplicação de coimas durante o prazo de três anos até 9 de julho 2022.
- No entanto, em início de Setembro/2019, a CNPD aprovou uma deliberação interpretativa (em 03 de Setembro) sobre a dispensa de aplicação de coimas às entidades públicas:
Só é possível requerer essa dispensa fundamentada após acusação da prática de um ilícito contraordenacional.

Regulamento Europeu Proteção de Dados

Legislação Nacional vs Regulamento

Lei - 58/2019

Paralelamente -

- **DELIBERAÇÃO/2019/494 (03 de Setembro 2019)**

A CNPD delibera:

- a. Fixar o entendimento de que determinadas normas desta lei são manifestamente incompatíveis com o direito da União, centrando, por ora, a sua atenção sobre aquelas disposições que, pela sua relevância e frequência de aplicação, suscitam a premência da adoção formal de tal entendimento;
- b. Que, com fundamento no princípio do primado do direito da União Europeia, e nos demais argumentos que a seguir expõe, desaplicará em casos futuros que venha a apreciar, relativos a tratamentos de dados e às condutas dos respetivos responsáveis ou subcontratantes, as seguintes disposições da Lei n.º 58/2019, de 8 de agosto:
 1. Artigo 2.º, n.º 1 e n.º 2;
 2. Artigo 20.º, n.º 1;
 3. Artigo 23.º;
 4. Artigo 28.º, n.º 3, alínea a)
 5. O regime das contraordenações: os artigos 37.º, 38.º e 39.º;
 6. Artigo 61.º, n.º 2;
 7. Artigo 62.º, n.º 2;

1. Introdução ao Regulamento (EU) 2016/679
2. Direitos do titular dos dados
3. Obrigações dos responsáveis pelo tratamento
4. Legislação Nacional vs Regulamento
5. **Impacto do novo regulamento na UA: resumo**

Impacto do novo regulamento na UA

A Academia



Impacto do novo regulamento na UA

O que foi feito

- ☐ Levantamento, análise e registo dos processos regulares e em curso, relativos ao funcionamento normal da Universidade;
- ☐ Levantamento, análise e registo de todas as fontes de informação que contenham dados pessoais;
- ☐ Levantamento, análise e correção de condições técnicas, sejam físicas sejam organizativas, para melhor salvaguarda dos dados, desde a recolha e tratamento até ao arquivo;
- ☐ Sensibilização e envolvimento da estrutura humana da Universidade;
- ☐ Preparação para a continuidade – Criação de modelo organizativo que garanta a *compliance* RGPD desde a conceção e por defeito.

Impacto do novo regulamento na UA

Ao iniciar um novo tratamento de dados deve ter-se em atenção o seguinte:

- É preciso fazer uma análise prévia de risco, relativamente aos direitos e garantias de privacidade dos potenciais titulares de dados envolvidos;
- Eventualmente será necessário realizar uma avaliação de impacto;
- **É necessário o registo e acompanhamento de todas as operações envolvendo dados pessoais;**
- Enquanto membro da universidade, será responsável pelos tratamentos de dados que realizar;

A Universidade tem um DPO e uma equipa de apoio, preparados para ajudar a construir, acompanhar e auditar os tratamentos de dados em curso.

No caso da UA existe um 'pivot' em cada unidade munido com técnicas e ferramentas capazes de satisfazer estas obrigações, minimizando o impacto do RGPD na atividade regular da Universidade.

Em resumo

Enquanto responsável por um tratamento de dados, o que devo fazer e quais os passos que devo dar:

- 1- **Preparar uma descrição completa do processo**, para melhor análise e compreensão do mesmo por todas as partes envolvidas, nomeadamente Pivot's RGPD, DPO, CNPD e outros auditores, para além de servir de orientação ao próprio.
- 2 – **Preparar a informação ao titular**, em função das condições do processo e de acordo com todos os possíveis diferentes passos, e verificar o fundamento para a licitude do tratamento, que por norma em processos de investigação assenta no consentimento do titular de dados;
- 3 – **Proceder ao registo da operação com a cooperação dos Pivot's de unidade**, e eventualmente a uma AIPD- análise de impacto sobre a privacidade de dados (DPIA em Inglês).

Em resumo

1-Descrição completa do processo:

- a) **Identificar o, ou os, responsáveis pelo tratamento (quem define a forma, os meios e os fins)** – Note-se que os orientadores de alunos em trabalhos autónomos (teses de Mestrado ou Doutoramento) podem não ser, e geralmente não são, responsáveis pelo tratamento de dados, porquanto os dados apenas servem para a investigação em causa. Além do mais os orientadores são também avaliadores (Júri), o que resultaria numa incompatibilidade e, mesmo, os eventuais dados recolhidos podem manter a sua existência para além da aprovação da própria tese, e depois do aluno ter saído da UA;
- b) **Identificar quais os dados a recolher**, especificando a existência ou não de dados sensíveis;
- c) **Identificar formas de recolha** – se em formulário, online ou em papel, se diretamente por via de entrevista, com ou sem gravação de vídeo, ou qualquer outra forma;

Em resumo

1-Descrição completa do processo: (cont.)

- d) **Explicar o tratamento que irá ser aplicado aos dados** (se em aberto se por aplicação de processos de pseudonimização ou anonimização), em que momentos, com que ferramentas (software, manualmente, videogravação, uso de telemóvel, etc ...);
- e) **Definir a população alvo do estudo** (crianças; adultos; populações vulneráveis; ...) e a forma como serão “recrutados”;
- f) **Certificar se serão recebidos dados de outras fontes** (de escolas ou hospitais, por exemplo). No caso de processos de investigação em escolas existe obrigação de registo e autorização prévios da no MIME – monitorização de inquéritos em meio escolar;
- g) **Certificar a sua posição pessoal no processo** – muitas vezes o investigador pode simultaneamente ter outra figura perante os titulares de dados (professor da turma, ou médico ...), e é importante definir qual a sua efetiva “veste” no momento da realização do trabalho;
- h) **Explicar se existe ou não partilha de dados com terceiras entidades** (ex. com os orientadores, ou por via do uso de software para o tratamento de dados – e.g. WebQda), e existindo, garantir que tais entidades cumprem com o RGPD, assinando contrato que o assegure → podem ser subcontratados ou assumir outras figuras jurídicas, como p.ex. corresponsáveis;

Em resumo

1-Descrição completa do processo: (cont.)

- i) **Explicar de que forma se pretende publicar os dados** (na tese, mas também em eventuais artigos de revistas especializadas, ou ainda em bases de dados ao abrigo do movimento open data) e assim sendo explicar em que formato o irão fazer – que em princípio deve ser anónimo e de resultados agregados;
- j) **Explicar a forma como irão guardar os dados em todo o processo** – oferecendo todas as melhores garantias técnicas e administrativas para a sua segurança e salvaguarda, aqui se incluindo o controlo de acessos, a reposição em caso de falha (backup's) e, para situações em que os dados sejam de natureza sensível, a encriptação;
- k) **Definir prazos para a guarda dos dados** (sempre que existam em formato não anónimo ou ainda pseudonomizados, porque depois de absolutamente anonimizados estão fora do escopo do RGPD);

Em resumo

1-Descrição completa do processo: (cont.)

- i) **Explicar de que forma se pretende publicar os dados** (na tese, mas também em eventuais artigos de revistas especializadas, ou ainda em bases de dados ao abrigo do movimento open data) e assim sendo explicar em que formato o irão fazer – que em princípio deve ser anónimo e de resultados agregados;
- j) **Explicar a forma como irão guardar os dados em todo o processo** – oferecendo todas as melhores garantias técnicas e administrativas para a sua segurança e salvaguarda, aqui se incluindo o controlo de acessos, a reposição em caso de falha (backup's) e, para situações em que os dados sejam de natureza sensível, a encriptação;
- k) **Definir prazos para a guarda dos dados** (sempre que existam em formato não anónimo ou ainda pseudonomizados, porque depois de absolutamente anonimizados estão fora do escopo do RGPD);

Em resumo

2- Preparar a informação ao titular (e o consentimento):

A informação ao titular deve assentar nos aspetos principais referidos ao longo desta apresentação, especificamente descritos no ponto anterior, construída numa linguagem simples e objetiva, contemplando:

- A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
- Os contactos do encarregado da proteção de dados, se aplicável – no caso de estudos autónomos (teses Mestrado e Doutoramento, e porque os dados podem persistir para além do tempo em que existe uma relação contratual do aluno com a UA, o DPO não assegura, pois não tem capacidade de intervenção sobre os dados) .
- As finalidades do tratamento .
- O fundamento jurídico para o tratamento (para processo de investigação em princípio o consentimento ao abrigo do RGPD)
- Os destinatários ou categorias de destinatários dos dados pessoais.
- Transferências, ou não, para países terceiros (explicando a existência de decisão da Comissão, ou garantias adequadas).
- Prazo de conservação dos dados pessoais (ou critérios).
- Direitos ARCO.
- Direito de retirar o consentimento.
- O direito de apresentar reclamação a uma autoridade de controlo .
- Existência de decisões automatizadas, lógica aplicada, importância e consequências.

Em resumo

2- Preparar a informação ao titular (e o consentimento): (cont.)

Sobre a referida informação ao titular, que deve ser apresentada previamente à recolha de dados (sejam eles recolhidos de que forma forem: em papel, em inquérito online, por videogravação, etc ...) **deverá ser implementado o consentimento do titular, no caso em que exista efetiva recolha de dados pessoais que o identifiquem de forma direta ou indireta**, para permitir o tratamento dos seus dados. O consentimento deve ser um ato informado, livre, específico e explícito. Para satisfazer todos estes requisitos apenas se consegue antever uma forma de decisão, **entre um sim e um não**, o titular aceita participar naquele estudo e dá consentimento ao tratamento de dados na forma explicada.

Não está definida a forma como deve a informação ao titular e a obtenção do seu consentimento registados, apenas é dito que o Responsável pelo tratamento deve ser capaz de o demonstrar, pelo que se sugere se registe o processo de alguma forma (em papel, no próprio formulário online, se for esse o caso, ou por registo de vídeo dessa parte também)

Em resumo

3- Proceder ao registo da operação com a cooperação dos Pivot's de unidade:

De toda esta atividade deve existir registo, com as devidas evidências da forma como serão os dados tratados, bem como de respetiva análise de riscos para os direitos, liberdades e garantias dos titulares de dados. Tal registo está ainda a ser feito por via do documento editável DPIA.pdf, mas será, a breve trecho, alterado para um sistema online que facilitará o procedimento, na forma e também no conteúdo.

Sendo o culminar de todo um processo, é relativamente indiferente a forma como este poderá ser registado, porquanto a base de uma boa aplicação do regulamento no caso de tratamento de dados pessoais assenta nos primeiros 2 pontos deste resumo.

Depois de aprovado o processo pelo DPO, este emitirá uma declaração que poderá ser usada como garante do cumprimento do RGPD, seja junto da CEDUA, seja perante outras entidades.



Questões?