



Regulamento Geral de Proteção de Dados



joao.gabriel@micc.pt



Introdução de conceitos de proteção de dados



ANCCD
Segurança Social



- *Compreender as alterações do Regime de Proteção de Dados*
- *Operacionalizar os conceitos de:*
 - *Dado Pessoal*
 - *Operação de Tratamento*
 - *Responsável pelo Tratamento*
 - *Subcontratante*
- *Compreender a funcionalidade dos princípios de Proteção de Dados*



Direitos dos titulares dos dados (consentimento, acesso, apagamento)



Articulação entre autoridades de controlo



Encarregado de protecção dados



Entidades subcontratadas



Operações de tratamento (ponderação para publicação; conservação)



Notificação de violações de dados



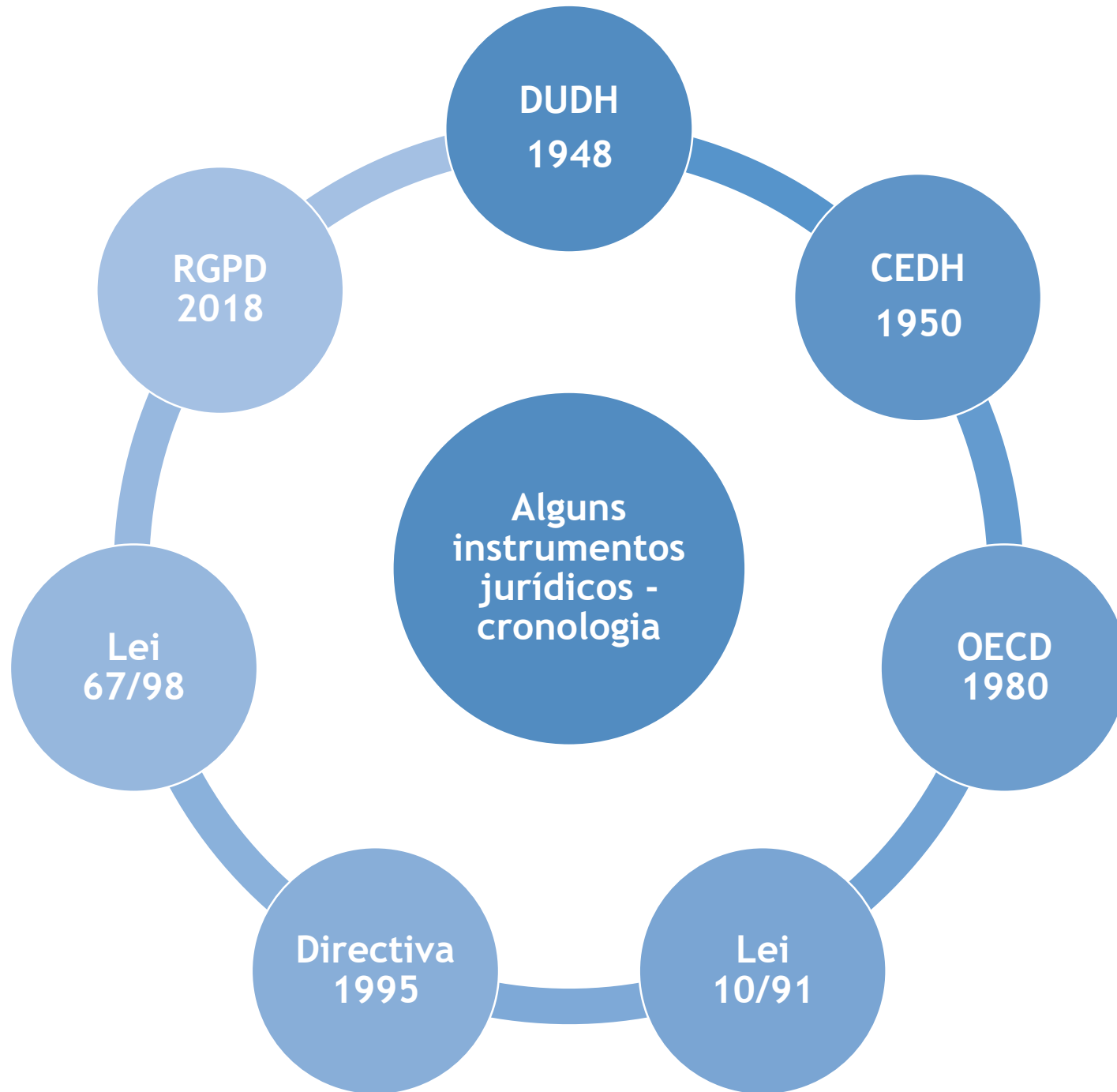
Papel da autoridade de controlo (CNPD)



Sanções e o dever de indemnizar

- “..... O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados”
- *Art.º 2.º (RGPD)*

Introdução ao RGPD



LPDP

- **Regulamento**

Directiva 95/46/CE (34 artigos em 17 páginas)

Lei n.º 67/98 (52 artigos em 11 páginas)

- Regulamento (UE) 2016/679 (99 artigos em 88 páginas)

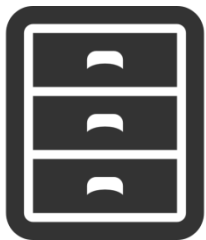


Âmbito de aplicação

Âmbito material – a que se aplica?

*“(...) O presente regulamento aplica-se ao tratamento de dados pessoais por **meios total ou parcialmente automatizados**, bem como ao tratamento por meios não automatizados de dados pessoais contidos **em ficheiros ou a eles destinados**”*

Art. 2.º RGPD



Âmbito territorial – onde se aplica?

*“(...) tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante **situado no território da União**, independentemente de o tratamento ocorrer dentro ou fora da União. (...).*

*tratamento de dados pessoais de titulares [**que se encontrem**] no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com (...) oferta de bens ou serviços [oneroso ou gratuito] (...) o controlo do seu comportamento [profiling], desde que esse comportamento tenha lugar na União.”*

Art. 3.º RGPD





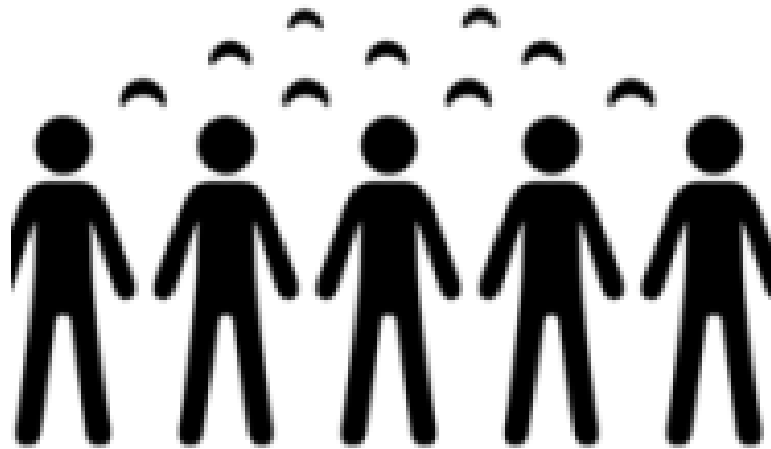
Alguns conceitos chave

Dados pessoais – O que são?

*“**Dados pessoais**, informação relativa a uma pessoa singular identificada **ou** identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, directa ou indirectamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via electrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.”*



Informação relativa a uma pessoa singular identificada ou identificável



Pessoa
Colectiva



Nome

Número
Cartão Crédito

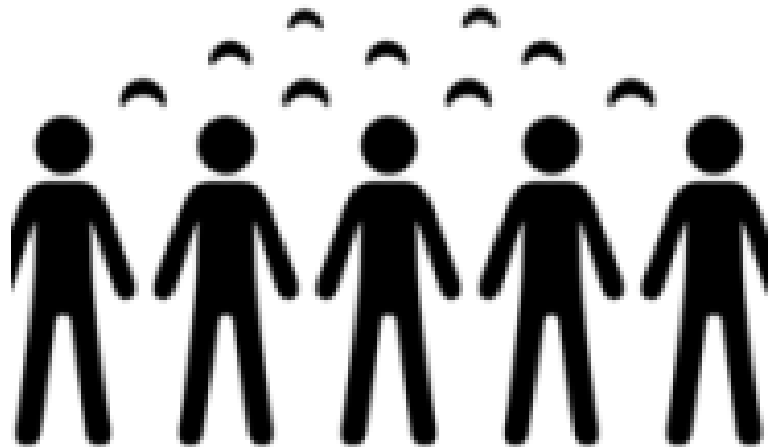
Número
telefone

Salário

Morada

Data
Nascimento

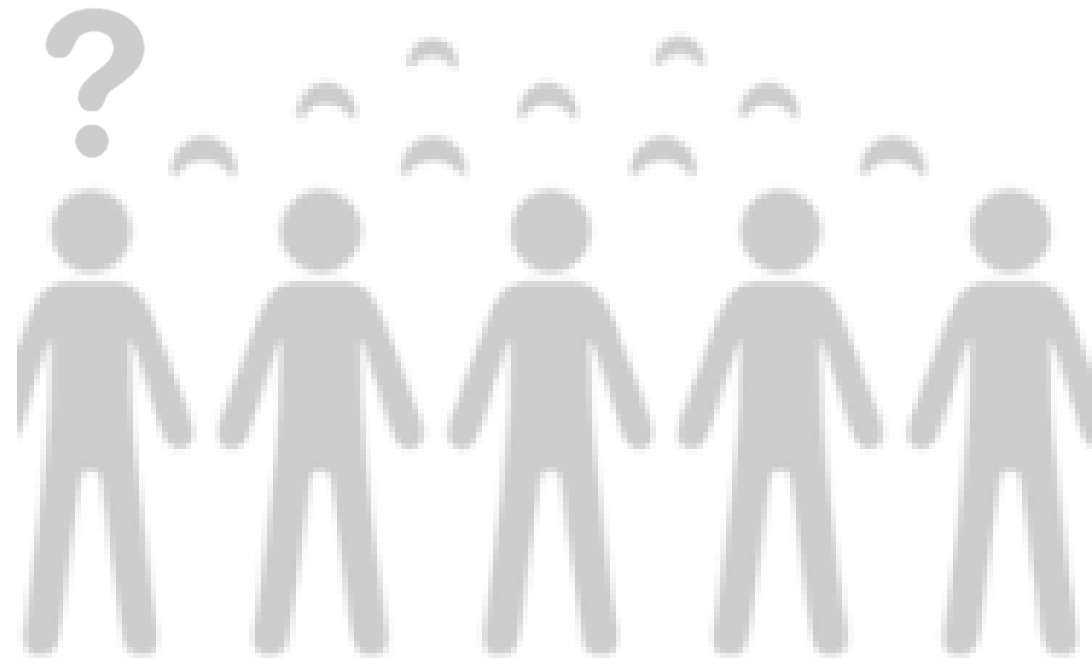
*Pessoa singular identificada **ou** identificável
directa **ou** indirectamente*



Nome

Endereço
I.P.

Anonimização



Anonimização

origem racial ou
étnica

opiniões políticas

convicções
religiosas ou
filosóficas

filiação sindical

tratamento de dados
genéticos, dados
biométricos para
identificar uma pessoa
de forma inequívoca

dados relativos à
saúde

dados relativos à
vida sexual ou
orientação sexual
de uma pessoa



Categorias especiais de
dados pessoais

Tratamento de dados pessoais – O que é?

*“**Tratamento**, qualquer operação ou um conjunto de **operações** efectuadas **sobre dados pessoais** ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição”*



Tratamento de dados pessoais – O que é?

a recolha, o registo, a difusão ou qualquer outra forma de disponibilização, o apagamento


Fotografia/nome do colaborador no *website*

Registo de acessos ao edifício

Consulta de bases de dados de terceiro

X





Licitude, lealdade e transparência do tratamento em relação ao titular dos dados;

Limitação das **finalidades**: determinadas, explícitas e legítimas;

Minimização dos dados: solicitar apenas os dados adequados, pertinentes e limitados ao necessário para as finalidades para as quais são tratados;

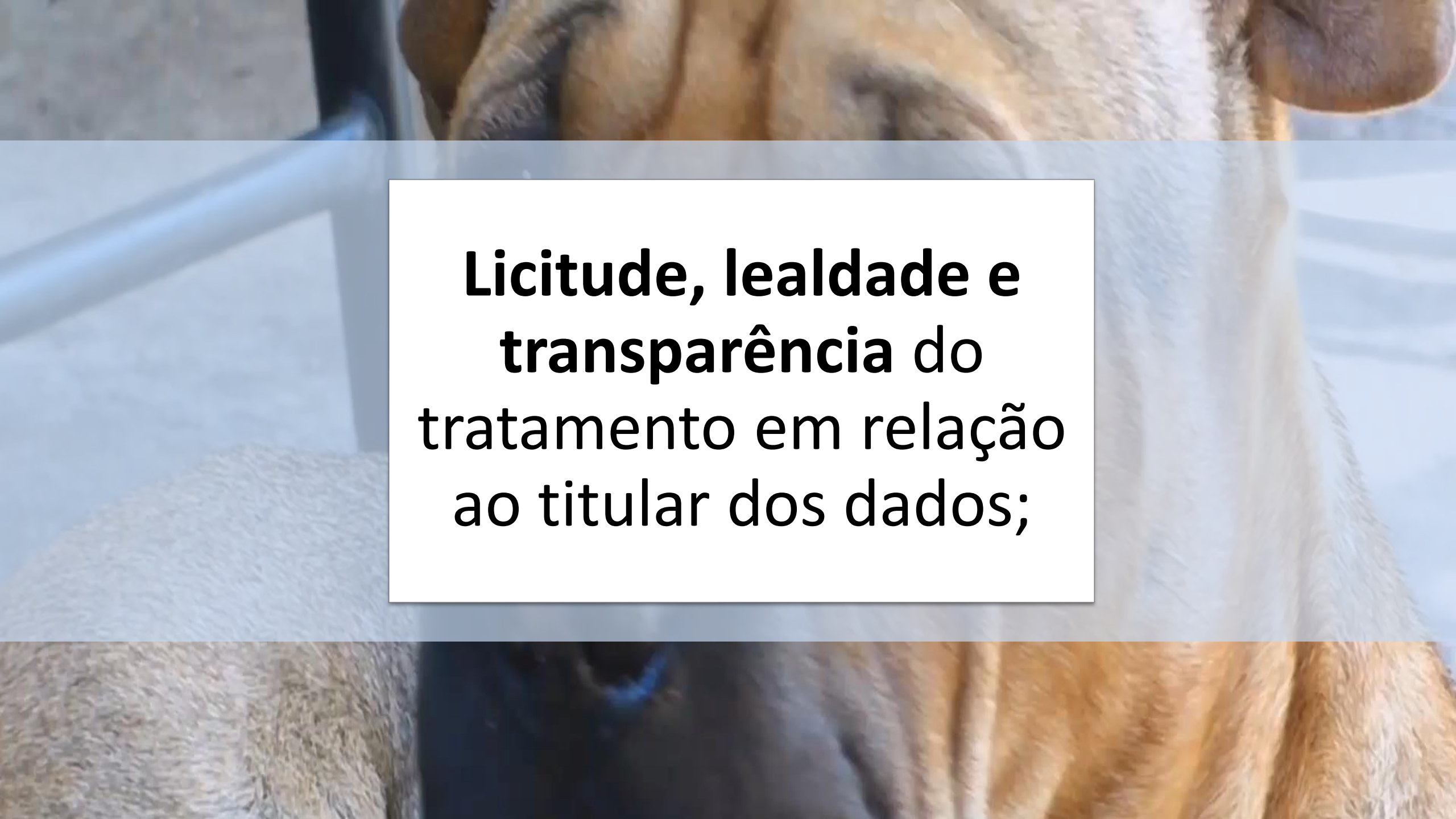
Exactidão: dados inexactos têm de poder ser eliminados/rectificados com prontidão:

Limitação temporal da conservação: apenas pelo período necessário;

Integridade e confidencialidade: o tratamento tem de ser seguro (perda, danificação, tratamento ilícito);

Responsabilidade: o responsável pelo tratamento tem de poder **comprovar** que observou estes princípios.

Direitos dos titulares

A close-up photograph of a dog's face, showing its eyes and nose. The dog has light brown fur. A white rectangular box with a thin black border is centered over the image, containing text. The background is slightly blurred, showing what appears to be a metal railing or fence.

**Licitude, lealdade e
transparência do
tratamento em relação
ao titular dos dados;**

Informações a facultar

- A identidade e os contactos do responsável pelo tratamento
- Identidade do seu representante (se aplicável)
- Os contactos do encarregado da proteção de dados, se for caso disso;
- As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
- Os destinatários ou categorias de destinatários dos dados pessoais (incluindo outros responsáveis pelo tratamento, subcontratantes, etc.).
- Prazo de conservação dos dados pessoais ou os critérios usados para definir esse prazo;
- Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro
- Quaisquer informações para garantir um tratamento equitativo e transparente
- Direitos do titular

Licitude do tratamento



- Há **consentimento** do titular dos dados;
- É necessário para a **execução de um contrato** no qual o titular dos dados é parte;
- É necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
- É necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
- É necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública;
- É necessário para efeito dos **interesses legítimos** prosseguidos pelo responsável pelo tratamento ou por terceiros.

Licitude do tratamento

- Há **consentimento** do titular dos dados;
- É necessário para a **execução de um contrato** no qual o titular dos dados é parte;
- É necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
- É necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
- É necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública;
- É necessário para efeito dos **interesses legítimos** prosseguidos pelo responsável pelo tratamento ou por terceiros.

Consentimento

- Manifestação de vontade livre
- Específico
- Explícito
- Informado
- Inequívoco
- Acção positiva demonstrável
- Retirável a qualquer momento
- O silêncio ou inactividade não permite o consentimento implícito

CONSENT



Freely Given
Reversible
Informed
Enthusiastic
Specific

Consentimento

- Demonstrável
- Pode-se retirar (o que tem de ser informado) e de forma fácil e livre
- Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente

Dados de categoria especial

- Consentimento explícito
 - Obrigações laborais
 - Interesses vitais do titular dos dados em caso de incapacidade
 - Atividades legítimas e mediante garantias adequadas, por uma fundação, associação
 - Dados pessoais que tenham sido manifestamente tornados públicos
 - Declaração, ao exercício ou à defesa de um direito num processo judicial
- Interesse público importante
 - Fins médicos
 - Fins estatísticos
 - Fins Políticos
 - Efeitos Tributários
 - Efeitos Contributivos



- Publicado Maio 2016;
- Entra em vigor Maio 2018;
- Clarifica o conceito de dados pessoais;
- Estabelece **novos direitos** para os titulares dos dados e **reforça** direitos dos mesmos: direito à portabilidade dos dados, direito ao esquecimento e direito de oposição a *profiling*.

«RGPD»

Deveres do responsável pelo tratamento

- Deveres de *accountability*;
- Notificação obrigatória à CNPD em caso de *data breaches*;
- *Privacy Impact Assessments*;
- *DPO*;
- Etc.

Consentimento

- Incumprimento punido com coimas que podem ascender a 4% da facturação anual global ou a €20.000.000,00.

Sanções



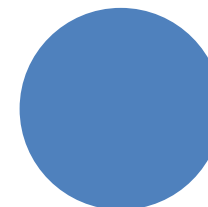
O artigo 28 requer que o contrato assegure que o subcontratante:

- Trata os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento
- Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;
- Adota todas as medidas técnicas exigidas
- Presta assistência ao responsável pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados
- Apaga ou devolve-lhe todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes,
- Disponibiliza ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no RGPD



- O responsável pelo tratamento recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos Dados
- O subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral
- O tratamento em subcontratação é regulado por contrato ou outro ato normativo
- O contrato deve estabelecer o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento.

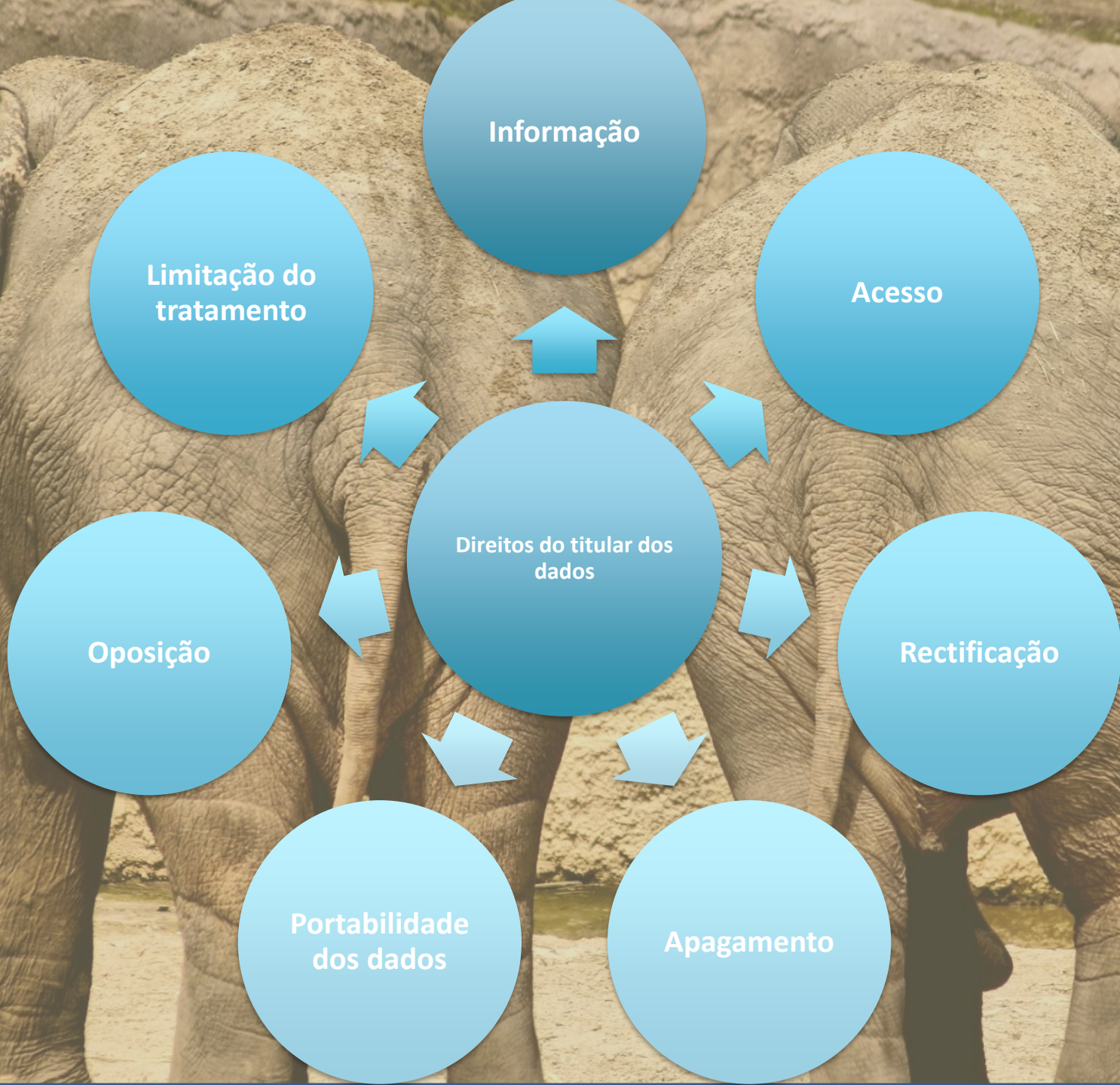
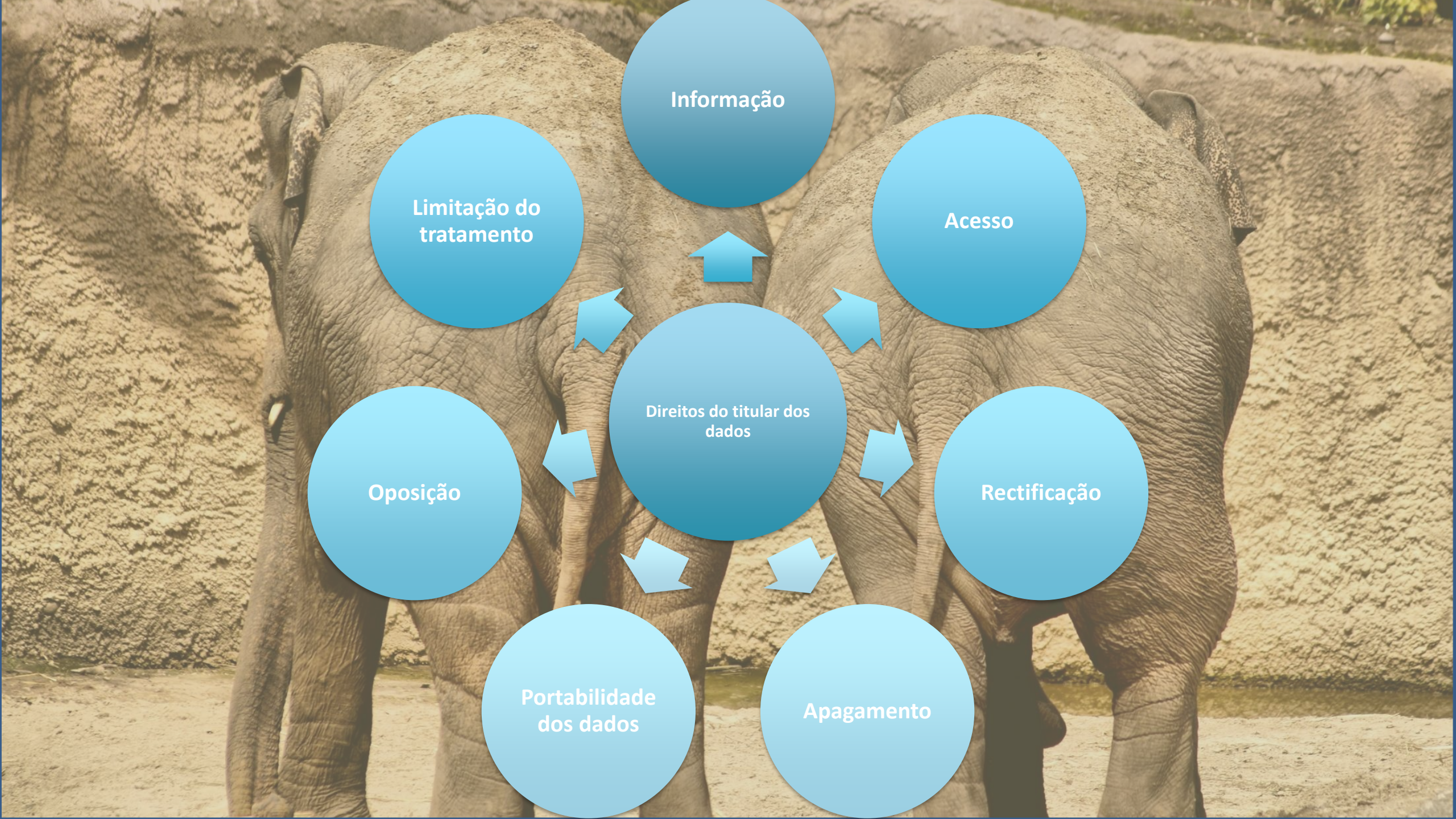
Relação entre o Responsável pelo Tratamento e o Subcontratante

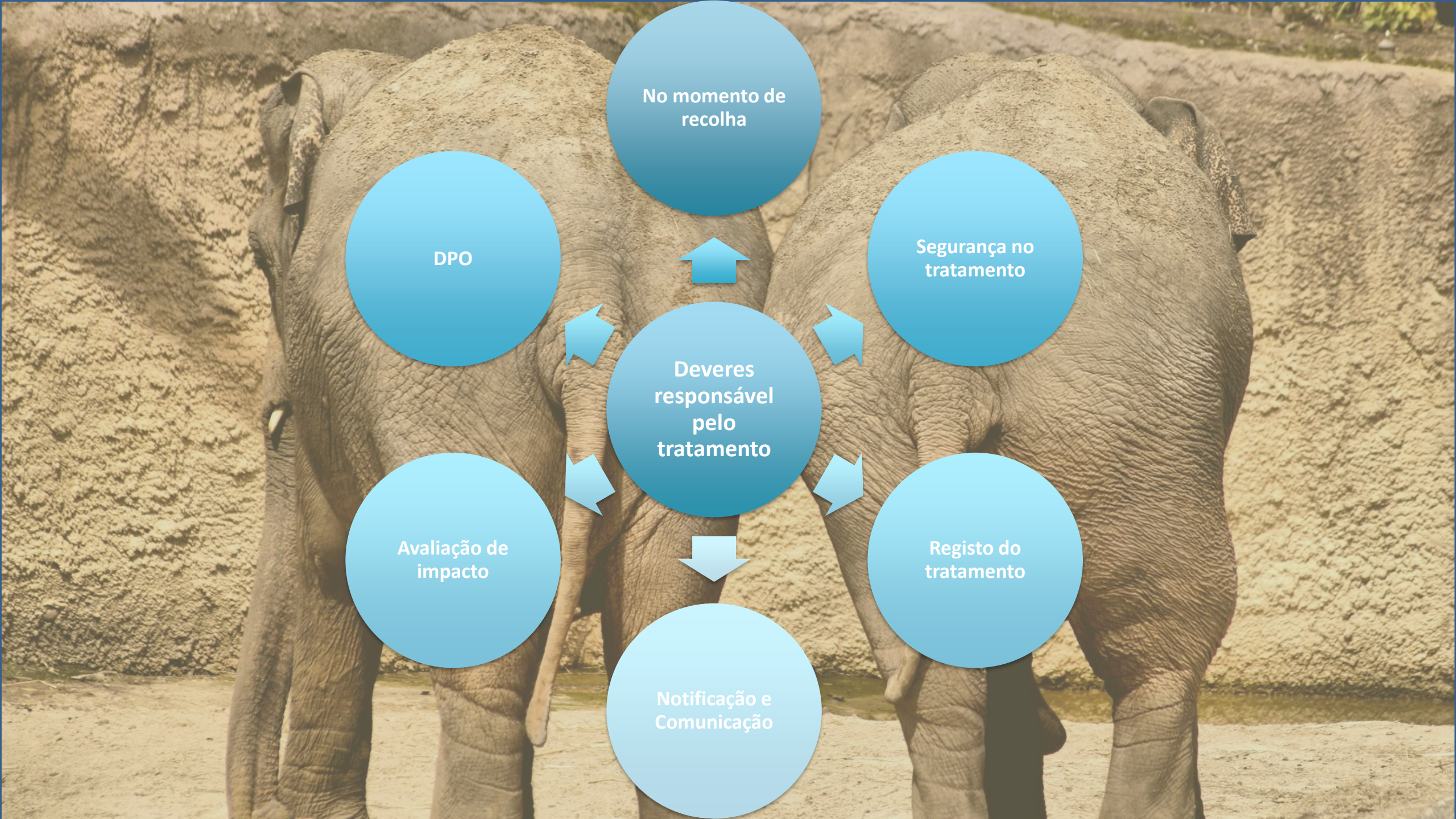




Sub-Subcontratação

- As mesmas obrigações em matéria de proteção de dados que as estabelecidas no contrato ou outro ato normativo entre o responsável pelo tratamento e o subcontratante,
- apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento seja conforme com os requisitos do RGPD
- 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.





No momento de
recolha

DPO

Segurança no
tratamento

Deveres
responsável
pelo
tratamento

Avaliação de
impacto

Registo do
tratamento

Notificação e
Comunicação

O TD tem o direito a:

- Solicitar ao RT a retificação, apagamento ou a limitação do tratamento ou o direito de se opor ao tratamento
- Direito a apresentar uma reclamação a uma autoridade de controlo
- Se os dados não tiverem sido recolhidos junto do titular, as informações sobre a fonte dos dados
- A existência de decisões automatizadas, incluindo a definição de perfis, e, neste caso, sobre a lógica subjacente, bem como a importância e consequências desse tratamento para o TD

O TD tem o direito de ser informado sobre:

- se os seus dados pessoais estão a ser tratados pelo RT ou por um Subcontratante
- As finalidades do tratamento
- As categorias de dados pessoais objeto de tratamento
- Os destinatários a quem os dados são ou vão ser comunicados
- O prazo de conservação dos dados pessoais ou os critérios usados para fixar esse prazo

O TD tem o direito a receber cópias da informação num formato intelegível e permanente, se solicitado

- ✓ Uma cópia grátis
- ✓ Outras cópias podem estar sujeitas ao pagamento de uma taxa razoável ao RT
- ✓ Os pedidos devem ser feitos por escrito
- ✓ Os pedidos podem ser em formato eletrónico caso em que a resposta também tem de ser dada em formato eletrónico, salvo pedido em contrário do TD
- ✓ A informação deve ser fornecida de forma concisa, transparente e numa linguagem simples

Prazo de resposta:

- Um mês
- Prorrogável por períodos adicionais de 2 meses (no máximo) quando necessário, dependendo dos seguintes elementos:
 - Complexidade do(s) pedido(s)
 - Número de pedidos
- O RT deve informar o TD no prazo de 1 mês da receção do pedido e dar razões para o atraso



- O RT pode recusar um pedido de acesso:
- Quando a identidade do TD não possa ser determinada
- Quando os pedidos forem manifestamente infundados ou excessivos (desproporcionais)
- Quando os pedidos forem repetitivos
- Quando o Pedido de Acesso seja repetitivo, o TD pode cobrar um valor administrativo ou recusar o pedido
- O ónus da prova de demonstrar que o pedido é infundado ou excessivo pertence ao RT





Nome e os contactos do responsável pelo tratamento e do encarregado da proteção de dados

Finalidades do tratamento dos dados

Categorias de titulares de dados e das categorias de dados pessoais

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

Transferências internacionais (requisitos adicionais)

Prazos previstos para o apagamento das diferentes categorias de dados

Descrição geral das medidas técnicas e organizativas no domínio da segurança

Registo



Casos Práticos



ANCCD
Segurança Social



1.º Caso Práctico – Marketing Directo

- No dia 4 de Março de 2018, A. decidiu aderir a uma actividade desportiva “família activa”, entregando ao balcão do CCD a proposta de adesão, da qual constava a seguinte frase pré-preenchida:
“Dou o meu consentimento ao tratamento de dados pessoais por parte da CCD. e outras entidades do Grupo, para quaisquer efeitos relacionados com a relação contratual ou outros conexos.”.
- No dia 4 de Julho de 2018, A. recebeu um e-mail promocional remetido pelo Instituto de Informática da Segurança Social relativamente à aplicação “Sociedade Directa”, propondo a adesão a um programa de benefícios.
- O e-mail não indicava contactos, mas apenas uma hiperligação para um site, que solicitava o preenchimento de dados de identificação e de contacto para que a pessoa pudesse receber mais informação.
- A. remeteu uma carta à Segurança Social, solicitando que o informasse como obteve os seus dados, que os apagasse e não o voltasse a contactar.

2.º Caso Prático – Inquéritos

- A Empresa X. solicitou, por e-mail remetido seus clientes, a indicação de pessoas entre os 10 e os 30 anos, que pudessem estar interessadas em participar num inquérito relativo a hábitos de poupança de água.
- B. respondeu por e-mail, remetendo informação de identificação e de contacto de C., D. e E., que julgou terem interesse em participar.
- A Empresa X. transmitiu a informação a um *call center*, que telefonou a tais pessoas no dia 12 de Junho de 2018, solicitando informação quanto aos seus rendimentos e hábitos de poupança de água.
- Passados três meses a empresa responsável pelo *Call Center* sofreu um ataque informático e toda a informação recolhida de C. e D. foi divulgada na internet.
- A informação de E., menor de idade, não foi divulgada, mas os seus pais pretendem uma indemnização por não terem sido informados quanto à recolha dos dados e quanto ao incidente.

3.º Caso Prático – Inscrição

Quem trata os dados

Os contactos do encarregado da proteção de dados

Porque tratam os dados

A quem são transmitidos

Durante quanto tempo

Para quem transferem os dados

VANTAGENS EM SER SÓCIO

Ao tornar-se associado do CCD de Lisboa passa a ter acesso a um conjunto exclusivo de atividades de lazer, desportivas, culturais e de convívio. Paralelamente, poderá usufruir de vários protocolos comerciais, que lhe garantem descontos em produtos óticos, culturais, educativos, lúdicos, desportivos e até de artigos para casa. Consulte nestas páginas as várias vantagens em vigor:

- > Protocolos
- > Agenda de Eventos

Formulário de Pedido de Sócio

Nome Completo *

Nome pretendido para Sócio *

E-mail *

Telefone *

Unidade de Trabalho *

Serviço *

Morada de Serviço *

Mensagem



O que fazer - Roadmap




ANCCD
Segurança Social



Licitude, lealdade e transparência do tratamento em relação ao titular dos dados;



A close-up photograph of a dog's face, showing its eyes, nose, and fur. The dog has brown fur and dark eyes. The image is partially obscured by a light blue horizontal band containing text boxes.

Minimização dos dados:
solicitar apenas os dados adequados, pertinentes e limitados ao necessário para as finalidades para as quais são tratados;

Exactidão: dados inexactos têm de poder ser eliminados/rectificados com prontidão:

Limitação temporal da conservação: apenas pelo período necessário;

Identificar os Processos

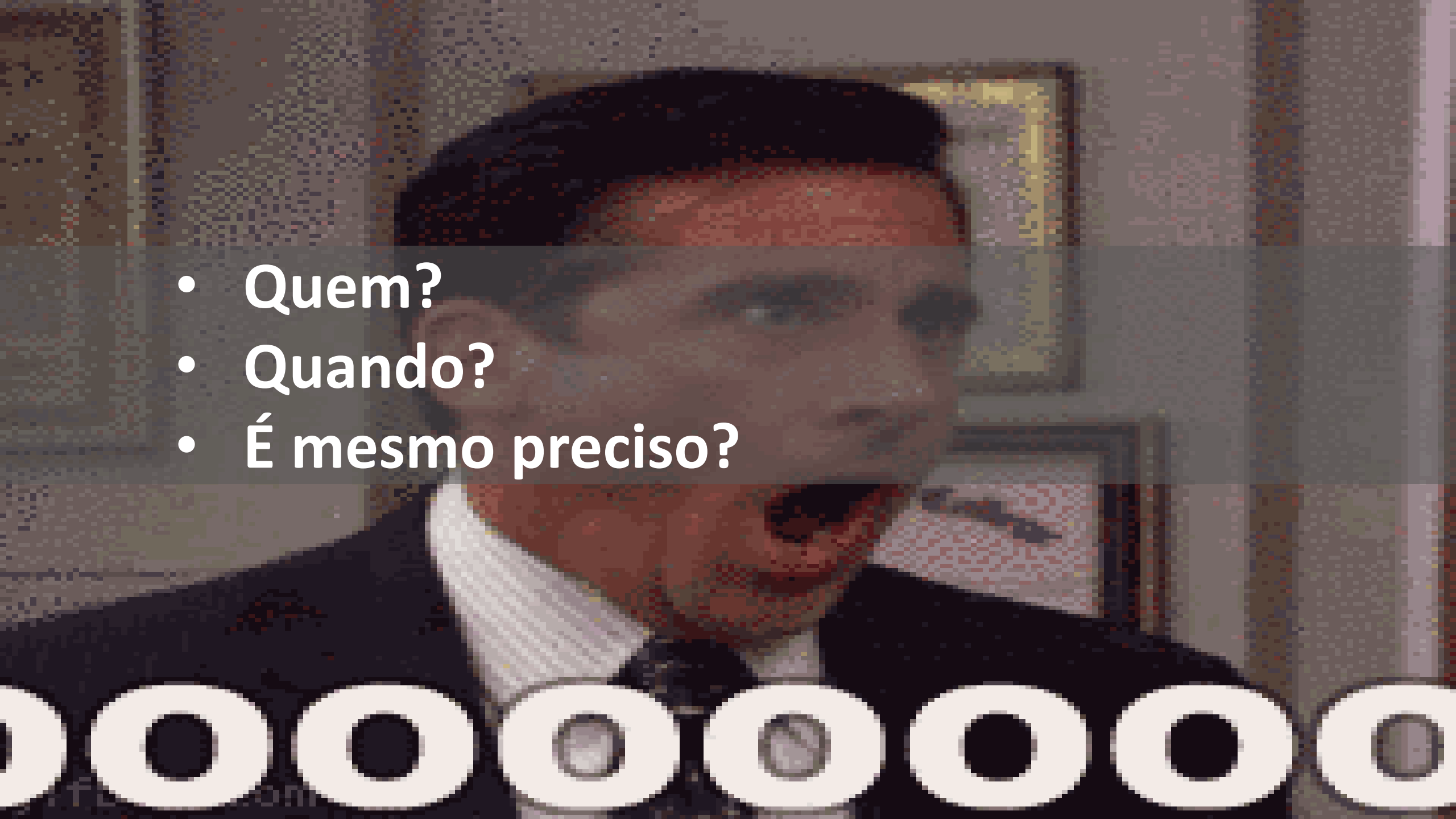
A lion is lying down in a field of tall, golden-brown grass. The lion's head is visible, looking towards the left. The grass is dense and reaches up to the lion's neck. The overall scene is a natural, savanna-like environment.

Os Dados Pessoais:

- Escondidos
- Correlacionados

A close-up photograph of a person's hand holding a pen, positioned over a piece of paper with a drawing. The background is blurred, showing a desk and other papers. A semi-transparent grey horizontal bar is overlaid across the middle of the image, containing the text.

Desenhar um PLANO

- 
- A man in a dark suit and white shirt is shown from the chest up. He has a thoughtful expression, with his hand near his chin. A semi-transparent dark grey box is overlaid on the left side of his face, containing a bulleted list of three questions in white text. The background is a blurred office setting with a framed picture on the wall.
- Quem?
 - Quando?
 - É mesmo preciso?

Cumprir o PLANO

Um exercício de Arte Abstracta:

- Laboral
- Liberdade de Expressão



Urgente:

Informar
Titulares

Preencher
Registo de
Atividades

Nomear DPO

Medidas de
Segurança

Responder a
Pedidos

Notificar
Violações



**MAIS SOLIDARIEDADE
MELHOR SEGURANÇA SOCIAL**

Regulamento Geral de Proteção de Dados



joao.gabriel@micc.pt