Cerejeira Namora Marinho Falcão

an auren member firm

A proteção de dados pessoais em contexto empresarial

Seminário ACIB – Associação Comercial e Industrial de Barcelos – Câmara de Comércio e Indústria

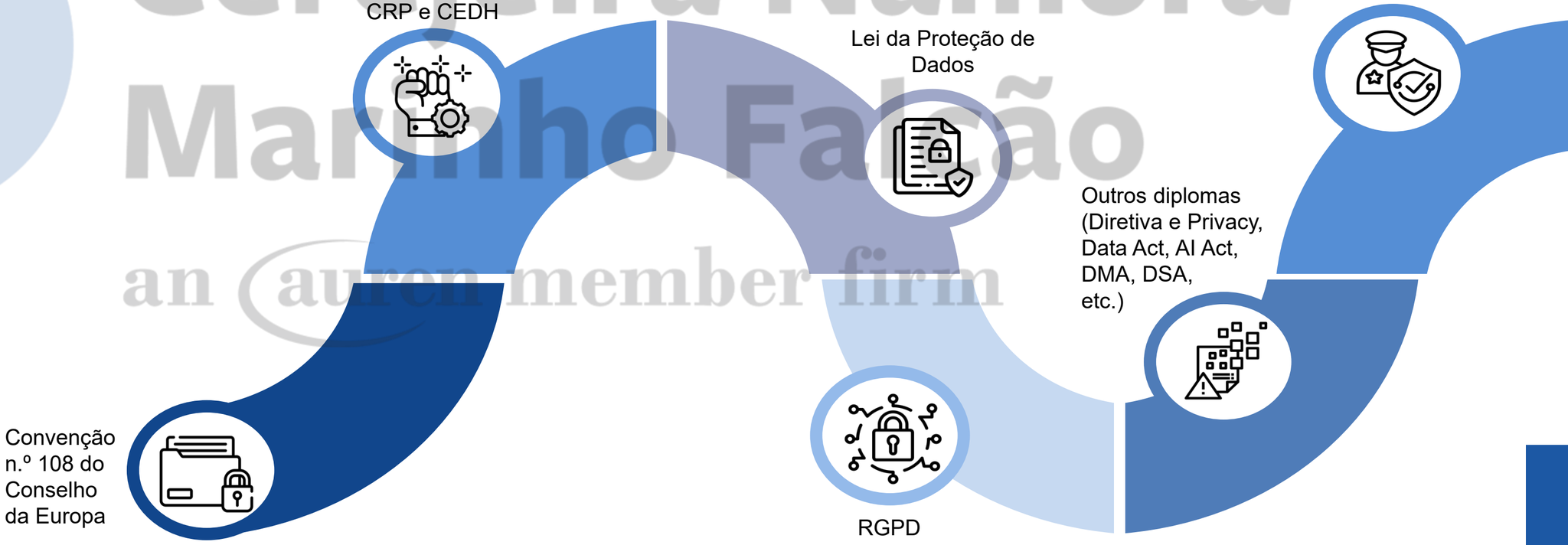
18 de março de 2026

shaping the **future**

Overview

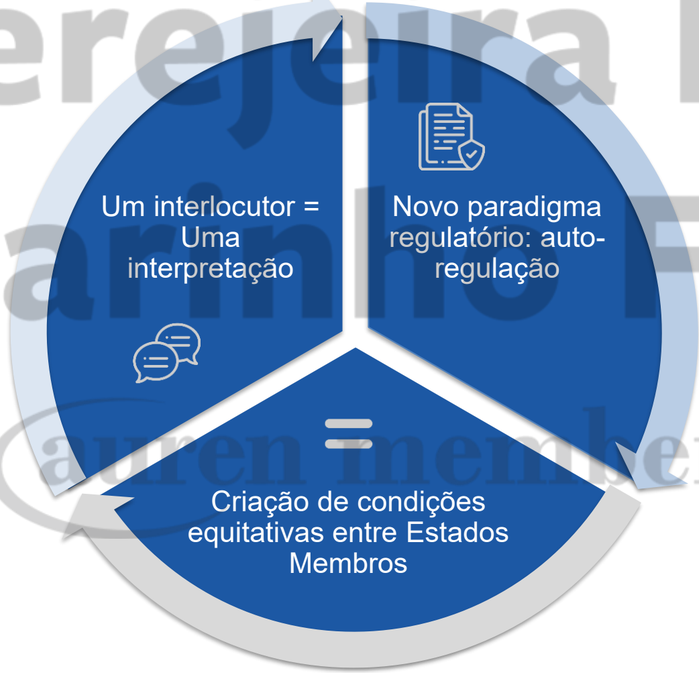
Enquadramento

1 Evolução legislativa



Paradigma regulatório

One-stop-shop



Accountability

2 Conceitos-chave

- **Dados pessoais** – qualquer informação relativa a uma pessoa individual identificada ou identificável (titular dos dados), artigo 4.º, n.º 1 RGPD.
- **Titular dos dados** – pessoa singular que possa ser identificada direta ou indiretamente por referência a um identificador.
- **Tratamento de dados** – operação ou um conjunto de operações efetuadas sobre dados pessoais através de meios automatizados ou não automatizados.

  - Recolha
  - Organização
  - Conservação
  - Alteração
  - Pagamento

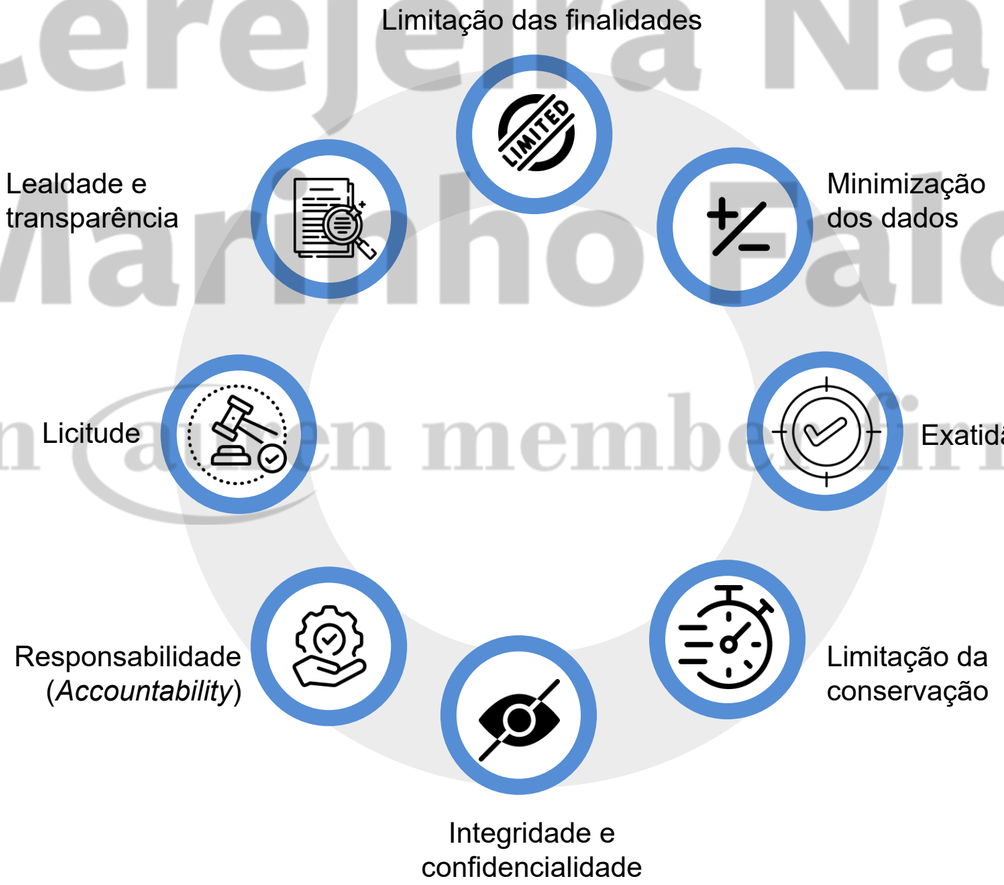
- **Responsável pelo tratamento** – a pessoa singular ou colectiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais

  - Porquê?
  - Como?
  - Para quê?

- **Subcontratante** – uma pessoa singular ou colectiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.
- **Terceiro** – pessoa singular ou colectiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade directa do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais.

Responsável pelo tratamento vs Subcontratante

3 Princípios fundamentais em matéria de protecção de dados



Princípios

Princípio da Licitude

- O tratamento apenas será lícito caso se verifique pelo menos uma das bases de licitude enumeradas anteriormente.

Princípio da Lealdade e Transparência

- o tratamento dos dados deve respeitar a finalidade para a qual os dados foram recolhidos (**leal**) e não se desviar da mesma sem o consentimento do titular;
- o titular dos dados deve conhecer todos os aspectos relativos ao tratamento a que foram sujeitos os seus dados pessoais (**transparente**).

Princípio da Minimização dos Dados

- Apenas devem ser tratados os dados adequados, pertinentes e limitados ao que é estritamente necessário tendo em conta as finalidades para as quais são recolhidos.

Princípio da Limitação das Finalidades

- Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de um modo incompatível com essas finalidades.
- Critérios para avaliar a **compatibilidade das finalidades**:
  - ✓ Ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
  - ✓ O contexto em que os dados foram recolhidos;
  - ✓ As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;
  - ✓ A existência de salvaguardas adequadas, como a cifragem ou a pseudonimização.
- Não se considera incompatível com as finalidades iniciais o tratamento posterior para fins de arquivo de interesse público, fins de investigação científica ou histórica, ou para fins estatísticos.

Princípio da Exactidão

- Os dados recolhidos devem manter-se actualizados, devendo implementar-se todas as medidas adequadas para que os dados inexactos sejam apagados ou rectificados sem demora, tendo sempre em linha de conta as finalidades para as quais os mesmos são tratados.

Princípio da Limitação da Conservação

- Os dados devem ser conservados de um modo que permita a identificação dos respectivos titulares apenas durante o período adequado às finalidades para as quais os mesmos são necessários;
- Os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, para fins de investigação científica/histórica ou para fins estatísticos.

Princípio da Integridade e Confidencialidade

- Manter a segurança dos dados pessoais em qualquer operação de tratamento, adoptando-se medidas técnicas e organizativas que asseguram a protecção contra o seu tratamento não autorizado ou ilícito, contra a sua perda, destruição ou danificação acidental.

Princípio da Responsabilidade/Responsabilização

- Além de ser responsável pelo comprimento dos princípios supra enumerados e das obrigações concretas que deles emanam, o Responsável pelo Tratamento tem de adoptar medidas que na prática permitam **comprovar esse cumprimento**.

Bases de licitude

Consentimento

O titular dos dados autoriza a que lhe seja enviada uma newsletter de uma loja para obter um desconto de 10% numa primeira compra. No entanto, ao fim de um ano, revoga esse consentimento para deixar de receber tantos e-mails.

Contrato

- no qual o titular é parte: A empresa trata dados bancários do trabalhador para processar o salário.
- diligências pré-contratuais a pedido do titular: Um candidato fornece o seu CV e dados pessoais para participar num processo de recrutamento.

Obrigação jurídica do responsável pelo tratamento

O empregador comunica dados de rendimentos e retenções à Autoridade Tributária e à Segurança Social, porque existe uma obrigação legal a impor essa comunicação – artigo 119.º Código do IRS e art.º 40.º do Código dos Regimes Contributivos do Sistema Previdencial de Segurança Social.

Interesses Vitais

Em caso de acidente de trabalho, o empregador fornece dados médicos básicos do trabalhador e os contactos de emergência (de familiares) aos serviços de emergência médica.

Funções de interesse público ou de poderes de autoridade pública de que está investido responsável pelo tratamento

O Governo solicitou ao Serviço Nacional de Saúde dados relativos à vacinação dos cidadãos para analisar a eficácia do plano de vacinação durante a pandemia Covid-19.

Interesses legítimos do responsável pelo tratamento ou de terceiros

A empresa instala um sistema de controlo de assiduidade por biometria e PIN nas suas instalações.

4 Direitos dos titulares dos dados

- **Direito à informação** – têm de ser informados, de forma clara, sobre como e porquê os seus dados são tratados.
- **Direito de acesso** – podem solicitar confirmação de que os seus dados estão a ser tratados e obter uma cópia.
- **Direito de retificação** – permite corrigir dados pessoais incorretos ou incompletos.
- **Direito ao apagamento ("Direito a ser esquecido")** – podem pedir que os seus dados sejam eliminados quando deixarem de ser necessários ou quando retirar o consentimento.
- **Direito à limitação do Tratamento** – possibilidade de restringir temporariamente o uso dos dados.
- **Direito de oposição** – o titular pode opor-se ao tratamento dos seus dados.
- **Direito à portabilidade** – permite receber os dados num formato estruturado e transferi-los para outro responsável pelo tratamento.
- **Direitos relacionados com decisões automatizadas e *profiling*** – podem contestar decisões tomadas exclusivamente por algoritmos e pedir intervenção humana.

Forma

- As comunicações devem ser prestadas forma concisa, transparente, inteligível e de fácil acesso;
- A resposta aos pedidos deve ser prestada:
  - Por escrito; **ou**
  - Oralmente, desde que a identidade do titular seja comprovada por outros meios

Prazo de Resposta

- Um mês a contar da data de recepção do pedido.
- Prazo pode ser prorrogado **até dois meses**, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos.

Se o responsável pelo tratamento recusar o pedido apresentado pelo titular, deve, num prazo de um mês a contar da data de recepção do pedido, informá-lo:

- Das razões que fundamentam a sua recusa; e
- Da possibilidade de apresentar uma reclamação a uma Autoridade de Controlo e intentar acção judicial.

As informações a prestar ao titular de dados são fornecidas **a título gratuito**, **MAS**, se os pedidos forem manifestamente infundados ou excessivos (carácter repetitivo) o **Responsável pelo Tratamento** poderá:

- Exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas; **ou**
- Recusar-se a dar seguimento ao pedido.

NOTA: Cabe ao Responsável pelo Tratamento fazer prova do carácter manifestamente infundado ou excessivo do pedido.

Proteção de dados em contexto empresarial

1 EPD/DPO – Encarregado de Proteção de Dados

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016

Artigo 37.º

1. "O responsável pelo tratamento e o subcontratante **designam um encarregado da protecção de dados** sempre que:
   a) O tratamento for efectuado por uma autoridade ou um organismo público, exceptuando os tribunais no exercício da sua função jurisdicional;
   b) As actividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou
   c) As actividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9.º e de dados pessoais relacionados com condenações penais e infracções a que se refere o artigo 10.º."

Obrigatoriedade de designação

Sector Público

- Estado
  - Por cada Ministério ou Área Governativa
- Regiões Autónomas
  - Por cada Secretaria Regional
- Autarquias Locais
  - Por cada Município
  - Freguesias em que tal se justifique, nomeadamente as com mais de 750 habitantes
- Entidades Supranacionais
- Entidades Administrativas Independentes
- Banco de Portugal
- Institutos Públicos;
- Instituições de Ensino Superior Público;
- Empresas do Sector Empresarial do Estado e dos Sectores Empresariais Regionais e Locais;
- Associações Públicas

Sector Privado

- Actividade principal envolva operações de tratamento que, em virtude da sua natureza ou âmbito, exijam um controlo regular e sistemático dos dados em grande escala **OU**
- Quando a actividade principal consista em operações de tratamento, em larga escala, de categorias especiais de dadose de dados relacionados com condenações penais ou infracções.

Competências e posição dentro da organização

- O EPD/DPO deve ser envolvido de forma adequada e em tempo útil em todas as questões relacionadas com o exercício das suas funções;
- O EPD/DPO deverá reportar ao mais alto nível de gestão ou de administração da organização;
- Têm de ser fornecidos os recursos necessários e acesso à informação;
- O EPD tem de informar diretamente a entidade designadora do andamento das actividades por si desenvolvidas.

NÃO recebe instruções da entidade quanto ao exercício das funções para as quais foi nomeado:

- Definição dos métodos de trabalho;
- Interpretação da legislação aplicável;
- Interpretar as práticas recomendadas no sector.

MAS, **o EPD/DPO NÃO TEM PODER DECISÓRIO**!

NÃO pode ser destituído e/ou e penalizado do pelo exercício correcto e diligente das suas funções.

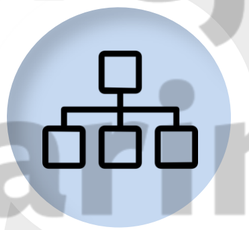
Cerejeira Namora
Marinho Falcão
an auren member firm

Um EPD é essencial para…

- Assegurar conformidade contínua com o RGPD;
- Aconselhar responsáveis e subcontratantes sobre obrigações legais, bases de licitude e boas práticas;
- Avaliar riscos e apoiar AIPDs;
- Promover medidas de segurança e mitigação, articulando com equipas técnicas e de gestão;
- Facilitar auditorias internas e externas;
- Ser ponto de contacto com a CNPD;
- Gerir pedidos dos titulares, garantindo respostas eficazes, completas e dentro dos prazos legais;
- Acompanhar subcontratantes e transferências internacionais, verificando salvaguardas e contratos;
- Prevenir incidentes e sanções;
- Promover uma cultura de proteção de dados, sensibilizando colaboradores e integrando a privacidade nos processos.

2 Acordos de tratamento de dados

Acordo de subcontratação



Acordo de partilha de dados

Acordo de responsabilidade conjunta

Cerejeira Namora Marinho Falcão an auren member firm

Acordos de subcontratação

- **Artigo 28.º do regulamento EU 679/2016**

  3. O tratamento em subcontratação é **regulado por contrato ou outro acto normativo** ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objecto 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.

  - **Contrato negociado entre as partes**
  - **Cláusulas contratuais gerais**

- **Conteúdo obrigatório:**
  - Objecto
  - Duração
  - Natureza e finalidade do tratamento
  - Categoria de dados pessoais
  - Categorias de titulares de dados
  - Obrigações e Direitos das partes

- **Conteúdo facultativo:**
  - Instruções para o tratamento;
  - Dever de sigilo e confidencialidade
  - Medidas de segurança
  - Modo de exercício dos direitos dos titulares
  - Cooperação no cumprimento das obrigações do Responsável
  - Destino dos dados no fim da subcontratação
  - Regulação da subcontratação ulterior

Subcontratação ulterior:

2. O subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, **previamente e por escrito**, **autorização específica ou geral**. Em caso de 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**.

- **Autorização Específica**
- **Autorização Geral**

NOTA: o incumprimento desta obrigação constitui uma contra-ordenação grave – artigo 38.º, n.º 1 al. f) da Lei n.º 58/2019.

Cerejeira Namora
Marinho Falcão
an auren member firm

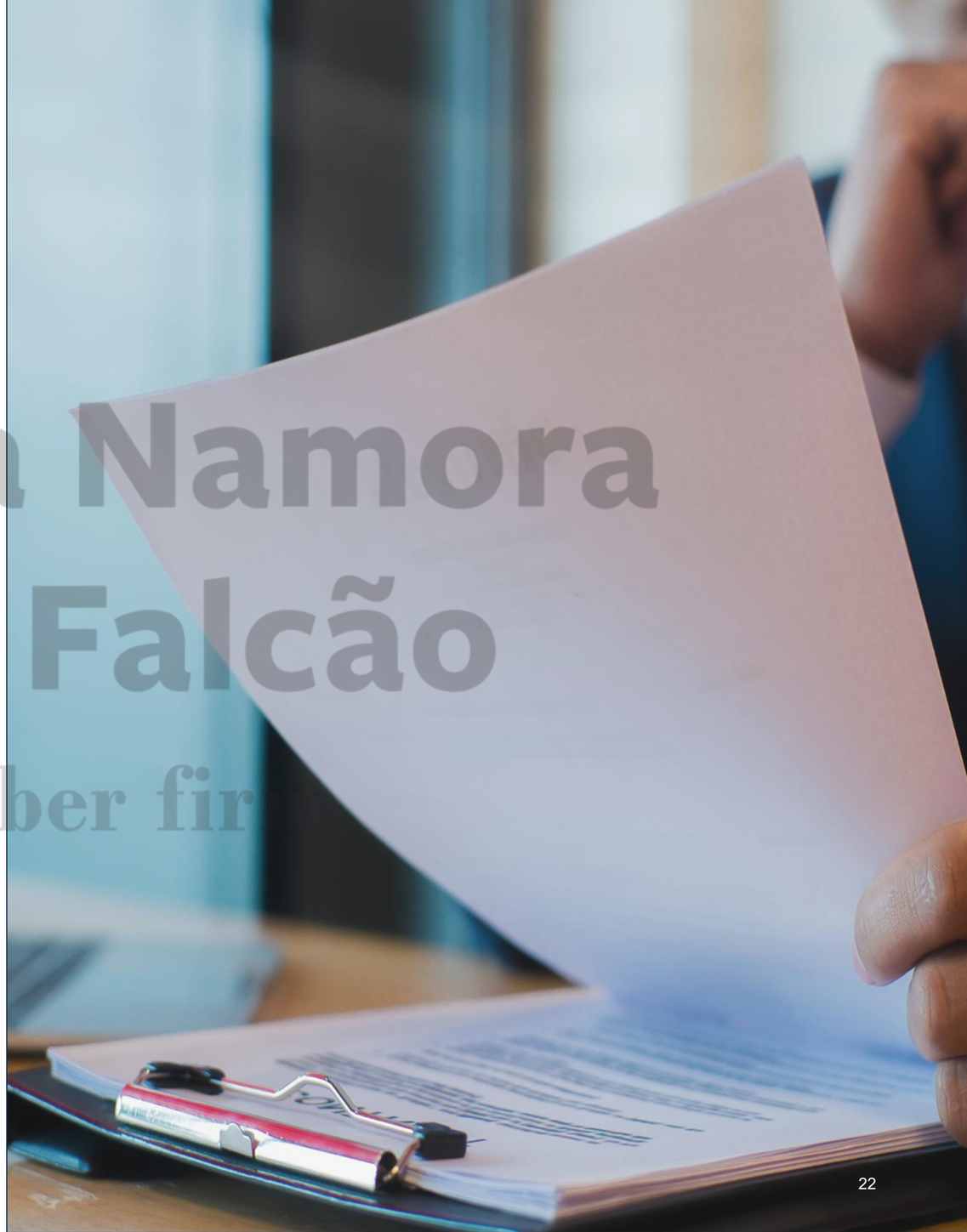
Acordo de co-responsabilidade

- **Artigo 26.º do regulamento EU 679/2016**
  - Duas organizações determinam conjuntamente os meios e as finalidades do tratamento;
  - Determinação por acordo entre si e de modo transparente as responsabilidades pelo cumprimento da regras previstas no Regulamento:
    - Exercício dos direitos do titular dos dados;
    - Cumprimento do dever de informação;
    - Funções e relações respectivas dos responsáveis conjuntos pelo tratamento em relação aos titulares dos dados.

A essência do acordo é disponibilizada ao titular dos dados.

NOTA 1: O titular dos dados pode exercer os direitos que lhe confere o presente regulamento em relação e cada um dos responsáveis pelo tratamento.

NOTA 2: o incumprimento desta obrigação constitui uma contra-ordenação grave – artigo 38.º, n.º 1 al. d) da Lei n.º 58/2019.



3 RAT – Registo de Atividades de Tratamento

Artigo 30.º do regulamento EU 679/2016

Cada Responsável pelo Tratamento e/ou subcontratante conservam um registo de todas as actividades de tratamento sob a sua responsabilidade.

Obrigatório?

- Empresas/organizações com mais de 250 trabalhadores;
- No caso de empresas/organizações com menos de 250 trabalhadores, o registo é obrigatório:
  - Há tratamento regular de dados pessoais;
  - O tratamento é susceptível de pôr em risco os DLGs dos titulares; **OU**
  - Haja tratamento de categorias especiais de dados ou de dados relativos a condenações penais e infracções

Elementos obrigatórios do RAT

- Finalidade do tratamento
- Categorias de dados pessoais
- Dados de contacto
- Titulares dos dados
- Bases de licitude
- Quem tem acesso
- Partilha de dados
- Envolvimento de terceiros
  - Subcontratantes
  - Transferências internacionais
- Prazos de conservação
- Medidas de segurança

NOTA: o incumprimento desta obrigação constitui uma contra-ordenação grave – artigo 38.º, n.º 1 al. h) da Lei n.º 58/2019.

O responsável pelo tratamento/ subcontratante estão obrigados a facultar o registo à autoridade de controlo, mediante solicitação.

O RAT é essencial para…

- Identificar quem trata os dados;
- Definir finalidades e base legal;
- Mapear riscos e operar medidas de segurança;
- Demonstrar conformidade com a lei;
- Facilitar auditorias;
- Responder de forma eficaz a pedidos de acesso;
- Gerir subcontratantes e transferências internacionais;
- Evitar sanções;
- Promover cultura de proteção de dados.

4 AIPD – Avaliação de Impacto sobre a Proteção de Dados

Artigo 35.º do Regulamento EU 679/2016

1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for susceptível de **implicar um elevado risco para os direitos e liberdades das pessoas singulares**, o Responsável pelo Tratamento procede, **antes de iniciar o tratamento**, a uma avaliação de impacto das operações de tratamento previstas sobre a protecção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.

HETERORREGULAÇÃO VS. AUTORREGULAÇÃO

Realização obrigatória:

- Actividades de tratamento forem *"susceptíveis de implicar um elevado risco para os direitos e liberdades das pessoas singulares".*
- Avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares;
- Operações de tratamento em grande escala de categorias especiais de dados (p. ex.: dados biométricos, dados de saúde) **ou** de dados pessoais relacionados com condenações penais e infracções;
- Controlo sistemático de zonas acessíveis ao público em grande escala;
- **Regulamento n.º 1/2018 da CNPD** (lista de actividades de tratamento de dados sujeitos a AIPD).

Em que consiste uma AIPD?

- Descrição da(s) actividade(s) de tratamento de dados pessoais;
- Avaliação a sua licitude, necessidade e proporcionalidade; e
- Mitigação dos riscos para os titulares.

O papel do EPD/DPO:

- Avaliar a necessidade de efectuar AIPD;
- Definir a metodologia a seguir na sua realização;
- Indicar as salvaguardas (incluindo medidas técnicas e organizativas) a aplicar no sentido de atenuar os eventuais riscos para os direitos e interesses dos titulares de dados;
- Elaborar parecer fundamentado (obrigatório!)

Metodologia:

- Enquadramento da solução
- Fundamentação da necessidade de AIPD
- Tipos e Categorias de Dados Pessoais envolvidos
- Finalidade e licitude do tratamento de dados
- Proporcionalidade e Necessidade de Utilização

- Medidas de Segurança na Utilização
  - Aplicação *in casu* dos Princípios (!)

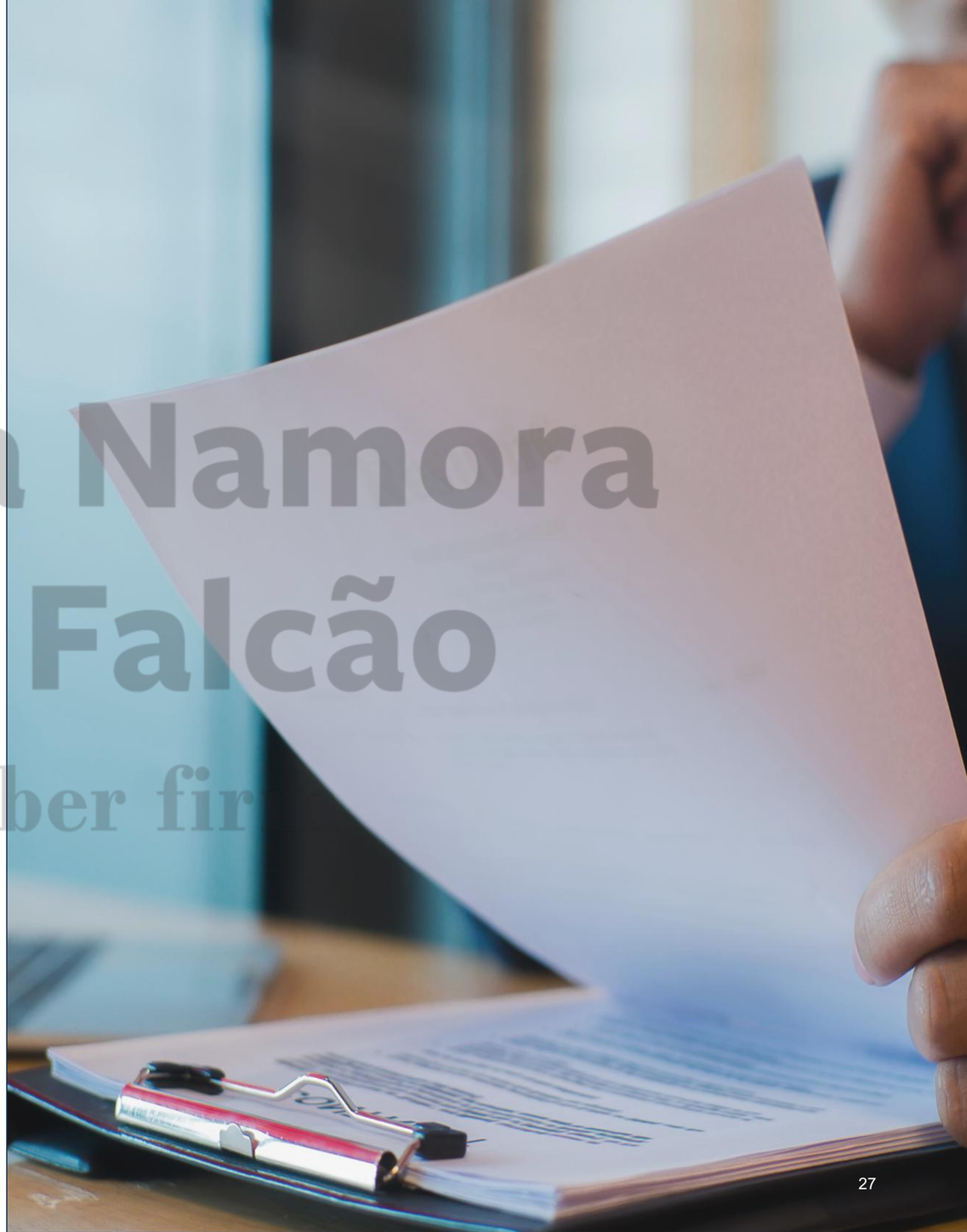
- Direitos dos titulares e gestão do seu exercício
- Termos do Tratamento
  - Incluindo a identificação de (eventuais) Subcontratantes e/ou Subcontratantes ulteriores;
  - Intervenção e regulação das responsabilidades entres estes;
  - Transferências internacionais;
  - Prazos de Conservação;
  - Efectivação e responsabilidade de gestão dos exercícios de direitos.
- Parecer do EPD/DPO
- Anexos (Declarações de conformidade de software/hardware, Acordo de Subcontratação, Instruções documentadas, Medidas técnicas e organizativas dos Subcontratantes, ...)

Cerejeira Namora
Marinho Falcão
an auren member firm

Consulta prévia à CNPD?

- De acordo com o n.º 1 e n.º 2 do artigo 36.º e com a alínea l) do n.º 1 do artigo 57.º do Regulamento, é possível submeter a Avaliação de Impacto para a Protecção de Dados a consulta prévia da CNPD sempre que:
  - A AIPD indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo Responsável pelo Tratamento para atenuar o risco, **i.e.**, há dúvidas quanto a legitimidade, adequação e segurança do tratamento.

NOTA: Este procedimento não se confunde com as anteriores autorizações de tratamento. É meramente consultivo e não tem carácter vinculativo.



5 Violações de dados pessoais

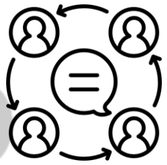
VIOLAÇÃO DE DADOS PESSOAIS: uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

- **Violação da confidencialidade** – quando existe uma divulgação ou acesso acidental ou não autorizado a dados pessoais;
- **Violação da integridade –** quando existe uma alteração acidental ou não autorizada dos dados pessoais;
- **Violação da disponibilidade –** quando existe uma perda ou a destruição acidental ou não autorizada de dados pessoais.

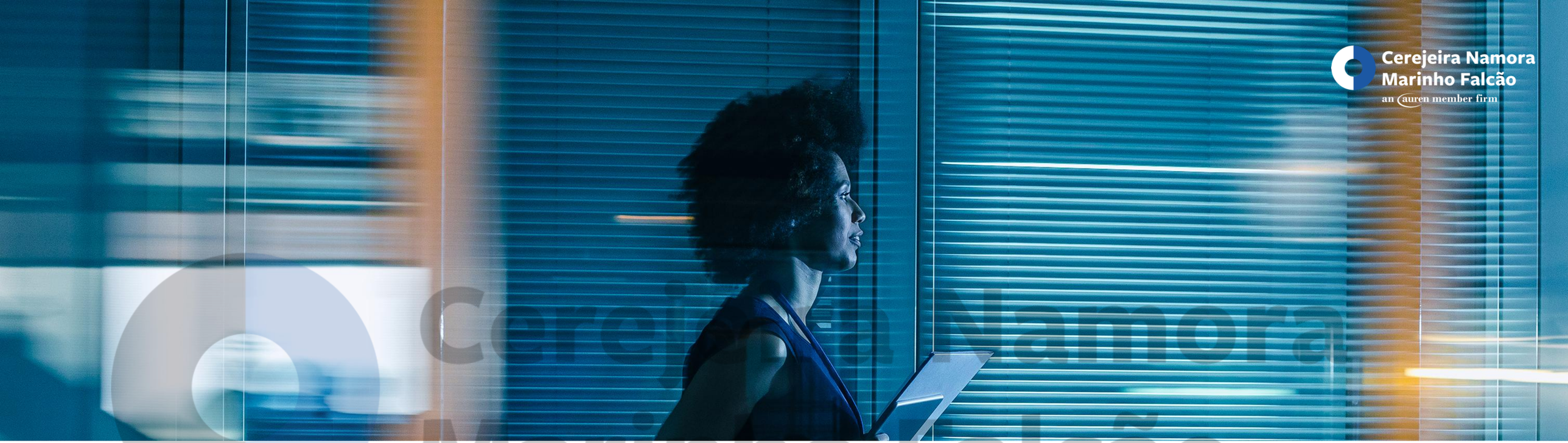
REAÇÃO:

- **Notificação da violação de dados à autoridade de controlo:**
  - Logo que exista um grau razoável de certeza sobre a existência de uma violação de dados, o Responsável pelo Tratamento tem de notificar a Comissão Nacional de Protecção de Dados Pessoais no prazo máximo de 72h após ter conhecimento da mesma.

Formulário disponibilizado no website da CNPD - https://www.cnpd.pt/DataBreach/.



- **Comunicação da violação aos titulares dos dados:**
  - Sempre que for susceptível de implicar um elevado risco para os seus direitos e liberdade;
  - Caso a comunicação individual implique um esforço desproporcional, basta um comunicado público ou uma medida semelhante que permita informar os titulares dos dados de forma eficaz;
  - Descrever a natureza da violação; nome e contactos do EPD; descrição das consequências; descrição das medidas adotadas.



Proteção de dados pessoais no âmbito laboral

1 Videovigilância

- **As câmaras não podem incidir sobre**:
  - Vias públicas, propriedades limítrofes ou outros locais que não sejam do domínio exclusivo do responsável, exceto no que seja estritamente necessário para cobrir os acessos ao imóvel;
  - A zona de digitação de códigos de caixas multibanco ou outros terminais de pagamento ATM;
  - O interior de áreas reservadas a clientes ou utentes onde deva ser respeitada a privacidade, designadamente instalações sanitárias, zonas de espera e provadores de vestuário;
  - O interior de áreas reservadas aos trabalhadores, designadamente zonas de refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetas ao seu descanso.
- Nos **estabelecimentos de ensino**, as câmaras de videovigilância só podem incidir sobre os perímetros externos e locais de acesso, e ainda sobre espaços cujos bens e equipamentos requeiram especial proteção, como laboratórios ou salas de informática.
- **Proibida a captação de som**, exceto no período em que as instalações vigiadas estejam encerradas **ou** mediante autorização prévia da CNPD.
- Conservação das imagens em registo codificado, pelo prazo de 30 dias contados desde a respetiva captação, findo o qual são destruídas, no prazo máximo de 48 horas.
- Pessoas com acesso às gravações **devem sobre as mesmas guardar sigilo**, sob pena de procedimento criminal.
- Proibida a cessão ou cópia das gravações , só podendo ser utilizadas nos termos da legislação processual penal.

Procedimentos a adoptar:

- **Elaboração obrigatória de uma Avaliação de Impacto sobre Protecção de Dados Pessoais:**
  - Controlo sistemático de zonas de acesso ao público
  - Existência de risco significativo para os direitos e liberdades fundamentais dos trabalhadores, prestadores de serviços, utentes e quaisquer pessoas singulares que possam frequentar as zonas.

- **Cumprimento do dever de informação:**
  - Existência e localização das câmaras de vídeo;
  - A menção *"Para sua protecção este local é objecto de videovigilância"*;
  - A entidade de segurança privada autorizada a operar o sistema, pela menção do nome e alvará/licença;
  - O responsável pelo tratamento dos dados recolhidos perante quem os direitos de acesso e rectificação podem ser exercidos – Responsável pelo Tratamento.
  - Uso de simbologia adequada que consiste *"num sinal em forma de triângulo, em fundo de cor amarela com orla interior em cor preta, ao centro, símbolo representando o pictograma de uma câmara de videovigilância em cor preta".*

No âmbito laboral…

- O sistema de CCTV não pode ser utilizado para controlar o desempenho profissional do trabalhador.

- Os trabalhadores devem ser informados sobre a existência de um sistema de CCTV no seu local de trabalho e das especificidades do mesmo.

- As imagens obtidas através da utilização dos sistemas de videovigilância poderão ser utilizadas pelo empregador no âmbito de procedimentos disciplinares, desde que:
  - Essas imagens tenham sido usadas em processo criminal e;
  - O procedimento disciplinar vise apurar a responsabilidade do trabalhador pelos factos relativos ao processo crime.

2 Tratamento de dados no recrutamento

- Tratamento dos dados pessoais do candidato e comunicações são efectuadas com base num interesse legítimo do Responsável pelo Tratamento/diligências pré-contratuais a pedido do Titular;

- No caso de haver manutenção dos dados do candidato para processos de recrutamento futuros, o candidato deve ser informado.
  As plataformas eminentemente profissionais ou de recrutamento:
  - Prossecução de interesse legítimo, onde há uma clara expectativa do (potencial) candidato em ser contactado para esse efeito.

- Conservar os CVs por um período não superior a **1 ano** com base no interesse legítimo do empregador/Responsável pelo Tratamento.

  - Durante esse período a candidatura pode ser integrada em eventuais processos de recrutamento;
  - Findo o período de conservação implementado, os CVs e todos os dados do candidato devem ser eliminados e destruídos de forma permanente.
  - Período **superior a 1 ano**: Obtenção do consentimento.

3 Controlo de consumo de substâncias psicotrópicas

- **Regra geral:** Proibição da entidade empregadora exigir aos seus trabalhadores a realização ou apresentação de testes ou exames médicos para comprovação das suas condições físicas ou psíquicas;
  - Direito dos trabalhadores a prestarem trabalho em condições de segurança e saúde;
  - Obrigação da entidade empregadora de assegurar a vigilância da saúde dos trabalhadores, devendo, para o efeito, vigiar as condições de trabalho e preservar a saúde dos trabalhadores em situações mais vulneráveis.

- **Finalidade da realização do exame:**
  - Destinam-se exclusivamente a verificar a aptidão do trabalhador para o desempenho das suas funções e só podem ser efectuados no estrito cumprimento da lei.
  - A finalidade do tratamento dos dados tem de ser necessariamente subsumida à medicina preventiva e curativa.
  - O consumo de substâncias psicoactivas em si não constitui justa causa de despedimento, mas antes o comportamento que dali, eventualmente, possa ser subsumido no âmbito do disposto no artigo 351.º do Código de Trabalho.

- **Procedimento a adoptar:**
  - Realização obrigatória de uma AIPD

Cerejeira Namora
Marinho Falcão
an auren member firm

Trabalhadores abrangidos

- Trabalhadores cuja actividade possa colocar em perigo a sua integridade física ou de terceiros.
- Exercício de funções que envolvam especiais riscos para os próprios trabalhadores, para terceiros ou para a sociedade em geral.

Que profissionais podem realizar os testes?

- Solicitação e/ou responsabilidade do médico do trabalho;
- O tratamento dos dados de saúde deve ser efectuado por um profissional obrigado a sigilo ou por outra pessoa sujeita a dever de confidencialidade (29.º/2 da Lei 58/2019 + 9.º/2/ h) e i) do RGPD).

Dever de informação

- A justificação da realização de exames de alcoolemia deverá ser prestada, por escrito, ao trabalhador.
- Informação deverá ser prestada através da existência de **regulamento interno**, do conhecimento dos trabalhadores, garantindo-se assim a possibilidade de oposição por parte destes, de forma clara e esclarecida

Sigilo

- A informação resultante do exame realizado deverá ser de acesso restrito ao médico do trabalho ou, sob a sua direcção e controlo, a outros profissionais de saúde obrigados a sigilo.
- Em caso algum a informação poderá ser comunicada ao empregador, apenas lhe sendo dado conhecimento do estado de aptidão do trabalhador, em termos de apto, não apto ou ainda, apto com restrições.

Direitos dos trabalhadores:

- O trabalhador tem direito à realização de contraprova através de exame médico para confirmação dos resultados e exame médico pericial.
- Os custos referentes à contraprova e à detecção são sempre da responsabilidade da entidade patronal.

4 Geolocalização

Artigo 21.º Código do Trabalho

1. A utilização de meios de vigilância a distância no local de trabalho está sujeita a **autorização da Comissão Nacional de Protecção de Dados**.
2. A autorização só pode ser concedida se a utilização dos meios for necessária, adequada e proporcional aos objectivos a atingir.
3. Os dados pessoais recolhidos através dos meios de vigilância a distância são conservados durante o período necessário para a prossecução das finalidades da utilização a que se destinam, devendo ser destruídos no momento da transferência do trabalhador para outro local de trabalho ou da cessação do contrato de trabalho.

MAS, a CNPD já não tem poderes de autorização, nem de fiscalização prévia…

↓

Avaliação de Impacto sobre a Protecção de Dados Pessoais
Deliberação n.º 7680/ 2014

Finalidades admissíveis para o tratamento de dados relativos à geolocalização:

- Gestão da frota em serviço externo: nas áreas de actividade de assistência técnica externa/ao domicílio; distribuição de bens; transporte de passageiros; transporte de mercadorias; segurança privada.
- Protecção de bens: transporte de materiais perigosos e transporte de materiais de valor elevado

5 Tratamento de dados biométricos

Artigo 18.º Código do Trabalho

1. O empregador só pode tratar dados biométricos do trabalhador após notificação à Comissão Nacional de Protecção de Dados.
2. O tratamento de dados biométricos só é permitido se os dados a utilizar forem necessários, adequados e proporcionais aos objectivos a atingir.
3. Os dados biométricos são conservados durante o período necessário para a prossecução das finalidades do tratamento a que se destinam, devendo ser destruídos no momento da transferência do trabalhador para outro local de trabalho ou da cessação do contrato de trabalho.

Artigo 28.º Lei n.º 58/2019

O tratamento de dados biométricos dos trabalhadores só é considerado legítimo para controlo de assiduidade e para controlo de acessos às instalações do empregador.

Procedimento a adoptar:

- Realização obrigatória de uma AIPD
- Requisitos mínimos obrigatórios quanto ao hardware e software utilizado;
  - Hardware só pode recolher uma representação dos dados biométricos;
  - Software não permite a reversibilidade dos dados.

Meios de tutela

1 Regime contraordenacional

O artigo 83.º RGPD determina os valores mínimos e máximos para essas sanções e estabelece que cada autoridade de controlo assegura a aplicação de coimas.

A Lei n.º 58/2019 estabelece critérios, atendendo à dimensão das entidades, para a atribuição de coimas para contra-ordenações graves e muito graves.

No entanto, a CNPD, pela Deliberação 494/2019, determina que aplica as coimas de acordo com o previsto no RGPD, apenas aplicando o estabelecido no artigo 37.º e 38.º da Lei n.º 58/2019 para sanções **não** previstas no RGPD.

Lei n.º 58/2019 RGPD

CONTRA-ORDENAÇÕES MUITO GRAVES	CONTRA-ORDENAÇÕES GRAVES
20 milhões de euros ou 4% do volume de negócios	**10 milhões de euros ou 2% do volume de negócios**
Grande empresa – De 2500 € a 10 000 000 € ou 2% do volume de negócios anual, a nível mundial, conforme o que for mais elevado;	**Grande empresa –** De 2500 € a 10 000 000 € ou 2% do volume de negócios anual, a nível mundial, conforme o que for mais elevado;
PMEs – De 1000 € a 1 000 000 € ou 2% do volume de negócios anual, a nível mundial, conforme o que for mais elevado.	**PMEs –** De 1000 € a 1 000 000 € ou 2% do volume de negócios anual, a nível mundial, conforme o que for mais elevado.
Pessoas Singulares – De 500€ a 250 000€.	**Pessoas Singulares –** De 500€ a 250 000€.

Cerejeira Namora Marinho Falcão an auren member firm

Problemas

- Afastamento a punibilidade da conduta negligente
  - Artigo 37.º, n.º 1 a) do qual resulta que a negligência não é punível em caso de violação dos princípios previstos no artigo 5.º do RGPD.

- Alteração dos limites máximos e limites mínimos de coima

- Critério de ponderação de medida da pena
  - Artigo 39.º n.º 3 que determina que, excepto em caso de dolo, a CNPD só pode instaurar processos de contra-ordenação se advertir previamente o agente, *para cumprimento da obrigação omitida ou reintegração da proibição violada em prazo razoável*.

Comissão Nacional de Protecção de Dados
DELIBERAÇÃO/2019/494

↓

Princípio do Primado do Direito da União Europeia

2 Responsabilidade criminal

Lei n.º 58/2019

- A Lei interna tipifica 7 crimes no que respeita ao tratamento de dados pessoais;
  - **Acesso indevido; desvio de dados; violação de dever de sigilo.**
- A tentativa é sempre punível;
- Responsabilidade penal das pessoas colectivas (com excepção do Estado e de pessoas colectivas que exerçam prerrogativas de poder público).

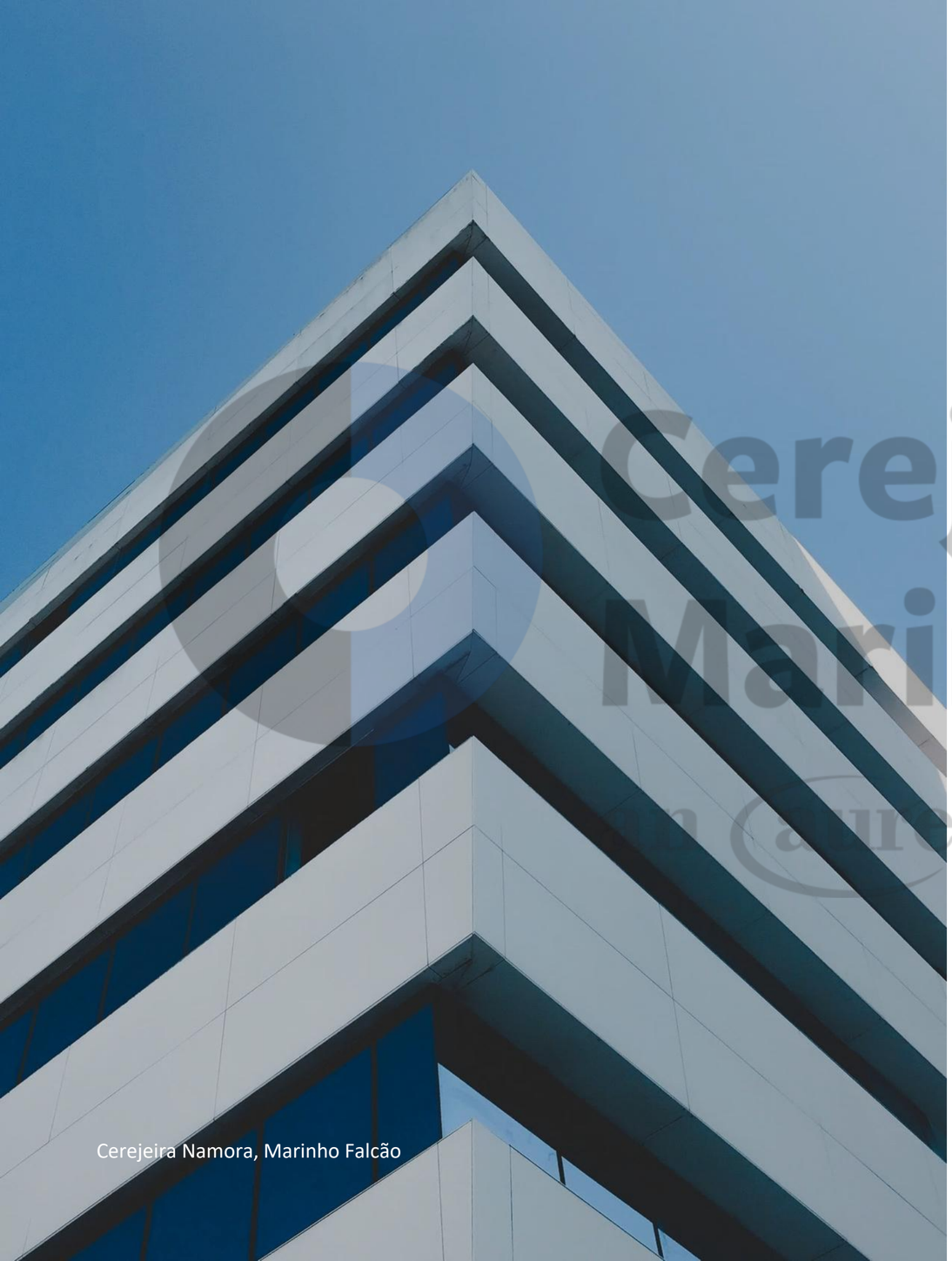
3 Direito de indemnização

Artigo 82.º RGPD

- Os titulares têm direito a indemnização por danos materiais ou imateriais resultantes de violação do RGPD.
- Responsável pelo tratamento responde por danos causados por tratamentos ilícitos.
- Subcontratante responde apenas se violar obrigações que lhe são dirigidas ou instruções lícitas do responsável.
- Exoneração de responsabilidade: possível se provar que não teve qualquer responsabilidade no evento que originou os danos.
- Responsabilidade solidária quando vários responsáveis/subcontratantes participam no mesmo tratamento.
- Quem pagar a indemnização pode reclamar aos restantes a parte correspondente à sua responsabilidade.

Desafios

- **Consciencialização** – noção de importância e promoção da cultura de proteção de dados;
- **Conhecimento** – obrigações legais, intervenientes e papéis a desempenhar e funções;
- ***Compliance*** – políticas adequadas e atualizadas; conhecer sanções aplicáveis;
- **Medidas técnicas e organizativas** – ações a adotar para mitigação de riscos e sanação de irregularidades;
- **Gestão de recursos** – conciliar recursos financeiros e humanos para *compliance* em matéria de dados.



Cerejeira Namora, Marinho Falcão

Cerejeira Namora Marinho Falcão an auren member firm

Compliance

Mapeamento da Informação	▪ RECOLHER informação ▪ IDENTIFICAR actividades de tratamento ▪ IDENTIFICAR os fluxos de informação
Gap Analysis	▪ IDENTIFICAR riscos ▪ RECOMENDAR medidas de mitigação ▪ RELATÓRIO DE CONFORMIDADE
Roadmap	▪ PLANO DE IMPLEMENTAÇÃO
Ongoing	▪ REAVALIAR a conformidade ▪ AUDITORIAS

Contactos

Gonçalo Cerejeira Namora
Sócio
gcn@cnmf.pt

Rafaela Pinheiro Fernandes
Associada Principal
rpf@cnmf.pt

Siga-nos nas redes sociais