LABORATÓRIO DE INSTRUMENTAÇÃO
E FÍSICA EXPERIMENTAL DE PARTÍCULAS
partículas e tecnologia

Proteção de dados e boas práticas de utilização em TI

parte 1: Regulamento Geral de Proteção de Dados

Esta apresentação:

- *é apenas um sumário do regulamento,*
- *baseada na minha perceção pessoal,*
- *pretende sensibilizar para a legislação,*
- *não é representativa da posição do LIP,*
- *não dispensa a leitura atenta da legislação.*

A legislação já está em força

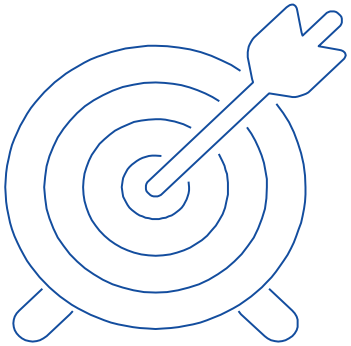
Hospital do Barreiro multado em 400 mil euros por permitir acessos indevidos a processos clínicos.

Coima ao abrigo do novo Regulamento Geral de Proteção de Dados aplicada pela CNPD em Outubro de 2018.

A legislação já está em força

- Queixa da ordem dos médicos
- Médicos que já não estavam no quadro tinham acesso aos repositórios clínicos.
- Agentes sociais com acesso aos repositórios clínicos.
- Falta de regras de acesso.

Coimas



- **Máximo → previsto pela CE**
  - **20.000.000 € (20 milhões)**
  - **4% do volume global de negócios**
- **Mínimo → grave em PT**
  - **1.000€ PME**
  - **2.500€ grandes empresas**
  - **500€ pessoas singulares**
- **Mínimo → muito grave em PT**
  - **2.000€ PME**
  - **5.000€ grande empresa**
  - **1.000€ pessoas singulares**
- **Pode incluir prisão até dois anos**

Coimas outros exemplos

- Facebook Cambridge Analytica
  - 500.000 £
- Equifax ocorrência de roubo de dados
  - 500.000 £
- TalkTalk SQL injection roubo de dados
  - 400.000 £
- Keurboom telefonemas s/ consentimento
  - 400.000 £
- UBER não informou clientes de roubo
  - 385.000 £
- Brighton Sussex Hospital discos com dados dos pacientes vendidos
  - 325.000 £
- Rede social usa passwords não encriptadas
  - 20.000 €
- Um café por videovigilância ilegal
  - 5.200 €
- Google por falta de consentimento
  - 50.000.000 €

LABORATÓRIO DE INSTRUMENTAÇÃO
E FÍSICA EXPERIMENTAL DE PARTÍCULAS
partículas e tecnologia

Sobre o RGPD

Regulamento Geral de Proteção de Dados
RGPD

- Proteção de dados pessoais de pessoas singulares de qualquer nacionalidade
- Valido em toda a União Europeia
- Regulamento valido independentemente de ser transposto (não é uma diretiva)
- Valido para entidades fora da União Europeia que processem dados relativos a sujeitos da União Europeia
- Para dados digitais e em papel
- Entrou em força a 25 de Maio de 2018

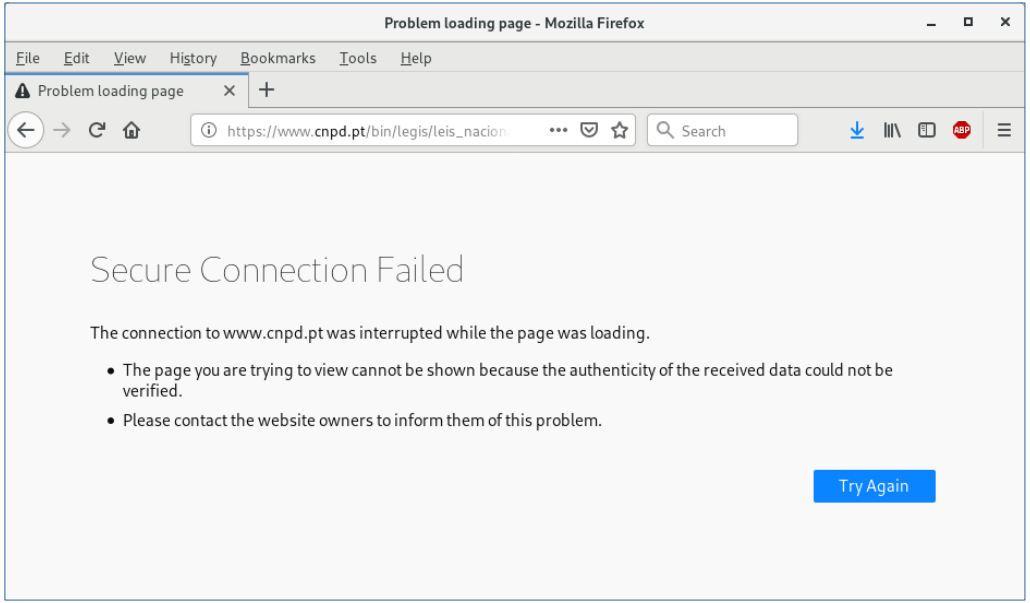
https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT

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

Regulamento Geral de Proteção de Dados
RGPD

- Comissão Nacional de Proteção de Dados (CNPD)

- www.cnpd.pt



Limites da aplicação do RGPD

- Não se aplica:
  - Ao processamento de dados pessoais no curso de atividades pessoais ou domésticas
  - Portanto sem relação com atividade profissional ou comercial
  - Não se aplica à segurança nacional e tribunais
  - Exercício da liberdade de expressão, informação e imprensa, incluindo jornalismo, expressão académica, artística e literária
- Aplica-se:
  - Atividade profissional e comercial

Dados pessoais

Informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

LABORATÓRIO DE INSTRUMENTAÇÃO
E FÍSICA EXPERIMENTAL DE PARTÍCULAS
partículas e tecnologia

O regulamento

Princípios do RGPD

- Os dados pessoais devem:
  - Processados para propósitos específicos, explícitos e legítimos
    - de forma adequada e limitada ao necessário
    - mantidos atualizados e precisos
  - Mantidos de forma que permita identificação do sujeito ...
    - ... apenas durante o tempo estritamente necessário
  - Processados de forma segura, protegidos contra:
    - acesso não autorizado, danos e destruição

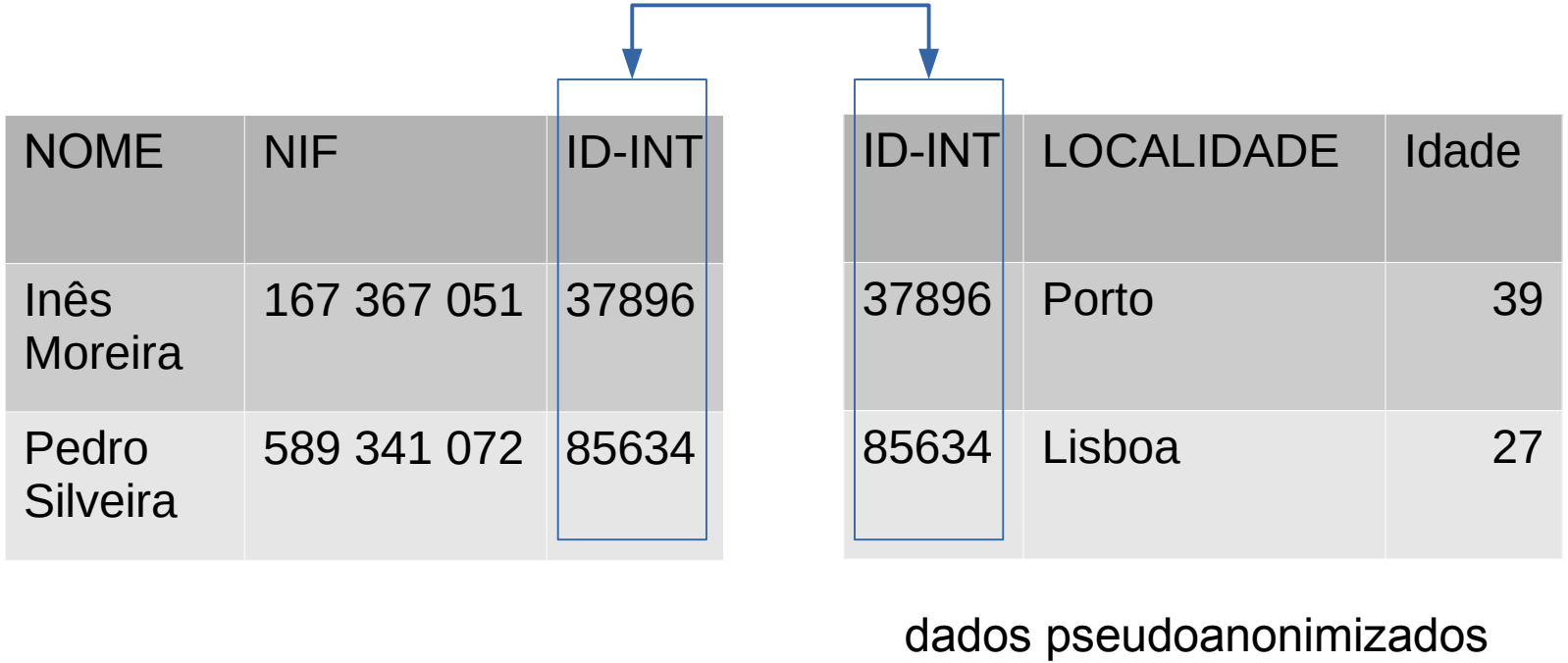
Pseudoanonimização e anonimização

- Dados que tenham passado por pseudoanonimização e portanto possam ainda ser associados a um sujeito continuam a ser dados pessoais => RGPD

- Sempre que exista informação que permita a associação dos dados ao sujeito os dados são pessoais => RGPD

- RGPD não se aplica a informação anonimizada e que portanto não permita a identificação do sujeito

Pseudoanonimização



NOME	NIF	ID-INT
Inês Moreira	167 367 051	37896
Pedro Silveira	589 341 072	85634

ID-INT	LOCALIDADE	Idade
37896	Porto	39
85634	Lisboa	27

dados pseudoanonimizados

Anonimização

NOME	NIF	ID-INT
X000001	000 000 000	37896
X000002	000 000 000	85634

ID-INT	LOCALIDADE	IDADE
37896	Porto	39
85634	Lisboa	27

dados anonimizados

Identificadores

- Identificadores de dispositivos, aplicações, ferramentas e protocolos quando permitam a identificação do sujeito são dados pessoais => RGPD
  - Tracking Cookies
  - Endereços IP
  - Endereços MAC (ethernet, wifi, etc)
  - RFIDs
  - etc

Limite temporal

- O tempo de armazenamento dos dados deve ser o mínimo estritamente necessário para o propósito
- Limites temporais têm de ser estipulados e tornados conhecidos
- Dados têm de ser periodicamente revistos e apagados

Statutory Retention Periods for HR Data	
Wage information	3 years
Working hours and related information	3 years
Collective redundancy information	3 years
Parental leave records	8 years
Carer's leave	3 years
Employment permit records	5 years or period equal to duration of employment (whichever is longer)
Employment records of young persons	3 years
Accident records	10 years

Exemplo do reino Unido
Carece adaptação à legislação
Quais os limites em Portugal ?

Processamento legítimo

- Para que o processamento seja legítimo
  - Livre consentimento
    - Não pode ser usado no processamento de dados de recursos humanos => relação hierárquica (não é livre)
  - Legitimidade consagrada na lei
    - Estabelecimento de contratos
    - Comprimento de obrigações legais
    - Futura proteção legal ou ação legal
    - Proteção de interesses vitais do sujeito
  - Legítimo interesse do controlador

Consentimento

- Ato livre, inequívoco, específico, conciso, informado, explicito, afirmativo
  - Inatividade não é consentimento
  - Omissão não é consentimento
  - Opções pré-validadas não são consentimento
- Prova de existência de consentimento
  - Recai sobre o controlador
- O consentimento pode ser retirado a qualquer momento
  - Têm que existir mecanismos simétricos para facilitar a retirada do consentimento pelo sujeito

Consentimento

- Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins.
- Não se deverá considerar que o consentimento foi dado de livre vontade.
  - se o titular dos dados não dispuser de uma escolha verdadeira ou livre
  - se não puder recusar nem retirar o consentimento sem ser prejudicado
  - se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados

Menores

- Para serviços ligados à sociedade da informação, o processamento dados de menores é legitimo:
  - Com consentimento do sujeito se tiver pelo menos 16 anos
  - Para idades inferiores requer consentimento dado por quem possuir a responsabilidade parental sobre o sujeito
  - O ónus da prova recai sempre sobre o controlador

Interesse legitimo do controlador

- Pode constituir base para o processamento:
  - O interesse do controlador tem de ser real e concreto
  - Os interesses e direitos fundamentais do sujeito não podem ser ultrapassados
  - Tem de ter em conta as razoáveis expetativas do sujeito baseadas na relação com o controlador
  - Exemplo:
    - Processamento de dados do cartão de credito para proteção contra fraudes
    - Lista de moradas que não querem receber publicidade

Categorias especiais de dados

- Dados pessoais que revelem:
  - Origem racial ou étnica
  - Opiniões políticas
  - Crenças religiosas ou filosóficas
  - Ligação a sindicatos
  - Dados genéticos
  - Dados biométricos
  - Dados referentes à saúde
  - Dados sobre vida sexual ou inclinação

- Permitidos apenas se:
  - Existir consentimento
  - Necessário exercer direitos legais ou obrigações do controlador
  - Proteção de direitos vitais do sujeito
  - Dados forem legalmente públicos
  - Necessário por razões médicas
  - Interesse público tal como ameaças graves de segurança ou saúde pública

Processamento

- Deve ser realizado apenas quando não exista outra forma de atingir o mesmo propósito
- O processamento tem de garantir a segurança e confidencialidade dos dados
- Todos os dados que não estejam corretos ou exatos devem ser corrigidos ou apagados

Investigação e interesse público

- O processamento incluindo arquivo de dados de interesse público é legal para:
  - Propósitos de investigação histórica e científica
  - Estatística de interesse público

- Realizado por instituições vocacionadas para o efeito:
  - Bibliotecas, arquivos, INE, etc

Segurança informática e de redes

- O processamento constitui interesse legitimo:
  - Na medida do estritamente necessário para garantir a segurança
    - Contra atos maliciosos, perda de informação, integridade, disponibilidade, autenticidade, etc
  - Por entidades:
    - Públicas
    - CERTs (emergências), CSIRTs (incidentes)
    - Fornecedores de rede e serviços de TI
    - Fornecedores de serviços de segurança

Acesso, retificação e remoção dos dados

- Controlador tem de disponibilizar mecanismos para o sujeito exercer os seus direitos.
  - Acesso aos dados, Retificação, Remoção, direito de objeção
- Devem ser disponibilizados por via eletrónica
  - Especialmente se forem processados por via eletrónica
- Pedidos de acesso, retificação, remoção por parte de sujeitos
  - Têm de ser respondidos no prazo de 1 mês (2 p/ casos complexos)
  - Se os pedidos do sujeito forem excessivos o controlador pode recusar-se ou cobrar os custos de processamento
  - A identidade do sujeito deve ser verificada

Direito de acesso

- A informação a dar ao sujeito inclui:
  - Propósitos dos processamentos e categorias de dados
  - Recipientes aos quais a informação possa ter sido passada
  - Período de armazenamento ou critério para o definir
  - Direitos do sujeito
  - Fontes de origem dos dados
  - Se existem tomadas de decisão automáticas
  - Cópia dos dados, em formato estruturado e interoperável
  - A lei prevê que um sujeito possa pedir a transferência dos dados entre dois controladores

Direito ao esquecimento

- O sujeito tem direito à remoção dos seus dados
  - Caso o controlador tenha passado os dados a outros controladores tem de os informar e pedir a remoção
- Condições para a remoção:
  - Quando os dados já não forem necessários
  - O consentimento é retirado (e não há base legal p/ retenção)
  - Os dados tenham sido processados ilegalmente ou sem autorização
  - Os dados tenham que ser apagados por razões legais
  - Quando o sujeito se oponha ao processamento (e não existam razões legais que se sobreponham)

Direito ao esquecimento

- Não se aplica:
  - Respeito por obrigações legais
  - Interesse público na área da saúde
  - Arquivos de interesse público, investigação científica ou histórica, estatística
  - Exercício de direitos de proteção legal ou ação legal
- Exercido num quadro de ponderação:
  - Exercício da liberdade de expressão, informação e imprensa

Informação a dar durante a colheita de dados

- Identidade e contacto do controlador
- Contacto do Responsável pela Proteção de Dados (RPD)
- Propósitos do processamento e sua base legal
- Quais os interesses legítimos do controlador (se for essa a base do processamento)
- Recipientes ou categorias de recipientes
- Indicação se os dados vão ser transferidos para um terceiro país ou organização internacional
- Período de retenção dos dados ou critério para determinar o período temporal
- Diretos do sujeito: acesso, retificação, remoção, objeção, restrição, portabilidade, retirada de consentimento, apresentar queixa ao supervisor (CNPD)
- Se a colheita decorre de requisito: contratual, legal
- Se a disponibilização dos dados e obrigatória e quais as consequências
- Se existem mecanismos automáticos de tomada de decisão incluindo *profiling*

Processamento adicional

- O controlador informa o sujeito
  - de qual o propósito do processamento adicional antes de o realizar
  - envia também novamente a informação constante do slide anterior atualizada para o novo propósito
- O sujeito pode opor-se ao processamento

Dados colhidos de outras fontes

O controlador informa o sujeito

- Qual a fonte de origem dos dados
- Identidade e contacto do controlador
- Contacto do Responsável pela Proteção de Dados (RPD)
- Propósitos do processamento e sua base legal
- Quais os interesses legítimos do controlador (se for essa a base do processamento)
- Recipientes ou categorias de recipientes
- Indicação se os dados vão ser transferidos para um terceiro país ou organização internacional
- Período de retenção dos dados ou critério para determinar o período temporal
- Diretos do sujeito: acesso, retificação, remoção, objeção, restrição, portabilidade, retirada de consentimento, apresentar queixa ao supervisor (CNPD)
- Se a colheita decorre de requisito: contratual, legal
- Se a disponibilização dos dados e obrigatória e quais as consequências
- Se existem mecanismos automáticos de tomada de decisão incluindo *profiling*

Responsabilidades do controlador

- O controlador é obrigado a:
  - Implementar o GDPR com medidas técnicas, organizacionais e políticas adequadas
  - Demonstrar que o processamento de dados pessoais cumpre o GDPR
  - Demonstrar que as medidas são eficientes
- O nº3 do Art 24 recomenda a demonstração através de:
  - Adesão a códigos de conduta
  - Certificação através de entidades certificadoras externas

Proteção por conceção e por defeito

- Medidas organizacionais e políticas
  - Políticas de privacidade => regras claras e públicas
  - Minimização de dados => manter o mínimo possível de dados
  - Limites temporais => apagar logo que legalmente possível
  - Minimização do acesso => acesso só quando necessário, aos dados estritamente necessários, pelos membros estritamente necessários
  - Adesão a códigos de conduta e certificação aprovados
- Medidas técnicas
  - Autenticação e autorização incluindo classes de acesso
  - Pseudoanonimização
  - Encriptação
  - Cópias de segurança
- Teste regular das medidas

Registo dos processamentos

- O controlador deve manter uma lista dos processamentos que realiza
  - Nome, contacto e detalhes do controlador
  - Propósito de cada processamento
  - Categorias de sujeitos e de dados processados
  - Categorias de recipientes
  - Limites de tempo para remoção
  - Descrição geral das medidas de segurança técnicas e organizacionais
- Não se aplica a organizações com menos de 250 trabalhadores
  - A menos que os processamentos impliquem risco !!!

Registo dos processamentos

Processamentos de risco incluem dados tais como

- Categorias especiais de dados (slide 21)
- Cartões de credito, contas bancárias (REQUER AVALIAÇÃO DE RISCO)
- Filiação sindical
- Informação de saúde (prescrições, exames, consultas, seguros, medicina do trabalho)
- Informação biométrica
- Cartões de identidade, passaportes etc
- Fotografias (fotos de rosto são informação biométrica !!!)
- Endereços postais
- Informação sobre rendimentos
- Certificados digitais, passwords e credenciais de acesso a serviços
- Avaliações profissionais
- Registos de acesso à Internet
- Páginas web pessoais protegidas
- Conteúdo de mailboxes
- Contas informáticas (histórico web, documentos, etc)

Avaliação de impacto da Proteção de Dados (AIPD)

- Obrigatório para processamentos de dados pessoais de risco elevado
  - Descrição sistemática do processamento e propósito
  - Justificação da necessidade do processamento
  - Interesses legítimos do controlador e/ou base legal
  - Avaliação dos riscos para as liberdades e direitos dos sujeitos
  - Medidas para minimizar os riscos e demonstração de cumprimento do RGPD
  - Caso as medidas a adotar possam não ser suficientes para mitigar o risco deve-se contactar a autoridade (CNPD)

Em caso de violação de dados

- Caso existam riscos potenciais para os sujeitos
  - Controlador tem 72 horas para notificar a CNPD
- A notificação tem de conter:
  - Natureza de violação de dados pessoais
  - Categorias e numero aproximado de sujeitos afetados
  - Categorias e numero de registos afetados
  - Nome e contacto do RPD
  - Consequências prováveis da ocorrência
  - Medidas tomadas e/ou propostas para mitigação
- Todas as violações de dados têm que ficar documentadas

Na violação de dados de risco elevado

- O controlador tem de contactar os sujeitos imediatamente
- Indicando:
  - Nome e contacto do RPD
  - Consequências prováveis da ocorrência
  - Medidas tomadas e/ou propostas para mitigação
- Não é necessário se os dados estiverem encriptados

Responsável pela Proteção de Dados (RPD)

- É necessário
  - Em organismos públicos e governados por legislação pública
  - Quando as atividades do controlador envolvem o processamento de dados pessoais em grande escala
  - Quando as atividades do controlador envolvem o processamento elevado de dados pessoais de categorias especiais
- RPD
  - Nomeado com base nas capacidades profissionais
  - Especializado na legislação e práticas de proteção de dados
  - Independente não pode receber diretivas da organização

Responsável pela Proteção de Dados (RPD)

- Funções
  - Informação e aconselhamento ao controlador
  - Monitorar o respeito pelo regulamento
  - Participar nas avaliações de impacto
  - Cooperar com as autoridades
  - Ponto de contacto com as autoridades

Transferência de dados para países terceiros ou organizações internacionais

- Entidades fora do controlo direto da União Europeia
  - Têm de possuir reconhecimento do nível de proteção por parte da Comissão Europeia
    - Decisão de adequação
  - Evidência de salvaguardas dos interesses dos sujeitos e de mecanismos de proteção
    - contrato, acordo, código de conduta, mecanismos de certificação, etc
    - consentimento após informação dos riscos
    - autorização do supervisor (transferências ocasionais)

Transferência de dados para países terceiros ou organizações internacionais

- EC Adequacy decisions
  - Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework)

Obrigado

Questões ?