CEGID & Associados

Consultoria e Gestão, Lda.

ENTIDADE FORMADORA CERTIFICADA

Ceg.01.06/01

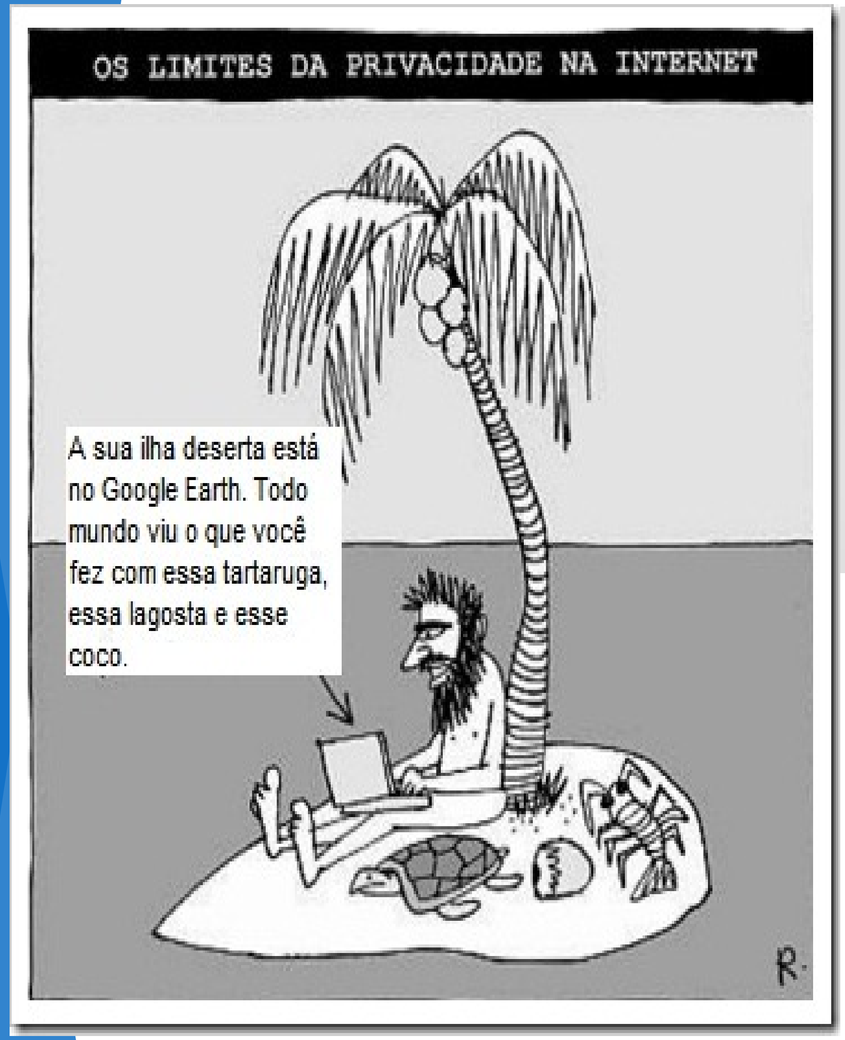
Proteção de Dados Pessoais (Reg.679/2016)

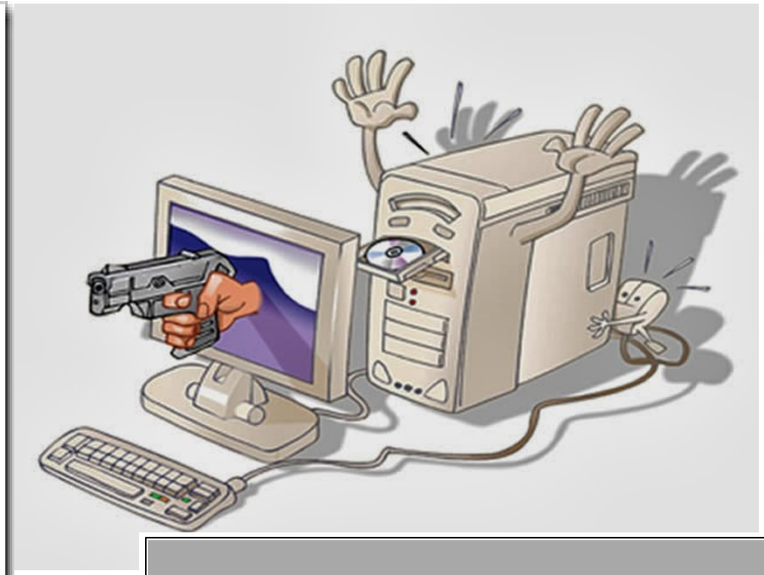
RGPD (679/2016) – Sociedade de Informação

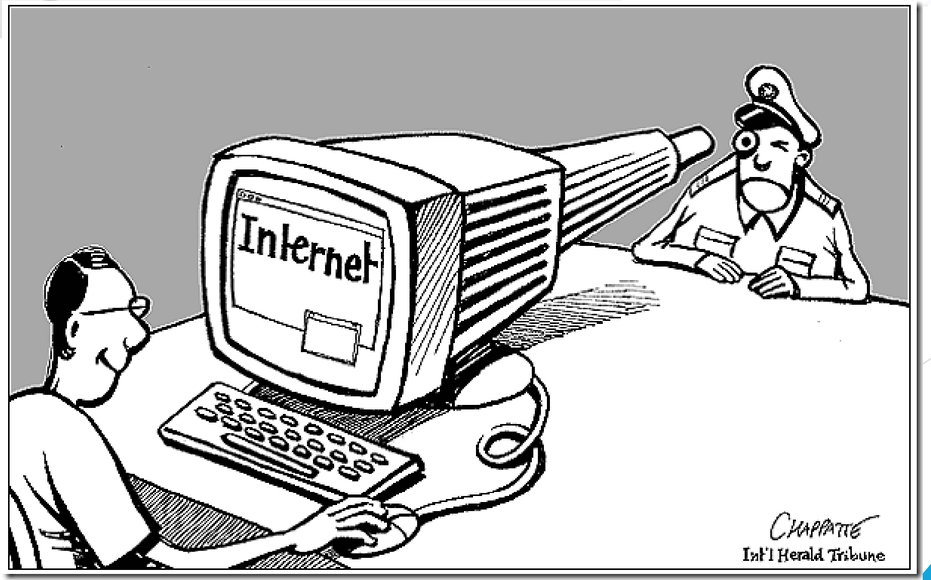
Tempo

Tecnologia

RGPD (679/2016) – Sociedade de Informação







RGPD (679/2016) – Enquadramento legal

Diretiva 95/46/CE

Lei 67/98

Reg.679/2016

- De carater imperativo;
- Com menos margem de adaptação em cada estado membro;
- Estabelece uma entidade reguladora única dentro do espaço Europeu ("one stop shop");
- Exige a evidência do cumprimento por parte das entidades subcontratadas (P.E: via contrato);
- Cria a figura DPO;
- Estabelece coimas mais elevadas;
- Auto regulação.

- De carater sugestivo;
- Sujeita a adaptações em cada estado membro;
- Pouco explicita ao nível das obrigações, por parte de quem realiza operações de tratamento de dados.

O RGPD não surge isolado mas enquadrado na seguinte "Família":

- Diretiva Europeia para a Cybersegurança;
- Acordo EUA/UE, relativo à transferência de dados pessoais (Privacy);
- Preparação do novo regulamento da UE para a comunicação Eletrónica;
- Preparação da nova diretiva Europeia para o comércio Eletrónico.

Casos de Incumprimento em matéria de Proteção de Dados

- Utilização de dados pessoais para a comercialização de novos serviços (telefone, mail); ***PRINCÍPIO DA LIMITAÇÃO DAS FINALIDADES***
- Solicitação de dados que não são necessários para a realização do serviço; ***PRINCÍPIO DA MINIMIZAÇÃO***
- Utilização de dados sem autorização explícita dos titulares de dados; ***PRINCÍPIO DA LICITUDE***
- Solicitação de dados por parte do titular a uma qualquer instituição sua detentora e a recusa por parte dessa instituição (exames médicos efetuados num local e solicitação dos mesmos para pedir uma 2ª opinião noutro local) – ***DIREITO Á PORTABILIDADE***
- Informação que circula num determinado site sobre o passado de alguém, possibilidade de ver o histórico de dados pessoais apagado – ***DIREITO AO ESQUECIMENTO***
- Pessoa que muda de nome por efeito de mudança de estado civil – ***DIREITO À RETIFICAÇÃO***

RGPD (679/2016) – Campo de Aplicação

Todas as organizações, que tratam dados pessoais, de cidadãos residentes na UE

Existem 3 tipos de dados pessoais :

- **Dados pessoais de trabalhadores** (Ex: sistemas biométricos de controlo de assiduidade, sistemas de geolocalização de colaboradores, sistemas de gestão de recursos humanos);
- **Dados pessoais de clientes e ou utentes** (Ex: informatização de dados em bases de dados para operações rotineiras como emissão de documentos, identificação célere, criação de perfis;
- **Dados de trabalhadores e de clientes em simultâneo** (Ex: sistemas de gravação de chamadas, sistemas de videovigilância).

RGPD (679/2016) – Conceitos

EXEMPLOS:

- Dados de ID (nome, morada, data nascimento, filiação, email)
- Dados de preferências (tipos de produtos, destinos de ferias, desportos ou hobbies)
- Matrículas;
- IP´s.

Dados Pessoais Sensíveis:

- Dados relativos à saúde;
- Dados de origem racial;
- Opiniões políticas, religiosas, filosóficas;
- Dados genéticos e biométricos.

Dados Pessoais – Informação relativa a uma pessoa singular identificada ou identificável, é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente em especial por referência a um identificador, como por exemplo: **nome**, **número** de **identificação**, dados de **localização**, **identificadores** por via **eletrónica** ou a um ou mais elementos específicos da identidade **física**, **fisiológica**, **genética**, **mental**, **económica**, **cultural** ou social dessa pessoa singular.

RGPD (679/2016) - Conceitos

Tratamento de dados – uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como: **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**.

EXEMPLOS:

Operações Macro

- Sistemas de Gestão de RH;
- Sistemas de Videovigilância;
- Sistemas de gravação de chamadas;
- Sistemas de Geolocalização;

Operações Micro

- Registo;
- Consulta;
- Destruição.

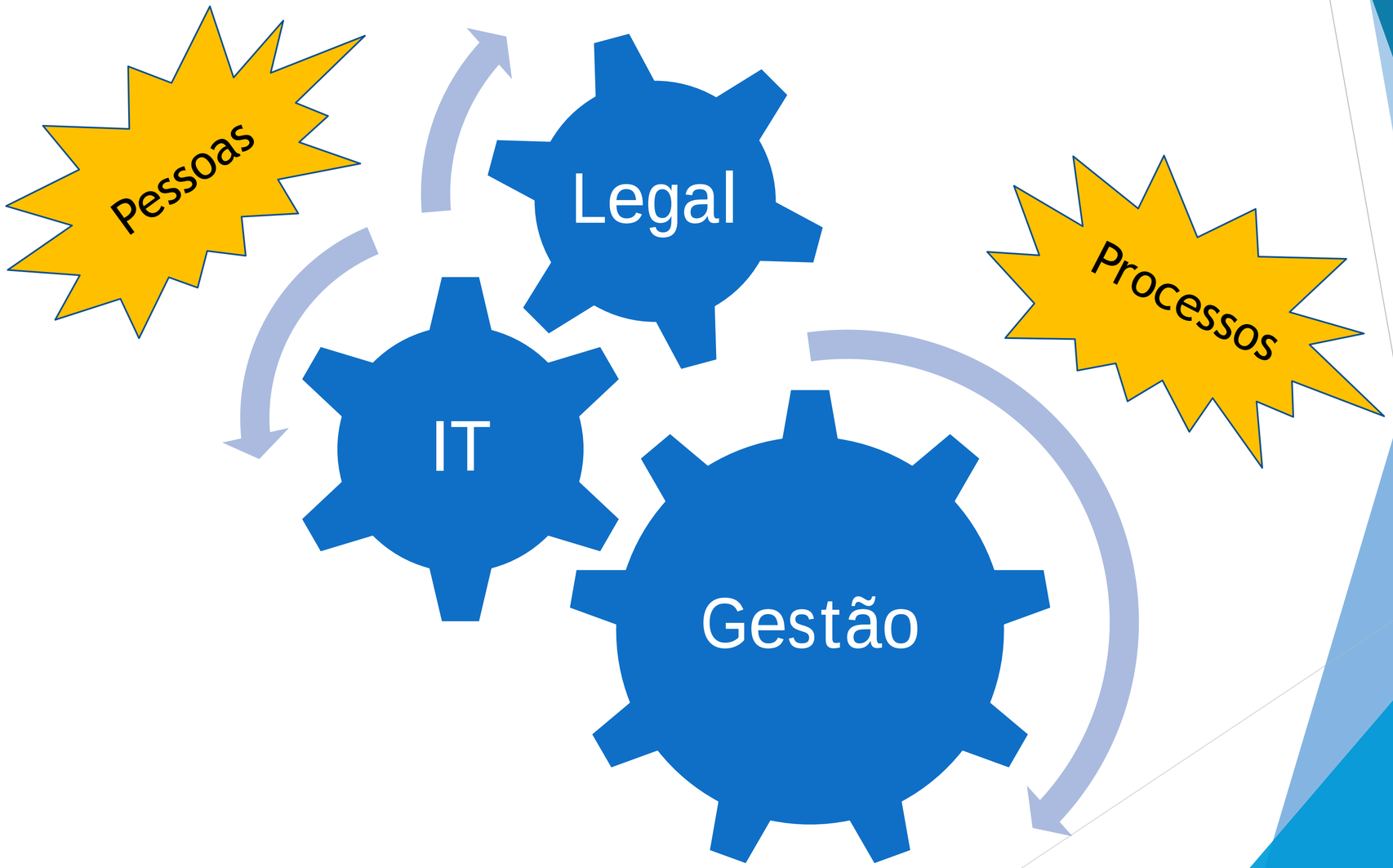
RGPD (679/2016) - Conceitos

Violação de dados – atuação que provoque de modo acidental ou ilícito, a **destruição**, a **perda**, a **alteração**, a **divulgação** ou o **acesso**, não **autorizado**, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

EXEMPLOS:

- Destruição involuntária dos dados;
- Perda dos dados;
- Acesso indevido aos dados;
- Divulgação não autorizada.

RGPD (679/2016) – Implementação



RGPD (679/2016) – Implementação

1ºFoco

- **Inventariar todos os dados, inventariar todas operações de tratamento de dados e caracterizar e mapear todos os Processos de tratamento de dados.**

2ºFoco

- **Gestão organizacional, tecnológica e financeira na proteção de dados.**

RGPD (679/2016) – Implementação

1ºFoco – Inventariar e caraterizar Dados Pessoais e operações de tratamento

Listar todos os dados pessoais;
Categorizar dados pessoais;
Localização dos dados pessoais;
Datar dados pessoais;
Quem trata Interna e Externamente;
Qual o objetivo do tratamento;
Definir acessos e responsabilidades;
Definir tempos de retenção;
Definir mecanismos de armazenamento;
Definir tempo e forma de eliminação.

2º Foco – Gestão Organizacional e Tecnológica

Organizacional –Novos Processos – "by design and by default", DPO, Políticas de privacidade, Procedimentos, Manuais de SGSI e PD, códigos de conduta, notificações de violação de dados, Subcontratados, Registos e evidências, análise do risco, monitorização, auditorias, testes de intrusão.

Técnicas – Software, controlo de acessos, Identificação e autenticação, cloud, VPN, firewall, encriptação em arquivo ou na transmissão(dispositivo móvel, pseudonimização/anonimização, rastreabilidade, Cloud.

RGPD (679/2016) – Gestão Financeira na Proteção de Dados

Valorização de Ativos

Oportunidade

RGPD

Cumprimento da legislação

Minimização de incidentes com impacto na Imagem

RGPD (679/2016) – Gestão Financeira na Proteção de Dados

Custos da proteção de dados

PREJUÍZO

Implementação do RGPD para a Proteção de Dados

CPD= CA+CP+CVD

Sanções/

Indeminizações e repercussões de Imagem

CUSTOS

CPD – Custos da proteção de dados

CA – Custos da avaliação (auditorias, monitorização do sistema, testes de intrusão)

CP – Custos de Prevenção (implementação do SGSI e PD, procedimentos, avaliação dos riscos, software, outras medidas tecnológicas, formação)

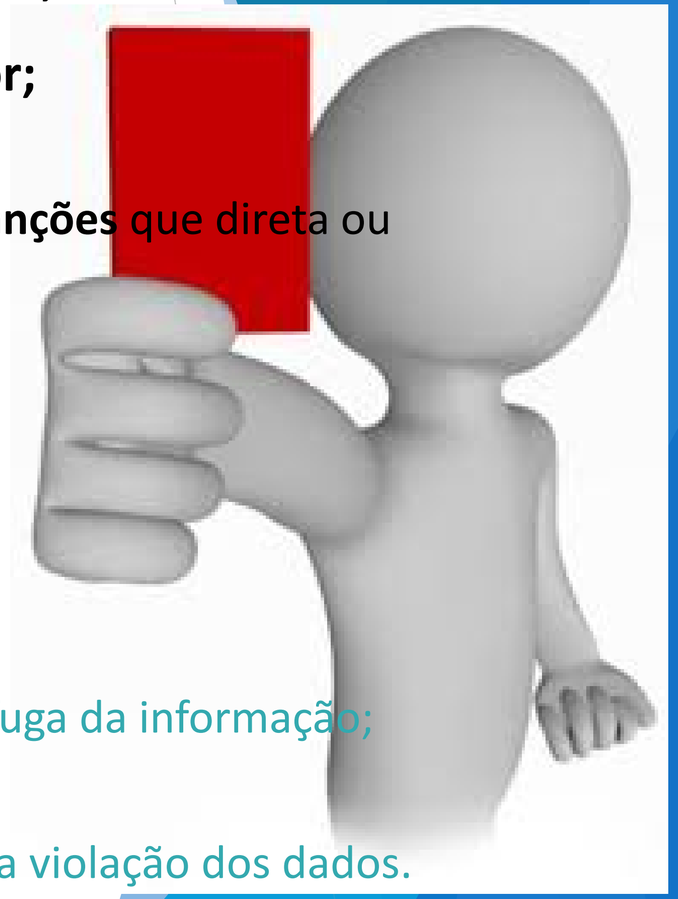
CVD – Custos da violação dos dados (custos de imagem, contra ordenações, indeminizações, resgates).

RGPD (679/2016) – Gestão Financeira na Proteção de Dados

Sanções:

Sanções normais: 10.000.000€ ou 2% do VN, o que for maior;

Sanções graves: 20.000.000€ ou 4% do VN, o que for maior;



As sanções estabelecidas pelo RGPD são contra ordenações. No entanto o **Espetro de Sanções** que direta ou indiretamente possam surgir por ilícitos no âmbito da proteção de dados são:

1 – Processos crime;

2 – Pedidos de indeminização civil;

3 – Contra ordenações;

4 – Processos disciplinares.

Exemplo: Escola privada que permite violação dos dados pessoais dos seus alunos:

a) Processo crime contra administradores, Diretor de TI e responsáveis pela fuga da informação;

b) Pedido de indeminização civil por parte dos lesados;

c) Processo de carater disciplinar contra os colaboradores que “permitiram” a violação dos dados.

Princípios do RGPD (679/2016)

Princípios da Proteção de dados (artigo 5º)

1- Licitude, Lealdade e Transparência – Os dados pessoais, só poderão ser tratados de forma lícita, leal e transparente;

2- Limitação das finalidades – O dados pessoais, só poderão ser tratados para fins determinados, explícitos e legítimos;

3- **Minimização** – O dados pessoais recolhidos, devem ser os adequados, pertinentes e limitados;

4- Exatidão – Os dados pessoais, devem ser exatos, e sempre que necessário devem ser atualizados;

5- Limitação da conservação – Os dados pessoais devem ser conservados apenas durante o tempo necessário/acordado e não mais do que isso;

6- Integridade e Confidencialidade – A segurança dos dados pessoais contra o tratamento ilícito, bem como a integridade dos mesmos deve ser garantida pelo responsável pelo tratamento;

7- Responsabilidade – O Responsável pelo tratamento, terá que evidenciar o cumprimento do RGPD.

Direitos dos Titulares dos Dados - RGPD (679/2016)

Direitos Tradicionais dos Titulares (capitulo III)

1- Transparência (art. 12º) – O titular dos dados (TD) deve ser informado pelo responsável pelo tratamento de forma **concisa**, **transparente** e **clara** de todas as regras relativas ao tratamento;

2 – Informação (art. 13) – O TD deve ter informação, sobre o responsável pelo tratamento (identidade e contato, contato do DPO, as finalidades das operações de tratamento de dados…)

3- Acesso (art. 15º) – O TD deve ter acesso

aos seus dados, junto do responsável pelo tratamento, bem como à informação sobre os mesmos;

4- Retificação (art. 16º) – O TD tem direito a que o seus dados sejam retificados, pelo responsável pelo tratamento, sempre que os mesmos evidenciem inexatidão;

5- Notificação (art. 19º) – O responsável pelo tratamento, deve comunicar qualquer **retificação**, **apagamento** ou **limitação** do tratamento;

Direitos dos Titulares dos Dados - RGPD (679/2016)

Direitos Novos dos Titulares (capitulo III)

6- Esquecimento (art. 17º) – O TD, tem direito ao apagamento de todos os seus dados por parte do responsável pelo tratamento;

7- Limitação do tratamento (art. 18º) – O TD, tem direito a limitação do tratamento;

8- Portabilidade (art. 20º) – O titular dos dados, tem direito a receber os seus dados, para os poder transmitir a quem entender;

9 - Oposição (art. 21º) – O TD, tem direito a opor-se em qualquer momento, face a sua situação, ao tratamento dos seus dados;

10 - Decisões individuais automatizadas (art. 22º) – O TD, tem direito a não ser sujeito a decisões automatizada, incluindo a definição de perfis

Obrigações - RGPD (679/2016)

Obrigações dos responsáveis pelo tratamento dos dados (capitulo IV)

1- Estabelecer política adequada (art. 24º) – Em função dos dados e das operações de tratamento e dos dados;

2 – Demonstrar cumprimento do RGPD (art. 24º) – As operações de tratamento de dados, devem evidenciar conformidade com o RGPD;

3- Proteção de Dados desde a Conceção e por Defeito (art. 25º) – Demonstrar a proteção de dados, desde a fase de conceção de produtos e serviços; *(by design and by default)*

4- Registos das atividades de tratamento (art. 30º) – O responsável pelo tratamento, deve registar as atividades de tratamento e conservar os respetivos registos;

Obrigações - RGPD (679/2016)

Obrigações dos responsáveis pelo tratamento dos dados (capitulo IV)

5 - Cooperação com a autoridade de controlo (art. 31º) – O responsável pelo tratamento, deve cooperar com a autoridade de controlo sempre que solicitado;

6 - Segurança do tratamento (art. 32º) – O responsável pelo tratamento, deve aplicar as medidas técnicas e organizacionais necessárias ;

7- Notificação de Violação (data Breach) (art. 33º) – O responsável pelo tratamento, tem 72h para notificar a autoridade de controlo;

8- Avaliação do impacto (art. 35º) – Sempre que o responsável pelo tratamento adote novas tecnologias, deve avaliar o impacto;

Obrigações - RGPD (679/2016)

Obrigações dos responsáveis pelo tratamento dos dados (capitulo IV)

9- Designação do DPO (art. 37-39º) – O responsável pelo tratamento dos dados deve designar um DPO;

10- Subcontratação regulada (art. 28º) – O responsável pelo tratamento terá que contratualizar, as operações externas de tratamento de dados;

11 – Comunicação da violação aos titulares (art. 34º) – O responsável pelo tratamento, deve comunicar as violações a que os dados foram sujeitos;

Obrigações - RGPD (679/2016)

Obrigações dos responsáveis pelo tratamento dos dados (capitulo IV)

12- Responsáveis conjuntos pelo tratamento (art. 26º) – Sempre que a responsabilidade do tratamento seja partilhada, ambos dever esclarecer as respetivas responsabilidades ;

13 – Cumprir códigos de conduta (art. 33º) – O responsável pelo tratamento, deve cumprir os códigos de conduta;

14 – Garantir os direitos dos titulares – O Responsável pelo tratamento, deve desenvolver todas as medidas necessárias, para que os titulares possam exercer os seus direitos;

Algoritmo do RGPD (679/2016)

$$Sanção = \frac{NC(7P;10D;14O)}{AT} \; X\,AG$$

NC= Não conformidade

P= Princípios da Proteção de dados

D= Direitos dos Titulares

O= Obrigações dos responsáveis pelo tratamento

AT= Atenuantes - Medidas Organizacionais e Técnicas implementadas, Código de Conduta Aprovado, Certificação, Orientações do DPO, SGSI, Sistema Gestão Risco, Sistema Auditado, Formação;

AG= Agravantes – Grande Escala, Elevado Risco, Natureza, Gravidade, Duração, Intencionalidade/Negligência, Dados Sensíveis, Benefícios Financeiros Obtidos;

Exemplos de Notícias sobre fugas de informação

Exemplos de Notícias sobre violação de dados

1- https://www.noticiasaominuto.com/politica/762049/cds-pede-esclarecimentos-sobre-violacao-de-dados-pessoais-dos-acorianos

2- https://www.inesctec.pt/haslab/noticias-eventos/nos-na-imprensa/aplicacoes-moveis-acedem-a-dados-pessoais-ilegalmente-jornal-de-noticias

3- http://expresso.sapo.pt/internacional/2017-06-06-Detida-alegada-autora-de-fuga-de-informacao-sobre-ingerencia-russa-nas-eleicoes-dos-EUA

4- http://www.jornaleconomico.sapo.pt/noticias/dois-bancos-em-cabo-verde-multados-por-falha-na-protecao-de-dados-171793

5- http://m.folha.uol.com.br/mercado/2017/05/1884434-facebook-e-multado-em-150-mil-euros-por-falha-na-protecao-de-dados.shtml?mobile

6- https://sol.sapo.pt/artigo/549734/piratas-informaticos-atacam-hospital-garcia-de-orta-

7- https://en.wikipedia.org/wiki/List_of_data_breaches


ESTA NÃO FLORIU! NO ENTANTO RECEBEU ÁGUA, LUZ, ADUBO... NÃO SEI O QUE FALTOU.
A PRIMAVERA CHEGOU!
!
INFORMAÇÃO.

Dúvidas?

Obrigado pela atenção!

CONTACTOS

Sede:

Estrada de Leiria nº 206
Edifício Embra Park, 1º, Escritório O
2430-068 Marinha Grande

Telefone / Fax: 244561088

Email: josemorais@cegid.pt
memoriacandidaturas@gmail.com

Delegação Norte: Santa Maria da Feira

Telemóvel: 913996004

Email: lenia_cegid@sapo.pt

Delegação Sul: Lisboa

Telemóvel: 910624136

Email: marisol_cegid@sapo.pt
justina.aragao_cegid@sapo.pt

Visite-nos