AP²SI Associação Portuguesa para a Promoção da Segurança da Informação

Os desafios

do *Regulamento Geral da Proteção de Dados* (RGPD)

da *General Data Protection Regulation* (GDPR)

João Paulo M. Ribeiro

28 junho 2017

REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

ISSN 1977-0774

Jornal Oficial

da União Europeia

L 119

Edição em língua portuguesa

Legislação

59.º ano
4 de maio de 2016

Índice

REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

DESAFIOS:

- Âmbito: sector público & sector privado – **25 maio 2018**
- Responsabilização / Contabilização / Acompanhamento / Conformidade: contratante/responsável (controla) *vs* subcontratante(s) (trata/processa); manutenção de registos sobre tratamentos de dados; sanções/coimas;
- Consentimento: **livre**, específico, **informado** e inequívoco e **expresso**; **parental**; **explícito**
- Princípios da Proteção: **desde a conceção** (*privacy by design*) **por defeito** (*privacy by default*)
- Direitos: **apagamento**; **esquecimento**; **portabilidade**; **limitação**;

REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

DESAFIOS:

- Notificação de Violações ("*data breaches*") – **Autoridade** *vs* **Titular**(es) 72 horas
- Avaliações de Impacto do Tratamento – "*Data Protection Impact Assessment*" (DPIA); Processo documentado;
- Políticas de Privacidade; Transparência; Facilidades no acesso; etc.
- Encarregado de Proteção de Dados – "*Data Protection Officer*" (DPO) – organismos públicos; tratamentos "*grande escala*"; tratamentos "*categorias especiais*"; tratamentos "*infrações*"; 250 colaboradores;
- Segurança do(s) Tratamento(s)

REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

DESAFIOS: Segurança dos Tratamentos

- aplicar **medidas de segurança adequadas** em **função dos riscos**
- registo de **todas as atividades** dos tratamentos e **suporte documental** (físico e digital);
- **Minimização**; **Pseudoanonimização**; **Cifragem**;
- capacidade de assegurar a **confidencialidade**, **integridade**, **disponibilidade** e **resiliência permanentes** dos **sistemas** e dos **serviços** do tratamento;
- capacidade de restabelecer **disponibilidade** e o **acesso** aos dados pessoais de **forma atempada** no caso de um **incidente** físico ou técnico;

REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

DESAFIOS: Segurança dos Tratamentos

- **processo** para **testar**, **apreciar** e **avaliar regularmente** a **eficácia** das **medidas técnicas e organizativas** para **garantir a segurança** do tratamento
- **avaliar o nível** de **segurança adequado face aos riscos** de destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, na **transmissão, conservação ou qualquer outra operação** – auditoria...

- Cibercriminalidade; *BYOD*; *Cloud*; *Big Data*; Data Analytics; *IoT*; …
- Códigos de Conduta; Formação/Sensibilização; Certificação e Selos; …

REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

DESAFIOS: Alargamento do conceito de Dados Pessoais

*«**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.*

[artº 4º "definições" al. 1)]

REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

DESAFIOS: Alargamento do conceito de Dados Pessoais

- *"dados biométricos"*
- *"definição de perfis" / "decisão tomada exclusivamente com base no tratamento automatizado"*
- *"endereços IP"*
- *"testemunhos de conexão (cookie)"*
- *"etiquetas de identificação por radiofrequência"; …*

REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

DESAFIOS: Normas, Boas Práticas e Frameworks

- NP ISO 27001:2013 – Gestão de Segurança de Informação
- ISO/IEC 27002 – "Controlos" de Segurança de Informação
- ISO/IEC 22301:2014 – Gestão da Continuidade de Negócios
- NP ISO 31000:2013 – Gestão do Risco (ISO/IEC 27005)
- NP ISO 20000-1:2015 – TI: Gestão de Serviços
- NP ISO/IEC 38500:2015 – Governação e Gestão das TI
- Melhores Práticas: Tribunal de Contas, Instituto de Seguros de Portugal, CMVM, Banco de Portugal,…
- CobiT®; ISACA; Privacy By Design (Ann Cavoukian, Ph.D.); outras…

REGULAMENTO GERAL DA PROTEÇÃO DE DADOS

EMPRESAS

2015	1.181.406

Fontes/Entidades: INE, PORDATA
Última actualização: 2017-03-14

Bancos, Caixas Económicas	Caixas de Crédito Agrícola Mútuo
2015	2015
4.532	734

Fontes/Entidades: INE (até 2005) | BP; INE (a partir de 2006), PORDATA
Última actualização: 2016-11-03

Anos	Empresas do sector público							
	Total	Administrações Públicas				Sociedades públicas		
		Total	Central	Regional	Local	Total	Sociedades não financeiras	Sociedades financeiras
2016	608	284	125	26	133	324	279	45

Fontes/Entidades: DGAEP/MF, PORDATA
Última actualização: 2017-04-11

https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf

Associação Portuguesa para a Promoção da Segurança da Informação

Obrigado!

Dúvidas?