Regulamento Europeu de Proteção de Dados Pessoais (RGPD) e os novos desafios das organizações

27 de setembro de 2017

Pedro Bernardino
Head of Compliance

Os principais impactos do RGPD (GDPR): Breve Síntese

Os principais impactos do RGPD (GDPR): Breve Síntese

Agenda

1. Introdução
2. Primeiro impacto: Para onde olhar?
3. Glossário
4. Encarregado de Proteção de Dados
5. Políticas, Instrumentos e Procedimentos de *Compliance*
6. Consentimento

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Agenda

7 *Data Privacy Impact Assessment* (DPIA ou PIA)

8 *Data Breaches*

9 Penalidades

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Introdução

- A publicação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril (RGPD) tem gerado enormes expectativas, muitas questões e apreensão por toda a Europa:
  - 173 Considerandos;
  - 88 páginas;
  - 99 artigos;
  - Lei n.º 67/**98**, de 26 de outubro.

- O RGPD implica profundas mudanças no paradigma legal e regulatório da proteção de dados pessoais, num quadro sancionatório agravado, com impactos muito relevantes na atividade económica, trazendo a proteção de dados pessoais e as questões e os procedimentos com ela conexos para o quotidiano de todas as empresas.

- Consequentemente, as empresas devem adotar elevados níveis de *compliance* em matéria de proteção de dados pessoais porquanto os mesmos podem ser vistos como mais-valias criando, desta forma, oportunidades junto dos respetivos Clientes/Consumidores.

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Introdução

- A dificuldade não está na distinção entre dados pessoais e dados pessoais sensíveis. Ela reside na determinação do que são dados pessoais.

- Existirá uma nova categoria de dados pessoais?

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Primeiro impacto: Para onde olhar?

- Glossário.
- Encarregado da Proteção de Dados (*Data Protection Officer*) e, eventualmente, de uma equipa especialmente dedicada à proteção de dados pessoais.
- Assegurar a existência de políticas, instrumentos e procedimentos de *Compliance* em matéria de proteção de dados pessoais.
- Rever os consentimentos prestados pelos titulares e adaptá-los às novas exigências legais.
- Rever todos os instrumentos contratuais com subcontratantes ou com terceiros, no que respeita às transferências e aos tratamentos de dados pessoais.

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Primeiro impacto: Para onde olhar?

- Identificar o tratamento de dados pessoais sensíveis (ou críticos para o negócio) e elaborar *privacy impact assessments.*
- Assegurar que os novos conceitos estão incluídos nas políticas e procedimentos da empresa.
- Criar modelos de comunicação de *datas breaches.*
- Formar e sensibilizar todos os níveis da empresa em proteção de dados e fomentar uma cultura de respeito pela privacidade.
- Penalidades.

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Glossário

Dados pessoais	Tratamento	Limitação do tratamento	Definição de perfis
Pseudonimização	Ficheiro	Responsável pelo tratamento	Subcontratante
Destinatário	Terceiro	Consentimento	Violação de dados pessoais
Dados genéticos	Dados biométricos	Dados relativos à saúde	Estabelecimento principal
Representante	Empresa	Grupo empresarial	Regras vinculativas aplicáveis às empresas
Autoridade de controlo	Autoridade de controlo interessada	Tratamento transfronteiriço	Objeção pertinente e fundamentada
Serviços da sociedade de informação	Organização internacional		

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Encarregado da Proteção de Dados (*Data Protection Officer*)

- Os responsáveis pelo tratamento de dados e os subcontratantes passam a ter de designar um Encarregado da Proteção de Dados (EPD) quando:
  - As suas atividades principais consistam em operações de tratamento de dados que pela sua natureza, âmbito ou finalidade impliquem um controlo regular e sistemático dos titulares dos dados.
  - As atividades principais do responsável consistam em operações de tratamento de dados sensíveis.

- Em regra, sempre que o tratamento seja efetuado por uma autoridade ou organismo público, a nomeação de um EPD é obrigatória.

- O EPD pode ser um elemento da entidade responsável pelo tratamento ou do subcontratante ou exercer as suas funções com base num contrato de prestação de serviços.

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Encarregado da Proteção de Dados (*Data Protection Officer*)

- As funções do EPD consistirão em controlar a conformidade do tratamento de dados com o RGPD, cooperar com a autoridade de controlo e informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações.

- Caso os responsáveis optem por indicar um EPD, ficam obrigados a assegurar a existência dos recursos necessários para o desempenho da sua função e a assegurar determinadas garantias de independência.

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Políticas, Instrumentos e Procedimentos de *Compliance*

- Código de Conduta.

- Política de Proteção de Dados Pessoais para diferentes destinatários (por exemplo, colaboradores, prestadores de serviços, *outsourcing*, entre outros).
  - Objeto;
  - Dados pessoais;
  - Tratamento;
  - Suporte dos dados;
  - Princípios gerais de proteção (por exemplo, licitude, legitimidade, pertinência, exatidão, conservação, direitos do titular dos dados e proteção, entre outros);
  - Formação;
  - Gestão de relações contratuais com terceiros e de projetos;
  - Responsabilidades e mecanismos de controlo.

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Políticas, Instrumentos e Procedimentos de *Compliance*

- Política de *Clean Desk.*
  - *Label*;
  - *Look;*
  - *Lock.*

- Obtenção e retirada do consentimento.

- Publicidade.

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Consentimento

- Introdução de maiores exigências em matéria de deveres de informação e obtenção do consentimento dos titulares dos dados quando este seja fundamento de legitimidade do tratamento dos respetivos dados.

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Data Privacy Impact Assessment (DPIA ou *PIA*)

- A avaliação de impacto sobre proteção de dados corresponde a uma avaliação prévia do impacto de determinado conjunto de operações de tratamento previstas sobre a proteção de dados.

- Pretende-se aferir ou determinar a origem, a natureza, a particularidade e a gravidade do risco de determinados tratamentos de dados pessoais para os direitos e liberdades dos respetivos titulares dos dados.

- Deve ser realizada pelo responsável pelo tratamento sempre que certo tipo de tratamento, que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, seja suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos dados a tratar.

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Data Privacy Impact Assessment (DPIA ou *PIA*)

- Exemplos:
  - Em caso de uma avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
  - Em caso de operações de tratamento em grande escala de dados sensíveis;
  - Quando ocorra controlo sistemático de zonas acessíveis ao público em grande escala.

- Deve incluir:
  - Uma descrição sistemática das operações de tratamento e a concretização das finalidades do tratamento;
  - Uma avaliação da necessidade e da proporcionalidade das operações de tratamento em relação aos objetivos de tratamento pretendidos;
  - Uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados;
  - As medidas previstas para fazer face aos riscos identificados, as garantias, as medidas de segurança e os procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade entre o tratamento em análise e o RGPD.

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Data Breaches

- Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares (por exemplo, a perda de controlo sobre os seus dados pessoais, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional, entre outros).

- Logo que o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, deverá:
  - Notificá-la à autoridade de controlo;
  - Sem demora injustificada e;
  - Sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido;
  - A menos que seja capaz de demonstrar em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares.

- Se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem demora injustificada.

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Data Breaches

- O responsável pelo tratamento deverá informar:
  - Sem demora injustificada;
  - O titular dos dados da violação de dados pessoais;
  - Quando for provável que desta resulte um elevado risco para os direitos e liberdades da pessoa singular;
  - A fim de lhe permitir tomar as precauções necessárias.

- A comunicação deverá:
  - Descrever a natureza da violação de dados pessoais;
  - Dirigir recomendações à pessoa singular em causa para atenuar potenciais efeitos adversos;
  - Ser efetuada logo que seja razoavelmente possível;
  - Em estreita cooperação com a autoridade de controlo;
  - Em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de polícia.

© Zurich

Os principais impactos do RGPD (GDPR): Breve Síntese

Penalidades

- Aumento relevante dos valor das coimas que podem ser aplicadas pelas autoridades de controlo em consequência da violação das normas do RGPD, com o valor máximo de € 20M ou 4% do volume de negócios do infrator.

© Zurich