GDPR
Notas de Implementação

Modelo de decisão da aplicabilidade

Estabelecimento na UE

Artigo 2 (Rec. 15-19, 27): Objeto

Princípios fundamentais e definições

Modelo de implementação

Faz executar

Faz executar

Procedimento legal Coletivo

Papel consultivo para a CE e estados membros

Autoridade de Supervisão

Article 29 Working Party (atualmente o EDPB - European Data Protection Body)

Principais tendências

Iniciativas afim

GDPR Notas de Implementação

Link: http://www.eugdpr.org/

- O GDPR vem substituir a Diretiva de Proteção de Dados 95/46/EC (the 1995 Data Directive). Uma descrição bem estruturada pode ser consultada através deste link.
Custos das quebras de privacidade:

- O ***Information Commissioner's Office*** (ICO), no Reino Unido, processou a Equifax Lda. com uma penalização de £500.000 por falhas na proteção de dados pessoais de mais de 10 Milhões decidadãos Ingleses, durante o Ciber ataque de 2017. A investigação teve por base o Data Protection Act de 1998 e não o GDPR (por não estar em vigor à data.
- A **Agência Espanhola para a Proteção de Dados** impôs uma coima de €1.08 milhões a uma produtora de programas de TV que, entre outras infrações, não protegeu devidamente a informação de 7000 concorrentes de shows de TV, permitindo que hackers acedessem à informação pessoal desses concorrentes
- No rescaldo de uma violação de dados que afetou 150,000 clientes, o gabinete do **Comissário para a Informação** do Reino Unido multou o prestador de serviços de comunicações TalkTalk em £ 400,000.
- O Grupo Financiero Banorte, o terceiro maior banco do México, sofreu uma violação de dados no final de 2014 / início de 2015. Após a investigação em 2015, as autoridades mexicanas multaram o banco 32 milhões de pesos (US $ 2 milhões).

- Um relatório da IAPP (junho de 2017) revela que de um universo de 204 profissionais de privacidade, pertencentes a várias áreas industriais, 61% ainda não tinha iniciado o processo de implementação do GDPR; 4% declaravam-se conforme

- Um outro relatório, mais abrangente (envolvendo 370,000 membros da comunidade de SegInfo, através do LinkedIn e com parceiros especializados em surveys), sobre empresas sediadas em território Europeu, revela:

1. A grande maioria está familiarizada com o GRPD mas apenas cerca de 33% está conforme ou em vias de o estar
2. 32% espera uma considerável alteração nas práticas de segurança, para atingir a conformidade
3. 50% experimenta limitações orçamentais para a mudança, enquanto 48% refere a falta de *experts*
4. O artigo que suscita mais preocupações: "Data protection by design and by default"; a razão são as implicações nas alterações do processos de desenvolvimento
5. **Apenas 5% das empresas na UE acreditam que estão em conformidade; 27% acreditam que não vão satisfazer a deadline**

06/14/2017 22:03
Henrique Santos said

Regulation (EU) 2016/679 of the European Parliament and of the Council 27 April 2016

1. Princípios fundamentais e definições

Link: https://www.titanhq.com/practical-guide-to-gdpr

1.1. Consentimento informado e explícito (Direito à informação)

1.1.1. Dado livremente, de forma clara, informada e sem ambiguidades

1.1.2. Requer uma ação afirmativa, clara (optout ou silencio não serve)

1.1.3. Demonstrável (algum registo)

1.1.4. Revogável, em qualquer instante

1.2. Solicitação de acesso a dados (direito ao Acesso e à Retificação)

> Sempre que um sujeito solicita o acesso aos seus dados privados, a organização tem que o facultar, SEM CUSTOS (o que não acontecia na anterior legislação). Este processo pode ser demorado e exigir alguns novos procedimentos. É conveniente dar essa informação aos sujeitos, na política de privacidade.

1.3. Direito ao esquecimento

> Não basta o Controlador eliminar os dados, pois precisa também **garantir que o processamento pelos Processors cessa** (a menos que haja escusa, por interesse público)

1.4. Divulgação de incidentes (Direito à informação)

> Notificação tem que ser enviada para o Gabinete do Comité da Informação (Information Commissioners Office - ICO), no máximo até 72h após a deteção; o sujeito deve igualmente ser notificado sem qualquer atraso **se a quebra representar um risco para os seus direitos e liberdades**.

1.4.1. Exemplos de quebras de privacidade

> Quebras de Privacidade incluem:
>
> - Acesso por terceiros, não autorizados **(Controlo de Acessos)**
> - Ação (ou inação) deliberada ou acidental de um Controlador ou Processador (**implica monitorização**)
> - Envio de dados pessoais a um destinatário incorreto (**como detetar?**)
> - Roubo ou perda de dispositivos com dados pessoais (**precaver com regras de utilização**)
> - Perda de disponibilidade de dados privados (**Segurança da Informação**)

1.5. Minimização de dados (Direito ao Controlo)

> O Direito ao Controlo e que obriga a monitorização, engloba o profiling, as ações publicitárias e o processamento para investigação (em geral)

1.6. Limitação do propósito

1.7. Limitação de armazenamento

1.8. Legalidade, imparcialidade e transparência

1.9. Rigor (precisão)

1.10. Integridade e confidencialidade

1.11. Prestação de contas (accountability)

> A "responsabilidade" é um novo conceito introduzido pelo GDPR (face à Diretiva). Exige que os **controladores possam demonstrar como eles cumprem os princípios de proteção de dados** identificados. Isto é significativo, uma vez que **altera o ónus da prova para o controlador de dados** no caso de uma investigação de conformidade por uma autoridade de proteção de dados. As organizações devem considerar este princípio à luz da obrigação de manutenção de registos, o requisito de provar a obtenção do consentimento e o conceito de privacidade por *design* e padrão.

1.11.1. Assegurar conformidade e demonstrá-la

1.12. Efeito Direto

1.13. Coimas

1.14. Direito à Portabilidade

1.15. Data Protection Impact Assessment (DPIA) - Artigo 35(7)

> Um **Risco** é um cenário que descreve um ou mais eventos e as suas consequências, estimadas em termos da severidade e probabilidade de ocorrência. A **Gestão do Risco**, por outro lado, pode ser definida como conjunto coordenado de atividades para dirigir e controlar uma organização, no que respeita ao Risco.

1.16. Entidades visadas

> Especificamente, qualquer organização que determina os propósitos e meios de processamento de **dados pessoais** é considerada um "**controlador**". Qualquer empresa que processa **dados pessoais** em nome do controlador é considerada um "**processador**".
> As organizações que precisam de estar em conformidade com o GDPR/UE são aquelas (controladoras e processadoras) estabelecidas na UE ou não, oferecendo bens ou serviços na UE ou para indivíduos da UE.

1.16.1. Controladores (DataController)

1.16.2. Processadores (DataProcessor)

2. Modelo de implementação

Link: Modelo_de_implementação-2.pdf

3. Procedimento legal Coletivo

- Nos EUA é já uma prática muito comum
- É possível que a UE venha a ter alguma iniciativa neste domínio

3.1. Alemanha

Link: http://www.alstonprivacy.com/germanys-christmas-present-data-protection-class-actions/

Na Alemanha, por exemplo, pode ser ativado por uma associação de proteção ao consumo

3.2. França

Link: https://www.huntonprivacyblog.com/2016/11/30/france-adopts-class-action-regime-for-data-protection-violations/

- A França regulamentou idêntico procedimento, em 2016

4. Principais tendências

4.1. Regulamentares

4.1.1. Penalizar mais fortemente os prevaricadores

Penalização dever ser efetiva, proporcional e dissuasiva

4.1.2. Aumento da exposição a procedimentos e investigações relacionados com quebra da privacidade

4.1.3. Mais regras para divulgação de incidentes de quebra de privacidade

4.1.4. Mais direitos para o sujeito detentor dos dados (Artºs 12-23)

4.1.4.1. Requisitar o acesso aos seus dados (SEM CUSTOS)

4.1.4.2. Alterar/Corrigir

4.1.4.3. Eliminar

4.1.4.4. Transferir

4.1.5. Garantir um nível de proteção idêntico em toda a UE

4.2. Incidentes que afetam a privacidade (exemplos)

4.2.1. Perda ou roubo de documentos em papel

4.2.2. Dados enviados para um destinatário incorreto

4.2.3. Páginas da Internet inseguras (inclui hacking)

4.2.4. Dados enviados por e-mail para um destinatário incorreto

4.2.5. Perda ou roubo de dados de dispositivos não cifrados

4.2.6. Falhas na redação de dados

4.2.7. Descarte de documentos (papel) inseguro

4.2.8. Informação colocada em páginas web

4.2.9. Descarte inseguro de hardware

4.2.10. Divulgação verbal

5. Article 29 Working Party (atualmente o EDPB - European Data Protection Body)

Link: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

> The Article 29 Working Party (WP29), set up under Directive 95/46/EC, is composed of the EU's national supervisory authorities, the European Data Protection Supervisor (EDPS) and the
> European Commission. The WP29 will be replaced by the "European Data Protection Board" (EDPB).

6. Iniciativas afim

6.1. Alemanha (1970) Datenschutzgesetzgebung

6.2. Privacy Act de 1974, EUA

> Uma das primeiras iniciativas na história a consagrar formalmente o direito a indivíduos de consultar e corrigir **informação Pessoal**.

6.3. 10/2016: França Digital Republic Bill

> Alinhando com o GDPR, esta lei permite à autoridade nacional da proteção de dados aplicar multas que podem chegar aos €3 milhões (anteriormente o máximo era €150.000)

6.4. Bélgica

Link: http://privacylawblog.fieldfisher.com/2015/belgian-privacy-commission-changes-enforcement-attitude-as-fining-powers-are-announced

6.5. Impacto em vários países da região Asia-Pacifico (ainda fruto da Diretiva de Dados 1995): APEC Privacy Framework Estado da California: regras de privacidade para a smart grid

6.6. Singapura - Personal Data Protection Act 2012 (PDPA)

Link: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview

6.7. e-Privacy Directive (Diretiva 2002/58/EC)

Link: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

Controla os direitos de privacidade, aplicados às tecnologias e conteúdos das comunicações eletrónicas.
Está em processo de revisão, para alinhar com o GDPR

6.7.1. e-Privacy regulation

Link: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

Também está em fase de revisão, com a entrada em vigor do GDPR - a proposta, intitulada "*Regulation on Privacy and Electronic Communications*", foi publicada en janeiro de 2017. O regulamento aplica-se a todos os provedores de serviços de comunicações eletrónicas, ou a qualquer entidade que processe dados de comunicações eletrónicas. Irá ter impacto na forma como as organizações interatuam eletronicamente com os cidadãos da UE, incluindo o rastreamento de utilizadores, a coleta de dados em dispositivos do utilizador, ou ainda o marketing direto, entre outras operações.

7. Autoridade de Supervisão

Link: https://edps.europa.eu/

Agência governamental competente para fiscalização/acompanhamento e investigação. - **DPA** (**Data Protection Authority** / Supervisory Authority / Lead Authority; em Portugal é a **CNPD**.
Deverá cooperar com a sua congénere na Europa - **EDPS** (**European Data Protection Supervisor**)

8. Artigo 2 (Rec. 15-19, 27): Objeto

Aplica-se ao processamento de **dados pessoais**, total ou parcialmente automatizado (e.g., por computadores), bem como ao processamento manual se os dados pessoais estão integrados num **arquivo**, ou se destinam a essa integração

8.1. Artigo 4(1): Dados Pessoais

Nos termos da Directiva, os dados pessoais são quaisquer informações relativas a uma pessoa física (**Data Subject**) identificada ou identificável. O GDPR adicionou expressamente **nomes**, **dados de localização**, identificadores on-line (incluindo IPs e Cookies - quando usados para identificar um dispositivo) e **fatores específicos da identidade genética de uma pessoa física** à luz dos fatores pelos quais uma pessoa física pode ser identificada. De acordo com a directiva, a definição de dados pessoais era menos específica, embora a visão geral fosse que esses identificadores geralmente já estavam contemplados

8.1.1. Artigo 4(5): Pseudonimização

Garantia de que o processamento de dados pessoais é feito de tal forma que os dados pessoais não podem mais ser atribuídos a uma pessoa específica, sem o uso de informações adicionais e desde que essas informações adicionais sejam mantidas separadamente e sujeitas a medidas técnicas e organizacionais para garantir que a os dados pessoais não são nunca atribuídos ao sujeito em questão.

8.2. Artigo 9: Dados Sensíveis

A definição de categorias especiais de dados, ou seja, dados pessoais sensíveis ou dados confidenciais, é ampliada pelo GDPR, adicionando dados genéticos e biométricos.
Sob esta definição expandida, as categorias de dados especialmente protegidas abrangem:

- Dados reveladores:
  - Origem racial ou étnica
  - Opiniões políticas
  - Crenças religiosas ou filosóficas, ou
  - Associação sindical
- **Dados genéticos (Artigo 4(13)) ou dados biométricos (Artigo 4(14)) com o objetivo de identificar de maneira explicita uma pessoa física**, ou
- Dados relativos à saúde (Artigo 4(15)), vida sexual ou orientação sexual de uma pessoa física

Os dados sensíveis podem ser processados quando a pessoa em causa dá o seu consentimento explícito a tal processamento, ou quando se aplicar uma derrogação específica.

8.2.1. Derrogações

Artigo 6:

- Processamento necessário nos domínios do emprego, segurança social e protecção social, quando autorizado por lei ou convenção coletiva;
- Processamento para proteger os interesses vitais do sujeito, ou de outra pessoa física, quando a pessoa em causa é incapaz de dar consentimento;
- Processamento por certas organizações sem fins lucrativos;
- Processamento de dados pessoais que são manifestamente tornados públicos pela pessoa em causa;
- Processamento em relação a processos legais ou por tribunais que atuam na sua capacidade judicial;
- Processamento necessário por razões de substancial interesse público, com base em compatibilidade e proporcionalidade legal;
- Processamento para fins de tratamento clínico preventivo;
- Processamento por razões de interesse público na área de saúde pública; e
- Processamento necessário para pesquisas científicas ou históricas.

8.3. Dados relacionados com ações criminais

8.4. Artigo 4(6): Arquivo

> Qualquer **conjunto de dados pessoais estruturados** que são acessíveis de acordo com algum critério específico, independentemente de estar **centralizado**, **descentralizado**, ou **disperso**, numa base **funcional ou geográfica**.

8.5. Artigo 4(2): Processamento

> Qualquer operação ou conjunto de operações que seja executado em dados pessoais ou em conjuntos de dados pessoais, com recurso ou não a meios automatizados, como coleta, gravação, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, eliminação ou destruição.

8.6. Exclusões

8.6.1. Por uma pessoa e no curso de uma atividade pessoal caseira (isenção doméstica)

8.6.2. Pessoas já falecidas

8.6.3. Por autoridades competentes, com o objetivo da prevenção, investigação, deteção e acusação em crimes

8.6.4. Por instituições da UE, quando existirem regulamentos específicos aplicáveis

8.6.5. No decurso de uma atividade fora do âmbito legal da UE

8.6.6. Enquadrado em políticas de estrangeiros e segurança comuns da UE

9. Modelo de decisão da aplicabilidade

10. Estabelecimento na UE

> Conceito "**One-stop-shop**" - não existe tradução:
> No caso de uma organização multinacional, com presença em vários países europeus, coloca-se a questão de saber qual o país cuja Entidade de Supervisão terá autoridade máxima (***lead authority***). Será aquele em que a organização dispõe da "maior" representação. No entanto, em cada país da UE em que esteja representada, a respetiva Entidade de Supervisão mantém poder regulamentar.

10.1. Artigo 3(2)(a) faz aplicar o regulamento a qualquer organização no mundo com relações comerciais com a UE e que processe dados pessoais de clientes (europeus) - Âmbito Territorial