Regulamento Geral de Proteção de Dados (RGPD)

3º Colóquio E3S

EY Advisory Services

Novembro, 2017

Building a better working world

Enquadramento

RGPD

O quê?

- Impacto da entrada em vigor do Regulamento (UE) 2016/679 do Parlamento Europeu e do conselho de 27 de Abril 2016 sobre a proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação dos mesmos – Regulamento Geral de Proteção de Dados (RGPD).

Quem?

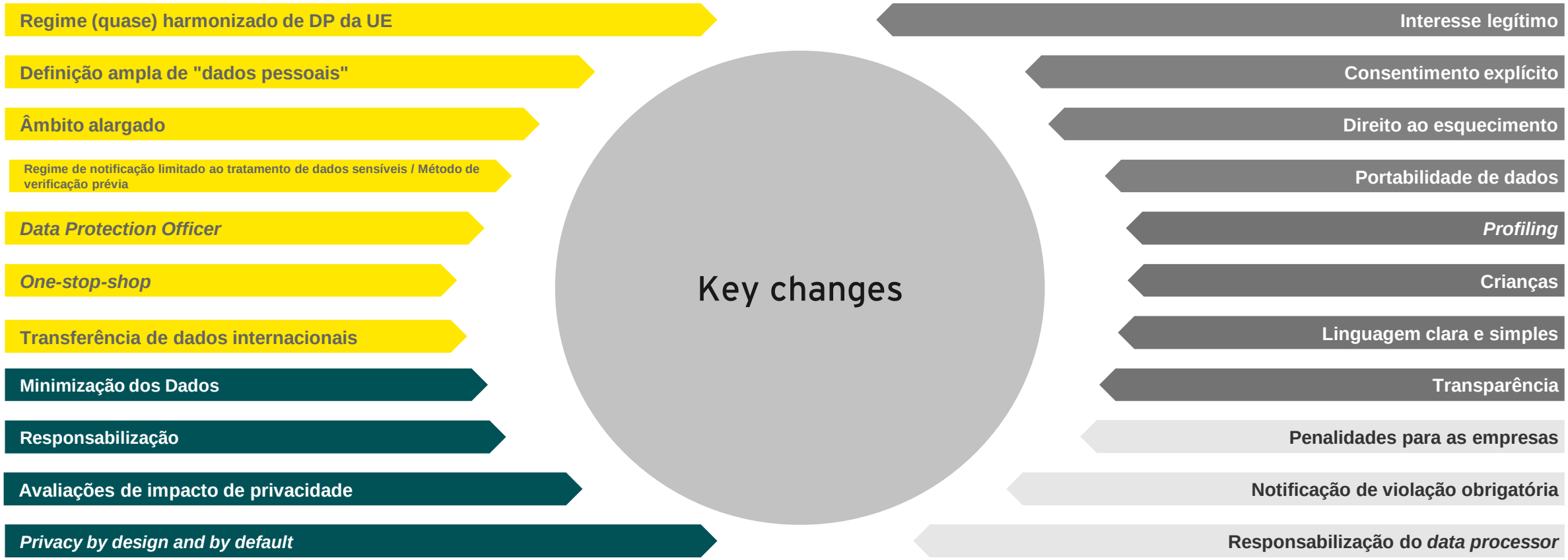
- Trata-se de legislação aplicada diretamente aos 28 Estados-Membros, sem necessidade de qualquer ato legislativo de transposição;
- Esta legislação será aplicada aos responsáveis pelo tratamento de dados (controladores) e aos subcontratantes a que recorram para efetuar esse tratamento (processadores);
- É também aplicada às operações de processamento que se focam nos assuntos de dados pessoais europeus, independentemente se o controlador (processador) esteja ou não localizado na EU.

Como?

- Depois de 4 anos de negociação, o RGPD foi publicado a 4 de Maio de 2016 no Jornal Oficial da União Europeia;
- O diploma prevê um período de transição de 2 anos até à implementação total, com entrada em vigor a 25 de Maio de 2018;
- As organizações terão esse período para se adaptarem às novas regras;
- A nova legislação apresenta mudanças significativas às regras de proteção de dados existentes impondo novas obrigações para as organizações cuja a sua violação é punida através de multas pesadas que podem ir até 4% do valor total anual da faturação da organização ou um valor de 20 Milhões de Euros.

Principais alterações propostas pelo RGPD

RGPD



Âmbito, Definições Formalidades

Novos princípios
Medidas de segurança adequadas

Novos direitos dos cidadãos, fundamento jurídico para o tratamento de dados

Aplicação / sanções
Notificação de segurança e violação

A nossa abordagem ao RGPD

RGPD

Legal

Interpretar o enquadramento legal
Traduzir os requisitos de proteção de dados em políticas internas e comunicação externa de forma a cumprir com a legislação:

- *Framework* de proteção de dados
- Consentimento explícito

Gestão de Risco

Avaliar o impacto no negócio
Avaliar o impacto no modelo de negócio da empresa.

Que fluxos de informação são permitidos?
Qual o impacto nas atividades internas / *outsourcing*? Como afeta os fluxos de receitas?

- Modelos de Negócio
- Contratos de *outsourcing*

Cyber Security

Analisar o nível de exposição aos riscos de *Cyber Security*
Perceber de que forma a organização está exposta e quais são os riscos mais prementes

Estamos protegidos contra riscos externos e internos? De que forma os riscos de negócio se traduzem na tecnologia de suporte? Qual o nível de maturidade da organização?

Tecnologia

Selecionar as ferramentas certas
Implementar a tecnologia necessária para proteger a privacidade de dados.

Como continuar "em controlo" constantemente?

- Portabilidade de dados
- Minimização de dados
- Direito a ser esquecido
- Violação de dados
- Gestão de terceiros

Organização

Incorporar a privacidade de dados na organização
Definir controlos e equilíbrios para permanecer em conformidade durante o processo.
Que parte da organização estará encarregada da proteção de dados?

- *Privacy by Design*
- *Privacy Impact Assessment*
- *Data Protection Officer*

A nossa abordagem ao RGPD

RGPD

Estratégia

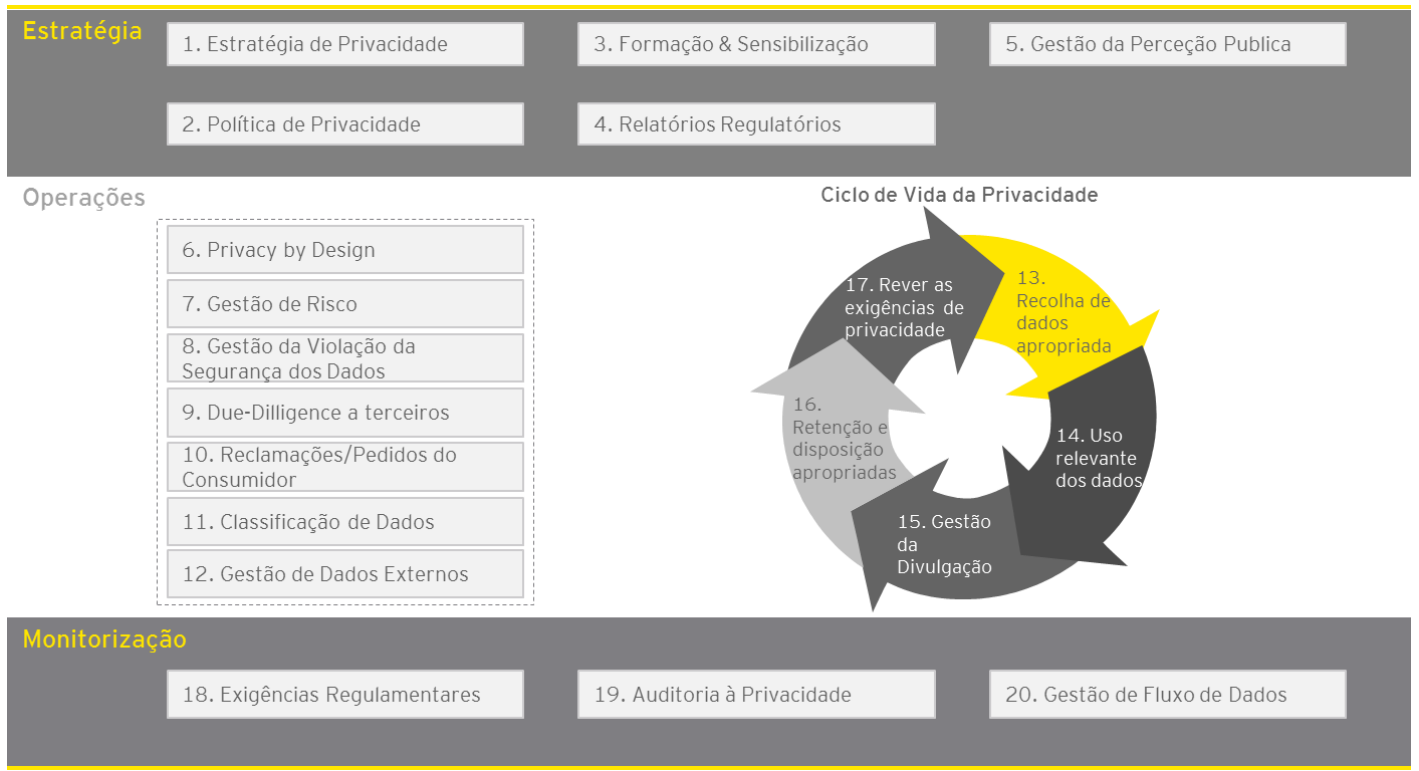
- Definição clara de responsabilidades e envolvimento forte de todos os elementos da organização
- A estratégia deve ter um modelo de governo claro, com processos estabelecido e do conhecimento global
- O *donos* dos dados devem ter um entendimento claro das suas responsabilidades

Operações

- Os programas de *data privacy*, assentam fundamentalmente na implementação efetiva de politicas e processos que promova o risco de exposição
- A inexistência de processos aumenta o nível de exposição e promove a não identificação de potenciais riscos atempadamente

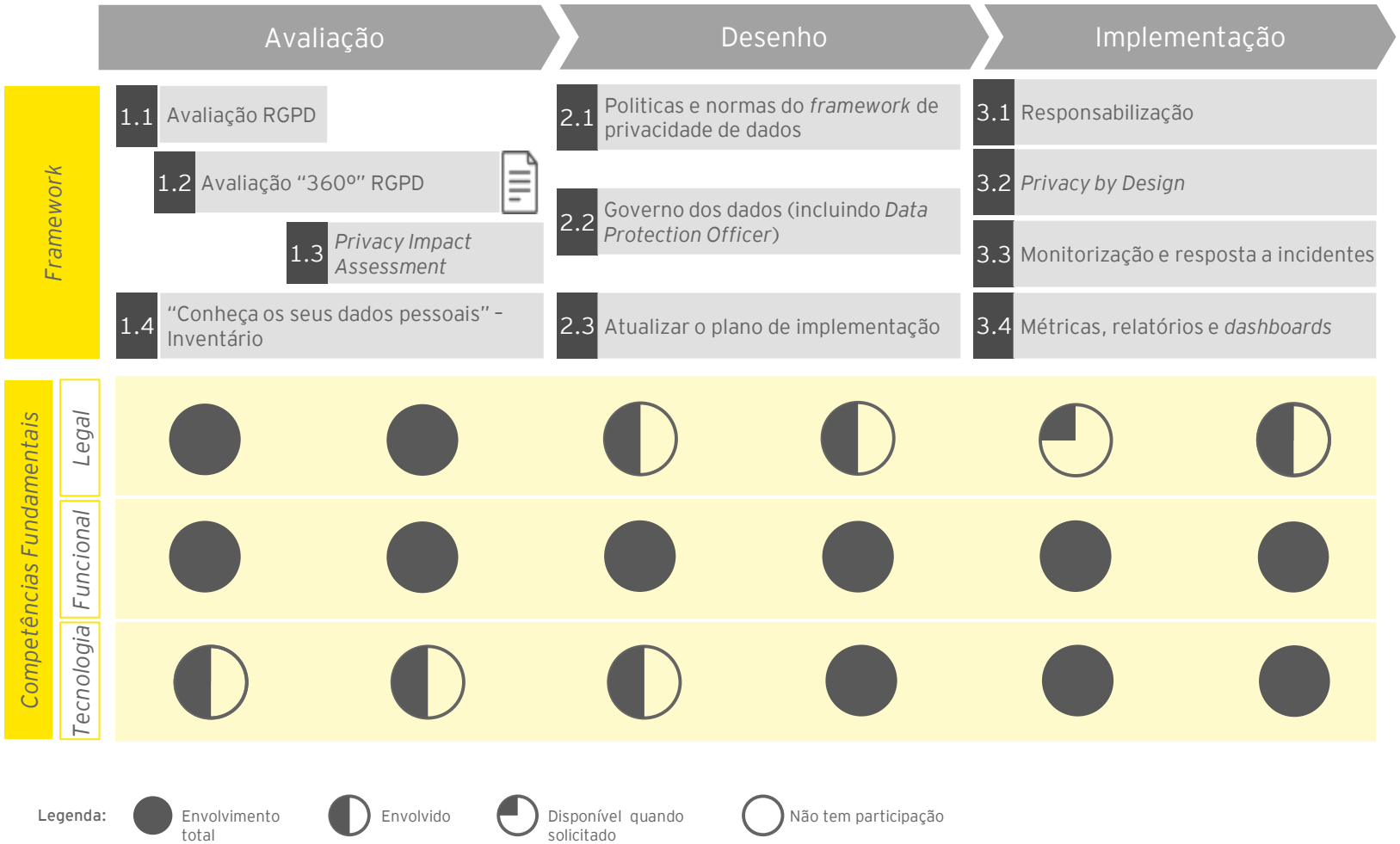
Monitorização

- As equipas devem estar integradas conjuntamente com o processos e ferramentas de suporte, de forma a promover uma monitorização contínua
- Deve existir uma ligação forte aos programas de segurança



A nossa abordagem metodológica

RGPD



Foco: avaliação de maturidade e *gaps*

Temos uma proposta forte relacionada com a fase de Avaliação da nossa abordagem transformacional.

O projeto de transformação deve ter como foco as seguintes áreas:

- Avaliação de Maturidade
- Modelo de Governo
- *Privacy Impact Assessment* em fluxos de alto risco
- Plano de implementação

Perguntas?

O RGPD é aplicável ao 3º sector?

- Sim

Que dados pessoais estão abrangidos pelo RGPD na instituição que represento?

- Dados pessoais de utentes, colaboradores, voluntários, sócios, mecenas, etc.

O que devo fazer primeiro?

- Conhecer os dados pessoais que a instituição recolhe, processa, arquiva, comunica.
- Proteger os dados pessoais sob o controlo da instituição e definir processos que permitam responder aos novos requisitos do RGPD
- Sensibilizar a instituição para a utilização dos dados pessoais de acordo com as novas normas do RGPD

...?

Obrigado

João Costa
Manager, Advisory – Lisboa (Portugal)

TIm: +351 937 913 006
Email: joao.costa@pt.ey.com

Building a better working world