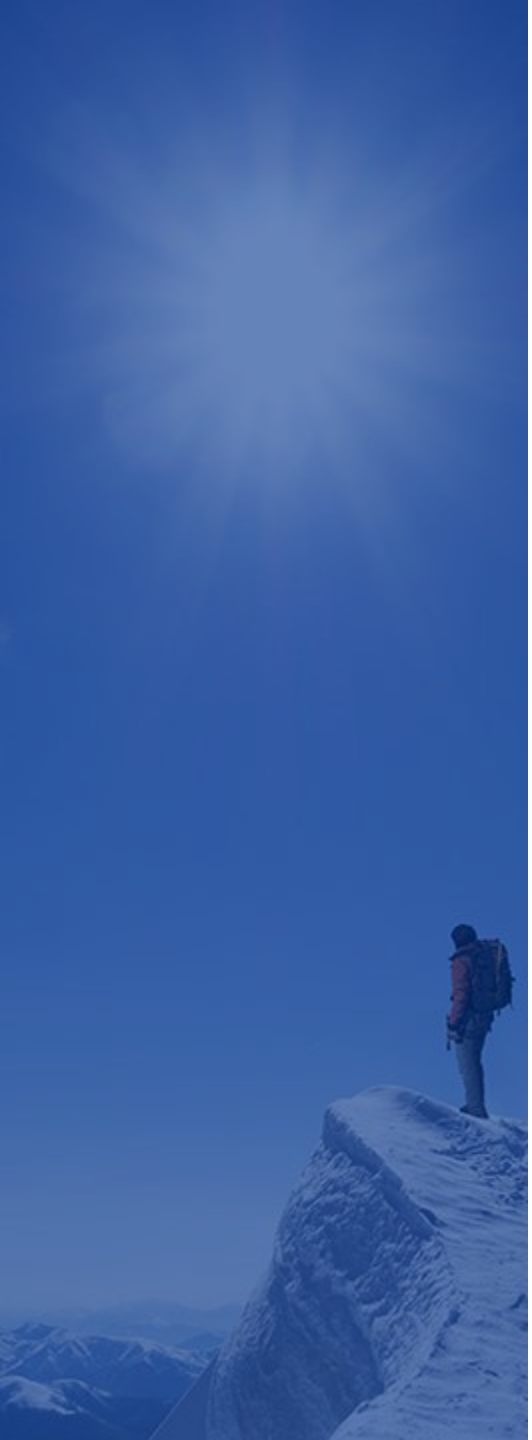
O Impacto do Regulamento Geral de Protecção de Dados em Portugal

Estudo

Março 2017

kpmg.pt



Introdução

A 27 de Abril de 2016 foi aprovado no Parlamento Europeu, com 95% dos votos a favor, o novo Regulamento Geral de Protecção de Dados (RGPD), após aproximadamente 5 anos de negociações e 4.000 adendas. O RGPD tem aplicação obrigatória a 25 de Maio de 2018 em todos os Estados Membro da União Europeia (UE), substituindo em Portugal a Lei 67/98, que transpõe para a ordem jurídica Portuguesa a anterior Directiva 95/46/CE.

Nas sociedades democráticas, o direito à privacidade é um princípio fundador da cidadania e da liberdade de pensamento e de expressão, e um instrumento fundamental na limitação do poder dos Estados e das Organizações sobre os indivíduos e da construção de relações de confiança. O direito à privacidade está consagrado artigo 35º da constituição Portuguesa.

O grande desafio está em garantir o controlo sobre a privacidade dos dados nesta nossa sociedade (justamente dita) de informação, onde a crescente adopção da Internet, das redes sociais e de modelos de negócio digitais criam uma equação de resolução difícil: por um lado, as pessoas sentem-se atraídas e partilham (às vezes voluntariamente, outras de forma inconsistente) dados da sua vida pessoal, frequentemente sem considerarem os potenciais efeitos colaterais; por outro, as Organizações capturam cada vez mais informação sobre os seus clientes, geralmente como o objectivo de fornecer mais e melhores serviços, ou como forma de monetizar a informação.

A realidade é que hoje as Organizações tendem a saber cada vez mais sobre os padrões de comportamento, a condição, os hábitos e as preferências dos seus clientes ou potenciais clientes, por vezes antes dos próprios; que o diga um cidadão Americano que descobriu que ia ser avô quando a sua filha adolescente começou a receber cupões de desconto para produtos pré-natais da Target, uma das maiores cadeiras de retalho dos EUA. Neste caso, a Target utilizou modelos analíticos avançados para determinar um grau de probabilidade de gravidez e estimar a data provável do parto, dentro de uma pequena janela de tempo.

Esta tensão entre o direito à privacidade e a importância dos dados pessoais para as Organizações tenderá certamente a crescer, nomeadamente com os produtos gerados pela constante inovação tecnológica, como os *smartphones* (cada vez mais inteligentes), os dispositivos *wearable* ou a *Internet of Things*.

Foi precisamente a necessidade de endereçar estes desafios e de garantir uma harmonização legislativa entre os Estados Membros, que suscitou a revisão das regras de protecção de dados pessoais na UE.

Comparando o RGPD com a Lei 67/98 em vigor, não existem grandes diferenças ao nível dos princípios de protecção de dados pessoais, mas existem diversas alterações significativas ao nível das regras do jogo e da operacionalização destes princípios, das quais destacamos as seguintes seis:

1. A alteração do **modelo de regulação**, que passa de um modelo de hétero-regulação, onde as organizações notificam e solicitam autorização à CNPD para os seus tratamentos de dados pessoais, para um modelo de auto-regulação. Neste modelo, as organizações têm a responsabilidade pela interpretação, operacionalização e manutenção da conformidade o RGPD, ficando sujeitas à acção inspectiva da Autoridade de Controlo.

2. A introdução de um **quadro sancionatório** agravado, que na sua expressão máxima pode ir até 20.000.000 Euros ou 4% do volume de negócios global do exercício financeiro anterior (o montante que for mais elevado). A dimensão destes números é, por si só, razão suficiente para colocar este tema na agenda dos órgãos de gestão da maior parte das organizações em Portugal.

3. O alargamento do **conceito de dados pessoais**, que passa a incluir quaisquer dados susceptíveis de identificar, mesmo que de forma indirecta, um determinado individuo.

4. O reforço dos **direitos dos titulares** de dados pessoais (e.g. direito ao esquecimento, direito à portabilidade), cuja implementação pode exigir alterações ao nível dos processos de negócio e dos sistemas de informação das organizações e a correspondente mobilização de recursos humanos e financeiros para as desenhar e implementar.

5. O reconhecimento da importância da dimensão da **protecção dos dados** na manutenção do direito à privacidade. As estatísticas mostram que todos os dias ocorrem milhares de ataques e são comprometidos mais de um milhão de registos de informação contendo dados pessoais. Garantir a implementação de medidas adequadas de protecção de dados pessoais é uma condição necessária para o respeito do direito à privacidade dos respectivos titulares.

6. A **obrigatoriedade de reporte** à Autoridade de Controlo de quaisquer incidentes relativos ao comprometimento de dados pessoais e, em certas condições, aos próprios titulares afectados. Esta obrigatoriedade, que já existe em alguns países (e.g. Estados Unidos da América e Reino Unido), aumenta significativamente a probabilidade de exposição mediática negativa das organizações, com o correspondente aumento do risco reputacional.

Reconhecendo o potencial impacto das novas regras, a UE estabeleceu um período transitório de 2 anos, durante o qual as organizações têm a oportunidade de implementar as medidas necessárias para endereçar as exigências deste novo paradigma no tratamento de dados pessoais.

Neste contexto, a KPMG promoveu um Estudo a nível nacional com o objectivo de avaliar o grau de conhecimento e o estado de preparação das organizações em Portugal para enfrentar os desafios impostos pelo RGPD. Tivemos o privilégio de contar com a participação de mais de 100 organizações, de diversas dimensões e sectores de actividades, o que permite obter um retrato representativo da realidade nacional nesta matéria. O nosso agradecimento a todos os participantes.

A pouco mais de um ano da entrada em vigor do RGPD, os resultados obtidos mostram que as organizações em Portugal começam a assimilar a importância do novo regulamento mas têm ainda, em termos gerais, um longo caminho a percorrer, não só para atingir a conformidade com o RGPD, mas também para convergir os seus processos de protecção de dados pessoais com melhores práticas internacionais.

No entanto, estamos convictos que as organizações nacionais têm capacidade para responder a mais este desafio e mobilizarem os recursos adequados para garantir a conformidade com o RGPD, no prazo exigido, neste contexto de mercado cada vez mais complexo e competitivo.

Rui Gomes
Partner

Índice

Principais Conclusões

Consciência

65% consideram ter um grau de consciência médio ou alto sobre as obrigações e impacto do RGPD

Impacto

53% anteveem um impacto alto ou muito alto na implementação do RGPD

Desafios

65% consideram a multiplicidade de processos de tratamento de dados pessoais como um dos maiores desafios na conformidade com o RGPD

Implementação

85% ainda não começaram a implementar medidas efectivas para garantir a conformidade com o RGPD

Data Protection Officer

43% nomearam um órgão responsável pela conformidade com as obrigações legais de protecção de dados pessoais

Entidades Terceiras

32% possuem contratos com cláusulas de protecção de dados com todas as entidades terceiras que fazem o tratamento de dados pessoais

Sensibilização e Formação

10% consideram que promovem acções de sensibilização e formação adequadas sobre protecção de dados pessoais

Resposta a Incidentes

43% têm implementados procedimentos de resposta a incidentes com dados pessoais

Consciência

Estarão as organizações conscientes sobre o RGPD?

Resultados

Aproximadamente 65% das organizações que participaram no Estudo considera ter um grau de consciência Médio ou Alto sobre as obrigações e impactos da implementação do Regulamento.

Os sectores que indicam ter um maior nível de consciência são o Financeiro e os Seguros, o que reflecte a importância dada por estas organizações à protecção dos activos de informação dos seus clientes, nos quais se incluem os dados pessoais.

Em oposição, os sectores Público, Indústria e Serviços são os que mencionam possuir uma menor consciência sobre o RGPD. Este resultado é mais fácil de enquadrar para o sector da Indústria, considerando que a sua base de clientes é fundamentalmente constituída por empresas. No espectro oposto, está o sector Público, dada a multiplicidade de tratamentos de dados pessoais que muitas das Entidades do Estado são responsáveis.

Perspectiva da KPMG

A pouco mais de 1 ano da aplicação do RGPD, existe uma crescente sensibilização por parte das organizações para a importância da conformidade com o RGPD. É provável que esta tendência estejam relacionada com dois factores em particular:

- O regime sancionatório, com o aumento muito significativo das coimas, que poderão atingir o valor máximo de 20.000.000 EUR ou 4% do volume de negócios.
- O sentimento gradual da necessidade capitalizar a confiança de *stakeholders* externos (e.g. clientes, potenciais clientes), que fornecem os seus dados pessoais para os mais variados fins.

Actualmente já existe em Portugal o entendimento de que a não conformidade com as obrigações legais de protecção de dados pessoais e/ou a ocorrência de incidentes que envolvam dados pessoais, pode acarretar impactos relevantes, não apenas ao nível de potenciais coimas, como na degradação da boa reputação e imagem das organizações. Naturalmente, não basta apenas haver consciência sobre a importância da aplicação do RGPD; é imperativo que as organizações materializarem esta consciência em acções concretas que conduzam à conformidade com o RGPD.

Figura 1 – Grau de Consciência com o RGPD

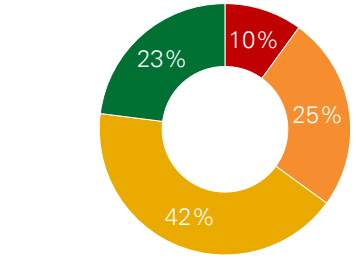
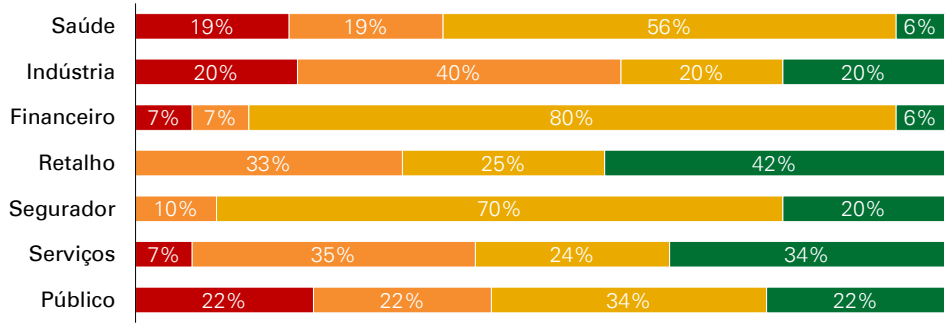


Figura 2 – Grau de Consciência com o RGPD, por sector



Impacto e Desafios

Que Impacto e Desafios irão as organizações enfrentar na conformidade com o RGPD?

"O RGPD é o mais elevado standard de protecção de dados no Mundo"

Věra Jourová
Comissária Europeia responsável pela Justiça, Consumidores e Igualdade de Género – Press Release da Comissão Europeia, 14 de Abril de 2016

Resultados

O RGPD tem por base os princípios de privacidade vertidos na Directiva 95/46/CE, apresentando novas obrigações em matéria de protecção de dados pessoais e novos direitos para os titulares dos dados. Por outro lado, não obstante ser um regulamento que apresenta conceitos normativos genéricos, o RGPD é extremamente exigente e abrangente sobre as medidas que as organizações devem implementar.

Foi observado que 53% das organizações prevê que a implementação do RGPD acarretará um impacto Alto ou Muito Alto em termos de tempo, esforço e custo de implementação.

Os sectores dos Serviços, Saúde e Segurador antecipam um maior impacto associado ao RGPD, naturalmente reflexo do volume e natureza dos tratamentos de dados pessoais associados aos seus processos de negócio, muitos dos quais são considerados categorias especiais de dados.

Perspectiva da KPMG

A avaliar pelos resultados do estudo, a maioria das Organizações portuguesas apresenta actualmente um nível de conformidade baixo com as futuras obrigações legais de tratamento de dados pessoais.

A implementação do RGPD requer um maior ou menor nível de exigência em termos de tempo, esforço humano e financeiro, em função de diferentes variáveis, como:

- Número e complexidade das práticas de tratamento de dados pessoais.
- Nível de maturidade das práticas de tratamento e protecção de dados pessoais.
- Apetite ao risco e decisões sobre estratégias para endereçar as obrigações do RGPD, nomeadamente as acções de natureza tecnológica.

É nosso entendimento que, face ao nível de exigências do RGPD, a Gestão de Topo deve mobilizar os recursos humanos e financeiros necessários para assegurar a implementação RGPD até Maio de 2018. Mais, as organizações devem ainda criar as condições adequadas para integrar as exigências do RGPD nas suas actividades operacionais diárias, para assegurar a manutenção contínua da conformidade.

Figura 3 – Impacto da implementação do RGPD

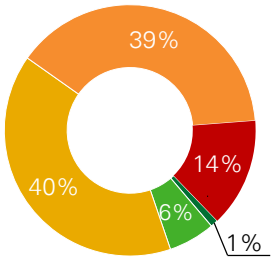
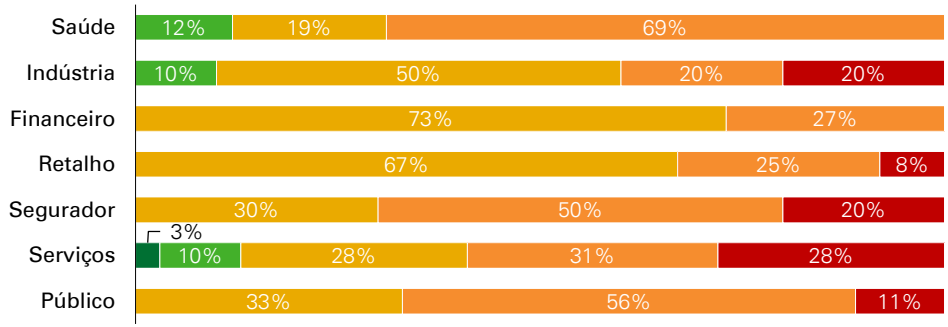


Figura 4 – Impacto da implementação do RGPD, por sector



Resultados

O nível de exigência do RGPD coloca desafios complexos, de natureza organizacional, processual e tecnológica, que podem exigir um esforço significativo no processo de transformação das organizações para garantir a conformidade com o Regulamento.

As organizações elegem (i) a ausência de recursos especializados, (ii) as limitações dos sistemas de informação, (iii) a necessidade de ajustamento de processos de negócio, e (iv) a multiplicidade das actividades de tratamento, como os principais desafios a enfrentar no esforço de conformidade com o RGPD.

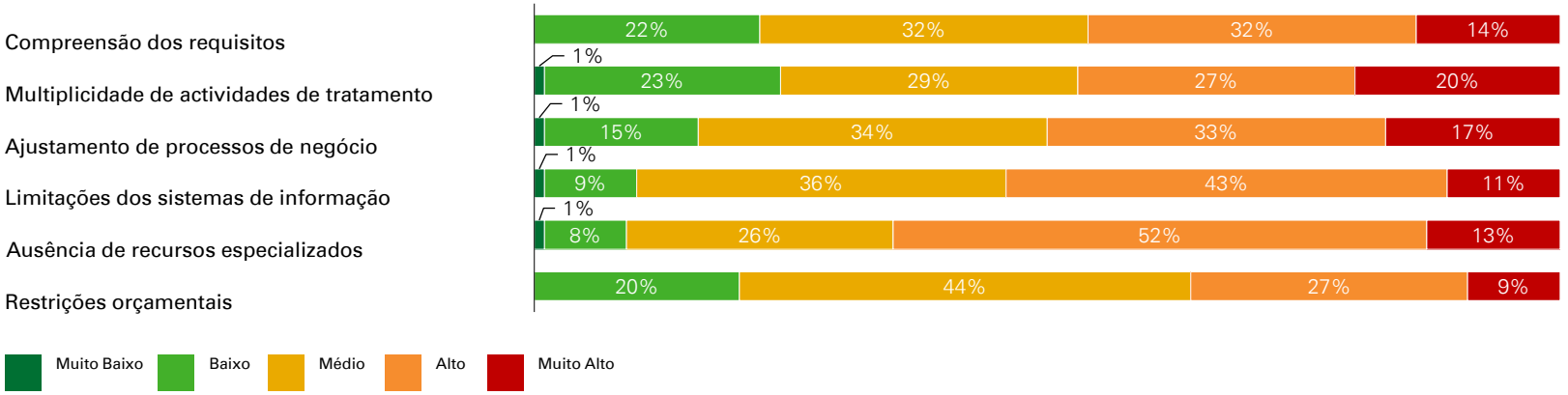
Perspectiva da KPMG

Os desafios potenciais mais indicados revelam uma consciência efectiva sobre as áreas-chave que devem ser analisadas no contexto da adaptação às exigências do RGPD.

De uma forma geral, as organizações efectuam múltiplos tratamentos de dados pessoais, de dados internos (e.g. colaboradores) e externos (e.g. potenciais clientes, clientes). Adicionalmente, existe uma tendência para a adopção de tratamentos de dados pessoais inovadores e mais sofisticados, com a utilização de técnicas de *big data* e modelos analíticos (e.g. análise de perfis de consumo, análise de dados de geolocalização, análise de dados de redes sociais) para potenciar modelos de negócio ou criar novos canais de comunicação com clientes. Nestes tipos de tratamento, as organizações assumem um papel de criadoras de dados pessoais, transcendendo o papel tradicional de receptor ou de entidade de custódia. Neste contexto, as organizações devem ter a capacidade para adaptar a especificidade de cada tipo de tratamentos de dados pessoais às exigências do RGPD.

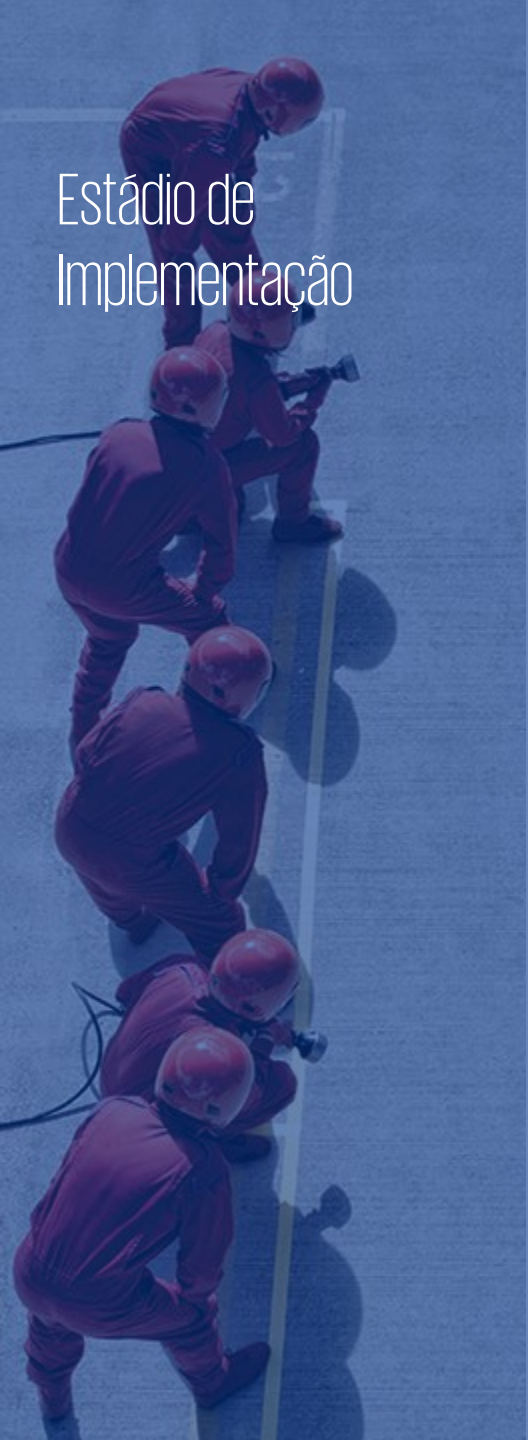
Os processos de negócio também devem ser ajustados para responder às necessidades intrínsecas de cada tratamento de dados pessoais, bem como com às novas exigências transversais a qualquer tipo de tratamento de dados (e.g. aplicação do princípio da protecção desde a concepção e por defeito, comunicação ao titular de toda a informação obrigatória aquando da recolha de dados pessoais).

Em muitas organizações, os sistemas de informação apresentam diversas limitações (e.g. ausência de modelos de autorização de acesso a dados pessoais, incapacidade para rastrear o acesso a categorias especiais de dados), que já hoje dificultam a implementação da actual legislação nacional de protecção de dados pessoais. Estas limitações serão ainda mais evidentes com as novas exigências impostas pelo RGPD, como por exemplo, o direito ao esquecimento ou a necessidade de ser mantida a evidência do consentimento explícito prestado pelos titulares dos dados para o tratamento dos seus dados pessoais.



Panorama Actual

Estão as organizações atrasadas na implementação do RGPD?



Estádio de Implementação

Resultados

Apesar da maioria das organizações estar consciente sobre as obrigações e desafios da implementação do RGPD e antecipar um impacto significativo na sua implementação, constata-se que 85% ainda não iniciou o processo de implementação de medidas efectivas para responder aos requisitos do RGPD, a pouco mais de um ano da entrada em vigor do regulamento.

Os sectores que indiciam estar num estádio mais avançado são a Saúde e o Retalho, o que pode ser explicado pela maior exposição destes sectores ao tratamento de grandes volumes de categorias especiais de dados pessoais.

Perspectiva da KPMG

Face ao nível de exigência do RGPD, as organizações devem iniciar, o quanto antes, esforços para implementar as medidas necessárias para assegurar, até Maio de 2018, a conformidade com o RGPD. Estes esforços devem ser alicerçados em medidas:

- Identificadas com base numa avaliação inicial do estado actual de conformidade dos processos de tratamento de dados pessoais face às exigências do RGPD.
- Avaliadas com base numa análise de risco de conformidade com o RGPD, considerando uma perspectiva de custo-benefício e o nível de apetite ao risco, sempre que as medidas identificadas exijam investimentos mais significativos.

Para os sectores mais regulados, as medidas a implementar devem ter em consideração outros requisitos legais e regulamentares aplicáveis com impacto ou que possam ser impactadas pelo RGPD (e.g. PSD2 - Payment Service Directive 2 - no sector Financeiro).

As páginas seguintes descrevem o panorama actual das organizações que participaram no Estudo para algumas das novas exigências impostas pelo RGPD.

Figura 6 – Estádio de Implementação do RGPD

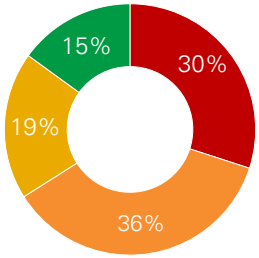
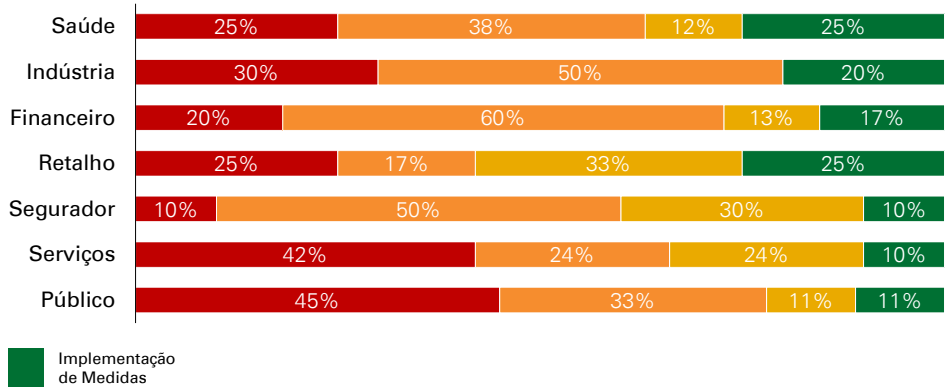


Figura 7 – Estádio de Implementação do RGPD, por sector



Modelo de Governo

Resultados

O RGPD estipula novas regras sobre as responsabilidades pela protecção dos dados pessoais. Estas responsabilidades incidem sobre *stakeholders* internos, mas também sobre *stakeholders* externos que façam o tratamento de dados pessoais em nome da organização contratante (e.g. outsourcing).

Face à multiplicidade e complexidade das actividades de tratamento de dados pessoais realizadas pelas organizações, é necessário formalizar responsabilidades, definir regulação interna, e formar e sensibilizar os colaboradores sobre os princípios e regras de protecção de dados pessoais.

Quando questionadas sobre a existência destes domínios de governo, as respostas das organizações consultadas demonstraram que apenas:

- 21% operacionalizaram a figura do Data Protection Officer (DPO).
- 4% possuem normativos internos adaptados aos requisitos do RGPD.
- 32% possuem contratos com cláusulas de protecção de dados pessoais com todas as entidades terceiras que fazem o tratamento de dados pessoais e apenas 5% realizam acções de verificação regulares sobre o grau de cumprimento dos contratos estabelecidos.
- 10% consideram que as acções de sensibilização e formação existentes são adequadas para comunicar aos colaboradores regras de protecção de dados pessoais.

Figura 8 – Órgão responsável pela protecção de dados pessoais

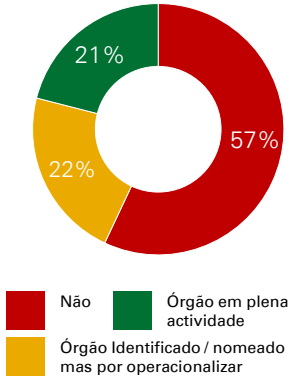


Figura 9 – Normativos de protecção de dados pessoais

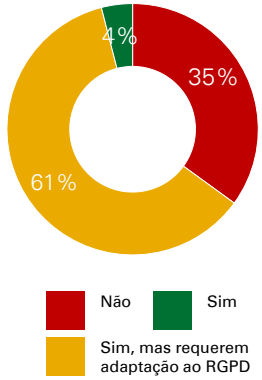


Figura 10 – Contratos de prestação de serviços com cláusulas de protecção de dados

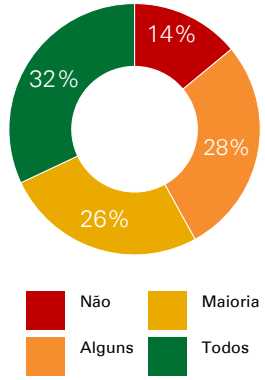
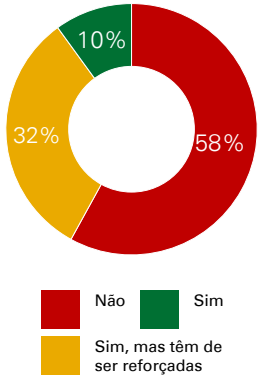


Figura 11 – Sensibilização e formação



Perspectiva da KPMG

Para endereçar o RGPD é necessário que as organizações implementem um Modelo de Governo de Privacidade de Dados, que enderece diferentes domínios distintos, como forma de fomentar a responsabilidades de todos os órgãos relevantes no tratamento de dados pessoais e, consequentemente, facilitar o estabelecimento de uma efectiva cultura de protecção de dados pessoais no seio da organização.

Como ponto de partida, as organizações devem avaliar, face aos critérios estabelecidos pelo RGPD (e.g. volume e categorias de dados tratados, duração do tratamento), a necessidade de criar a função de DPO. Para a criação desta função, é fundamental que as organizações reflictam, entre outros, nos seguintes aspectos:

- Posicionamento orgânico da função do DPO, garantindo que a função possa ser exercida de forma independente, com autoridade e sem conflitos de interesses.
- Perfil de competências técnicas e funcionais do responsável pela função.
- Modelo de articulação da figura do DPO com a organização.

Por outro lado, deve ser criado um corpo normativo de privacidade de dados, suportado por uma estrutura hierárquica de políticas, processos e procedimentos, para regular os tratamentos de dados pessoais em conformidade com os requisitos do RGPD e boas práticas de protecção de dados pessoais.

O RGPD menciona a necessidade da existência de um Código de Conduta para facilitar a correcta aplicação do Regulamento. Este normativo pode ser considerado como uma Política de Privacidade que especifique orientações sobre os direitos dos titulares dos dados e princípios gerais de protecção de dados pessoais. Não obstante esta exigência, a KPMG entende que as Organizações devem formalizar e publicar um conjunto adicional de regulação direccionado para fomentar a correcta aplicação das obrigações relevantes do RGPD (e.g. Avaliação de Impacto da Protecção de Dados, Protecção de Dados desde a Concepção e por Defeito, Direito ao Esquecimento, Direito à Portabilidade, Registo de Actividades de Tratamento de Dados, Gestão de Entidades Subcontratadas).

Um aspecto relevante da regulação prende-se com a definição de princípios para a contratação de parceiros externos que fazem o tratamento de dados pessoais. Nesta matéria, o RGPD eleva o nível de exigência, definindo regras para as diferentes etapas do ciclo de vida da relação com entidades contratadas, nomeadamente:

- Aferir a capacidade da entidade terceira em tratar os dados pessoais em conformidade com as obrigações impostas pelo RGPD, antes da mesma ser contratada.
- Formalizar instrumentos contratuais, com cláusulas específicas, que regulem as obrigações e direitos das duas partes.
- Implementar medidas de protecção dos dados, por parte da entidade contratada, após o término do contrato.

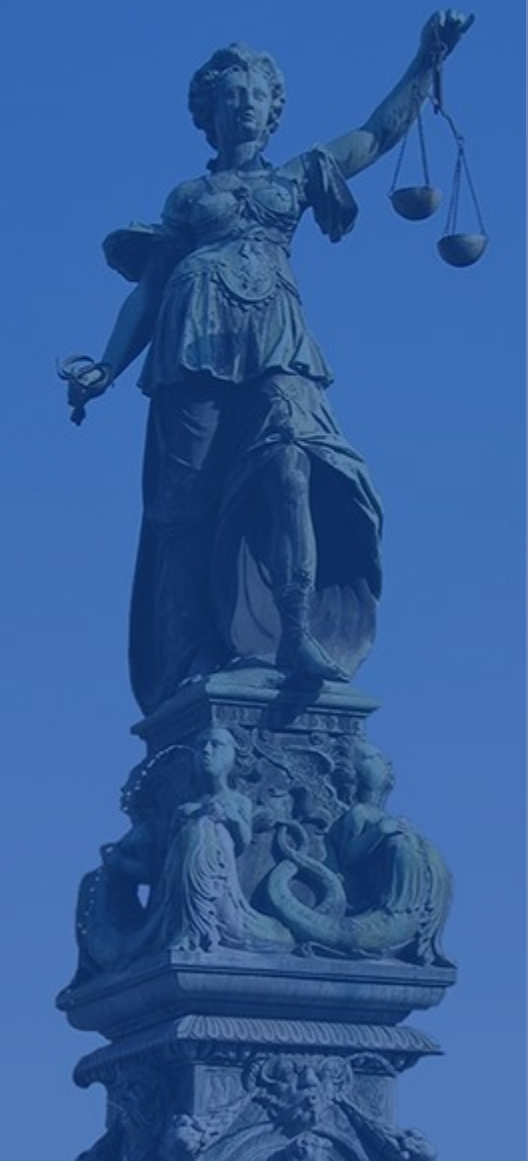
Para este efeito, é necessário que as organizações inventariem as entidades terceiras que têm acesso directo ou indirecto aos seus dados pessoais, e que revejam os instrumentos contratuais existentes, para que os mesmos estejam em conformidade com as obrigações impostas pelo RGPD.

Uma percentagem significativa dos incidentes ocorridos nas organizações têm origem interna, em resultado do erro humano, desconhecimento ou má aplicação dos normativos internos. Como forma de endereçar o aspecto que é muitas vezes qualificado como o elo mais fraco na cadeia de protecção dos dados – as pessoas, as organizações devem definir programas de sensibilização e formação em matéria de protecção de dados pessoais, que considerem:

- Exercícios de sensibilização (e.g. e-Learning, cartazes) direccionados para a generalidade dos colaboradores, apresentando mensagens sobre os comportamentos adequados em termos de protecção de dados pessoais.
- Acções de formação direccionadas para audiências específicas que lidem directa ou indirectamente com dados pessoais (e.g. Marketing, Recursos Humanos, Serviços de Apoio a Clientes, Gestão de Sistemas de Informação).

Estes programas são instrumentos eficazes para fomentar a consciência e o conhecimento dos colaboradores em matéria de protecção de dados pessoais.

Direitos dos Titulares



Resultados

Um dos fundamentos que esteve na origem do RGPD foi o reforço dos direitos dos cidadãos perante a forma como as organizações recolhem e utilizam os seus dados pessoais.

Com a aplicação do Regulamento, os dados pessoais só podem ser tratados no caso de existir um consentimento do titular, através de uma acção positiva e explícita no momento da recolha dos seus dados pessoais, sempre que o tratamento dos dados for baseado no consentimento. O RGPD exige ainda que seja mantida uma prova do consentimento prestado pelo titular dos dados.

Por outro lado, foram criados novos direitos do titular dos dados pessoais, após os dados estarem na custódia das organizações (e.g. direito à portabilidade dos dados, direito ao esquecimento dos dados).

Relativamente a estes aspectos, os resultados mostram que apenas:

- 23% cumprem, de forma integral, os requisitos definidos pelo RGPD em matéria de consentimento de recolha de dados pessoais.
- 15% instituem práticas que asseguram o direito ao esquecimento.
- 5% têm práticas para endereçar o direito à portabilidade dos dados.

Figura 12 – Consentimento para o tratamento de dados

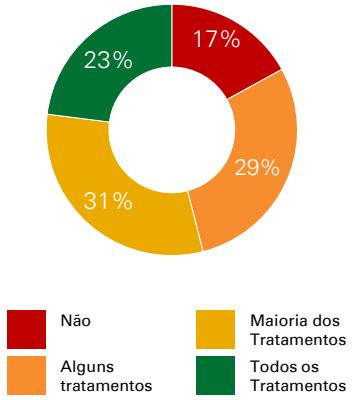
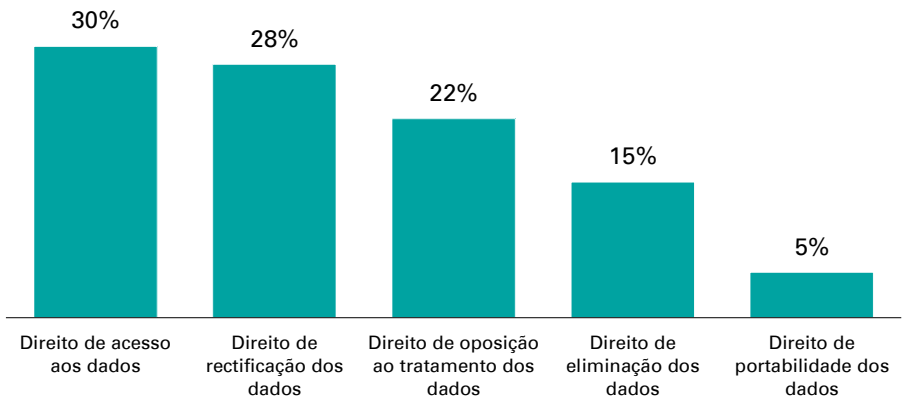


Figura 13 – Cumprimento dos direitos dos titulares



Perspectiva da KPMG

Os resultados do estudo indicam uma tendência natural para o cumprimento com os direitos já em vigor na actual legislação nacional de protecção de dados pessoais, e a tendência contrária para os novos direitos impostos pelo RGPD.

No que diz respeito aos processos de recolha de dados, as novas obrigações aplicam-se independentemente do suporte (e.g. formulários electrónicos, formulários em papel, voz), ou da forma como os dados são recolhidos (e.g. directamente junto do titular ou por terceira parte).

Esta nova forma de obtenção do consentimento pode trazer desafios, mais ou menos complexos, em função da multiplicidade de canais de recolha existentes e da especificidade intrínseca de cada canal.

Assim, a recolha e o tratamento de dados assente em plataformas tecnológicas que constituem hoje canais de comunicação importantes, como os sites Internet (onde se incluem o tratamento de dados pessoais registados em cookies), redes sociais, aplicações para dispositivos móveis (e.g. *smartphones*, *tablets*) e newsletters que utilizem *web beacons*, devem ser cuidadosamente avaliadas à luz dos novos requisitos do RGPD.

No que diz respeito ao direito ao esquecimento, um dos direitos mais exigentes estabelecidos pelo RGPD, o titular dos dados pode requerer o seu exercício em qualquer momento da sua relação com a organização. Para este efeito, as organizações devem ter capacidade para:

- Aferir da efectiva possibilidade de eliminação dos dados, face à existência de requisitos de retenção exigidos por outras obrigações legais ou regulamentares.
- Definir procedimentos de gestão da comunicação com o titular dos dados quando, por razões legais ou contratuais, o direito ao esquecimento não pode ser exercido.
- Assegurar a eliminação segura dos dados em todos os repositórios de dados físicos ou lógicos onde estes residem, incluindo nas cópias de segurança.
- Assegurar que o expurgo dos dados pessoais do requerente não compromete a integridade dos repositórios dos dados.

Princípios de Protecção, Minimização e Avaliação de Impacto

Resultados

O RGPD, em alinhamento com boas práticas internacionais de controlo e segurança da informação, introduziu três novos princípios de protecção de dados pessoais:

- Protecção de dados desde a concepção, que determina que os mecanismos de protecção dos dados pessoais devem ser pensados e implementados desde a concepção de um novo produto ou serviço.
- Protecção de dados por defeito, que determina que devem apenas ser recolhidos e tratados os dados pessoais mínimos necessários para cada finalidade específica de tratamento de dados, e conservados apenas durante o período considerado necessário para cada finalidade de tratamento.
- Avaliação de impacto sobre a protecção de dados pessoais, que requer a realização de uma avaliação de impacto sobre as operações de tratamento de dados pessoais, antes de serem efectuados tratamentos que possam acarretar riscos para os titulares dos dados (e.g. adopção de novas tecnologias, utilização de modelos analíticos).

As respostas obtidas, indicam que apenas:

- 14% cumprem com o princípio da protecção de dados desde a concepção, no contexto dos seus processos de implementação de novos produtos ou serviços.
- 12% definem antecipadamente os dados pessoais que são permitidos recolher no contexto de cada finalidade de tratamento de dados.
- 12% têm políticas de retenção e destruição de dados pessoais para todos os tratamentos de dados.
- 45% efectuam consistentemente análises de impacto aquando do lançamento de novas iniciativas relevantes que envolvam o tratamento de dados pessoais.

Figura 14 – Protecção de dados desde a concepção

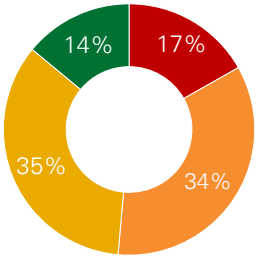


Figura 15 – Dados pessoais a recolher

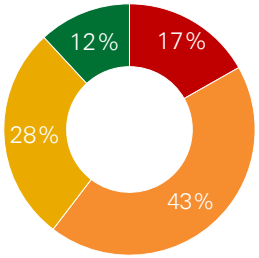


Figura 16 – Retenção de dados pessoais

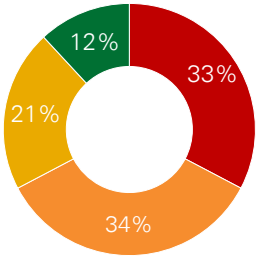
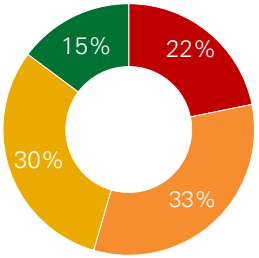


Figura 17 – Avaliação de impacto sobre os dados pessoais



Perspectiva da KPMG

Os resultados obtidos não surpreendem, uma vez que as organizações não têm o hábito de:

- Introduzir na fase de desenho de produtos ou serviços medidas específicas para protecção de dados pessoais.
- Limitar a recolha de dados somente ao que é considerado essencial para cada finalidade de tratamento.
- Implementar mecanismos de expurgo de dados pessoais, não obstante à luz do quadro legal actual estarem definidos períodos de retenção para diversas finalidades de tratamento (e.g. videovigilância, gestão de recursos humanos, gravação de chamadas para efeitos de prova contratual). Em muitos casos verifica-se que os dados só são destruídos quando é atingido o limite de espaço existente nos repositórios de armazenamento de dados.
- Efectuar, com maior ou menor formalismo, práticas de análise de risco, para determinar as medidas de protecção de dados apropriadas para endereçar os riscos identificados.

A implementação destes novos princípios vai obrigar a uma mudança cultural importante, pois requer que as organizações mudem a forma como habitualmente constroem e implementam serviços e produtos (e os sistemas de informação associados), e como fazem os tratamentos de dados pessoais.

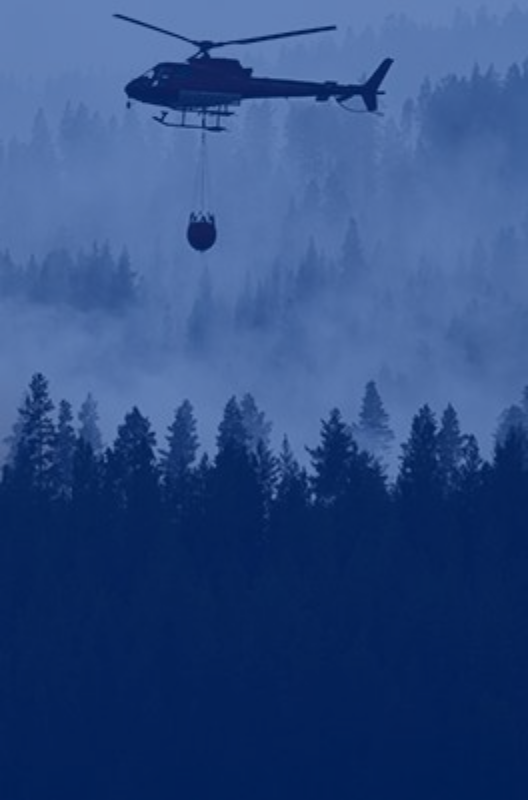
Como parte integrante desta mudança, as organizações devem identificar, *a priori*, os dados pessoais estritamente necessários para a cada finalidade de tratamento, antes de proceder à sua recolha junto dos titulares dos dados.

Adicionalmente, a definição de baselines de medidas de protecção (e.g. controlo de acessos, registos de auditoria, mecanismos de expurgo de dados, cláusulas contratuais) transversais para qualquer tratamento de dados pessoais pode ser um mecanismo facilitador e acelerador para a operacionalização dos requisitos do RGPD nas organizações.

Em função de uma avaliação de impacto para tratamentos de dados com maior nível de risco, poderão ser consideradas medidas adicionais (e.g. anonimização de dados, cifra dos dados) para protecção dos dados pessoais.

Para facilitar a implementação destes princípios as organizações devem definir metodologias que assegurem o seu cumprimento. Estas metodologias devem ser testadas antes da aplicação do RGPD em 2018, como forma de exercitar a sua implementação pelas várias áreas da organização responsáveis pelo tratamento de dados pessoais.

Mecanismos de Segurança e Resposta a Incidentes



Resultados

Face à tendência crescente de ameaças internas (e.g. colaboradores movidos por ganhos financeiros ou vingança) e externas (e.g. crime organizado dedicado ao ciber crime) nenhuma organização está a salvo de ocorrência de um incidente associado ao acesso, alteração ou eliminação indevida de dados pessoais. Aliás, é convicção corrente entre muitos especialistas de ciber segurança que a questão chave para a generalidade das organizações não é "se" mas "quando" vão ser vítimas de incidentes de segurança de informação.

As consequências destes incidentes podem ser várias e de elevada severidade, podendo conduzir a penalizações financeiras, custos operacionais e, não menos importante, provocar a degradação da imagem da organização afectada.

Assim, as organizações devem estar preparadas para prevenir, detectar e responder a incidentes que possam comprometer a sua informação em geral, e naturalmente, os dados pessoais que se encontram à sua guarda.

Os resultados do estudo mostram que as medidas mais populares nas organizações em Portugal para a protecção de dados pessoais, embora com percentagens de adopção absolutas baixas, são as seguintes:

- Mecanismos de controlo do acesso a dados pessoais baseados na função (21%).
- Autorização específica para acesso a dados pessoais sensíveis (15%).
- Rastreabilidade de acessos a dados pessoais (13%).

Por outro lado, o RGPD estabelece novas regras de reporte à Autoridade de Controlo e aos titulares dos dados afectados em caso de incidente. Nesta matéria o panorama também não é positivo, uma vez que 57% das organizações referem não ter processos instituídos para responder a incidentes relacionados com dados pessoais. Numa análise detalhada às respostas dadas, evidenciam-se pela negativa os sectores Público e Retalho, estando do lado oposto os sectores dos Serviços e Financeiro.

Figura 18 – Medidas de segurança

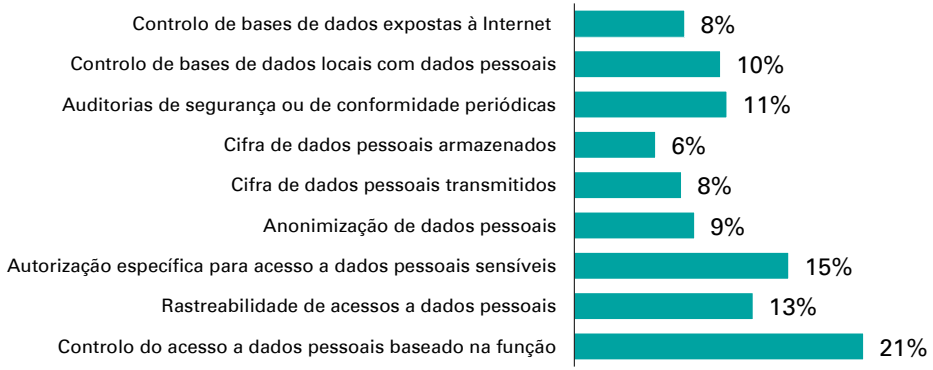
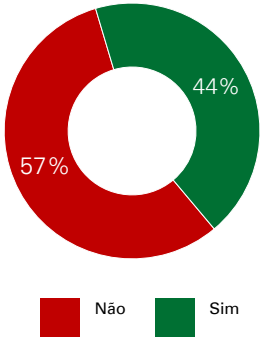


Figura 19 – Processos de resposta a incidentes



Perspectiva da KPMG

O RGPD não define de forma objectiva quais as medidas de segurança que devem ser implementas para protecção de dados pessoais, delegando nas organizações a identificação e implementação destas medidas em função do risco a que se encontram expostos os dados pessoais.

É nossa convicção que as organizações devem definir e implementar uma estratégia integrada de ciber segurança para a protecção dos dados pessoais, que enderece de forma holística os diferentes riscos internos e externos a que se encontram expostos os dados pessoais, considerando o actual contexto de risco, em que:

- Os ciber ataques são cada vez mais sofisticados, demonstrando um conhecimento profundo do negócio e dos sistemas de informação.
- As organizações não estão preparadas para identificar, caracterizar e responder a incidentes.
- O tempo de reporte de incidentes à Autoridade de Controlo / titulares dos dados é muito reduzido.

Esta estratégia de ciber segurança deve ser concebida através da:

- Identificação objectiva dos diferentes vectores de ameaça, internos e externos, que podem comprometer a confidencialidade, integridade e disponibilidade dos dados pessoais.
- Implementação de mecanismos de ciber segurança (tecnológicos e processuais) para prevenir a ocorrência das ameaças identificadas, tendo por base uma análise de custo-benefício.
- Implementação de mecanismos de ciber segurança que permitam rastrear e monitorizar o acesso a dados pessoais. Esta monitorização deve contemplar as várias dimensões do acesso, nomeadamente, acessos aplicacionais dos colaboradores e acessos em modo privilegiado por parte das equipas de gestão de sistemas de informação.
- Definição de responsabilidades e procedimentos operacionais de resposta a incidentes com dados pessoais.
- Realização de exercícios periódicos de resposta a incidentes utilizando cenários plausíveis e concretos relacionados com dados pessoais.

Novas Tecnologias

Qual a relação entre o RGPD e as novas tecnologias?

"Informação é o petróleo do século 21 e os modelos analíticos o motor de combustão"

Peter Sondergaard
Senior Vice President – Gartner Research – Press Release da Gartner, 17 de Outubro de 2011

Resultados

Cerca de 55% das organizações participantes no Estudo afirmam que não armazenam dados pessoais na *cloud*.

Por outro lado, existe uma tendência clara para as organizações coleccionarem grandes volumes de dados (estruturados e não estruturados), oriundos das mais diversas fontes internas ou externas (e.g. redes sociais, aplicações móveis, cartões de fidelização), sobre os quais aplicam modelos analíticos para obter padrões comportamentais ou outros.

Apenas 12% das organizações refere que utiliza modelos de *Big Data/Data Analytics* sobre os dados pessoais que recolhe. No entanto, 44% reconhece estar numa fase exploratória de utilização destas soluções.

Figura 20 – Adopção *cloud*

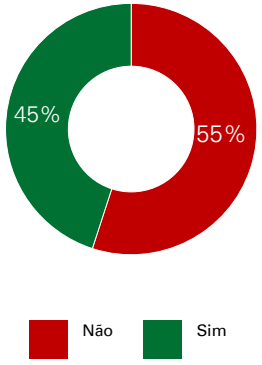
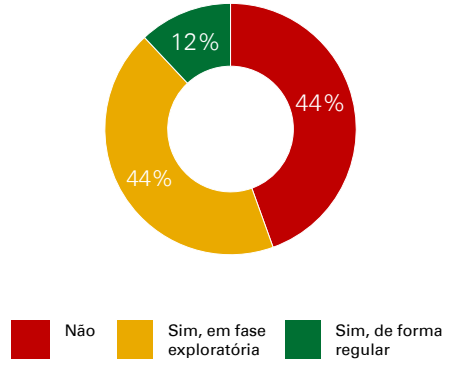


Figura 21 – Adopção *Big Data*



Perspectiva da KPMG

A adopção de serviços na *cloud*, além das naturais vantagens operacionais e financeiras, traz potenciais riscos para as organizações, que devem ser identificados e geridos. A *cloud* é um tópico que merece reflexão por parte das organizações que já a adoptaram ou que estão em vias de o fazer, face à natureza e sensibilidade dos dados pessoais que podem ser armazenados em infraestruturas externas ao perímetro da organização.

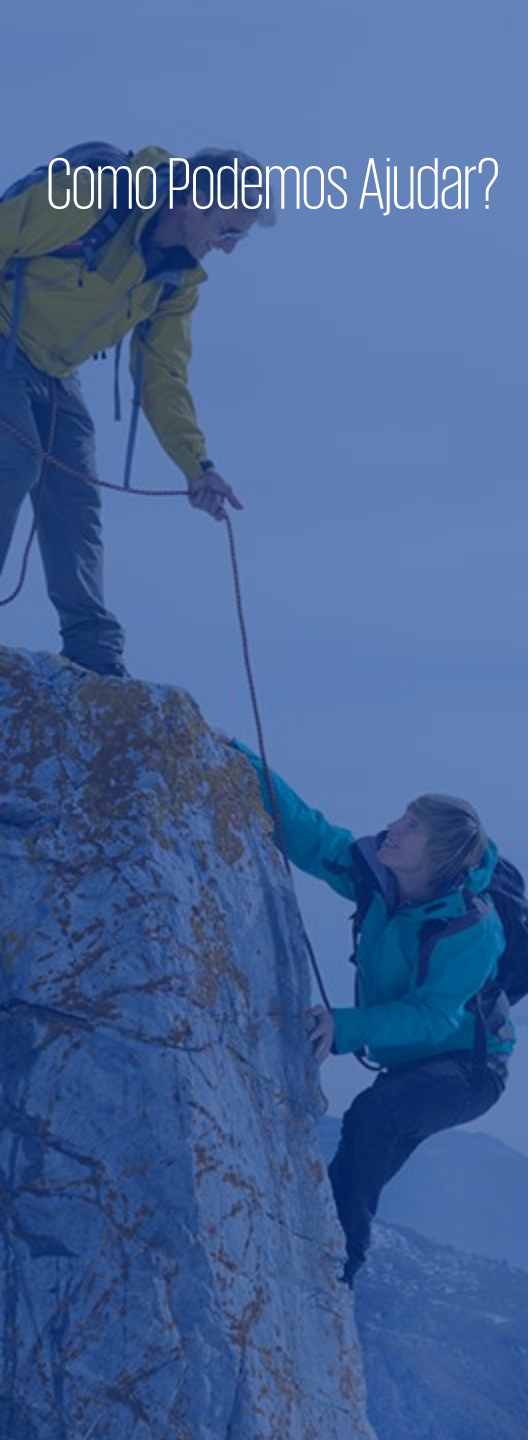
As organizações devem assim analisar um conjunto de tópicos relevantes por forma a assegurar a conformidade com o RGPD, nomeadamente:

- Localização geográfica onde os dados pessoais estão armazenados ou partir de onde podem ser directa ou indirectamente acedidos pelo prestador de serviços *cloud*.
- Disponibilização pelo prestador de serviços *cloud* de instrumentos contratuais adequados face aos requisitos do RGPD.
- Capacidade do prestador de serviços *cloud* em implementar medidas de controlo e segurança para protecção adequada do dados pessoais, em função do modelo cloud em causa (e.g. SaaS, PaaS, IaaS), em conformidade com boas práticas internacionais de segurança para ambientes *cloud*.

Adicionalmente, devem ser realizados exercícios de avaliação de impacto da protecção de dados, tendo por âmbito os tratamentos de dados efectuados na *cloud*, uma vez que a adopção da *cloud* pode trazer potenciais riscos para os titulares dos dados.

Relativamente ao *Big Data*, apesar de haver ainda um potencial significativo por explorar em Portugal, as organizações devem considerar que a utilização de modelos analíticos (e.g. análise de perfis de consumo, preferências, tendências) requer o cumprimento das diferentes regras impostas pelo RGPD, incluindo a:

- Manutenção de um registo actualizado dos tratamentos de dados efectuado através do *Big Data/Data Analytics*.
- Obtenção do consentimento explícito por parte dos titulares dos dados para a(s) finalidade(s) de utilização dos dados endereçadas pelo *Big Data/Data Analytics*.
- Utilização exclusiva dos dados para fins compatíveis com os autorizados pelos titulares dos dados.
- Aplicação, caso necessário, de mecanismos tecnológicos de protecção dos dados analisados (e.g. anonimização ou pseudonimização dos dados pessoais).



Como Podemos Ajudar?

Porquê a KPMG

A KPMG tem apoiado com sucesso inúmeras organizações, em Portugal e a nível internacional, de diferentes sectores de actividade, na conformidade com obrigações legais de protecção de dados pessoais.

Equipa com experiência comprovada

A KPMG Portugal possui uma área especializada em protecção de dados pessoais, que inclui profissionais experientes, com competências nas diversas dimensões relevantes. Os nossos profissionais têm:

- Conhecimento profundo das actuais leis e regulamentos de protecção de dados pessoais e do RGPD.
- Experiência em boas práticas de protecção de dados pessoais.
- Visão holística sobre a protecção de dados pessoais, na perspectiva da organização, processos e tecnologia.
- Experiência comprovada em realizados em inúmeros sectores (e.g. financeiro, retalho, energia, telecomunicações).

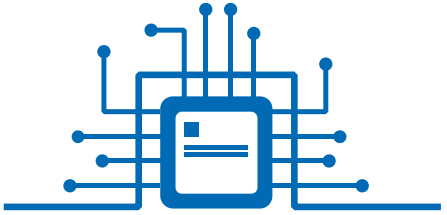
Recursos globais

A KPMG possui um Centro de Excelência em Data Privacy, com recursos que desenvolvem metodologias internacionais aplicadas pelas várias firmas da KPMG.

Este centro permite aos nossos clientes o acesso a melhores práticas na avaliação, implementação e monitorização da conformidade com obrigações europeias de protecção de dados pessoais.

Este centro têm ainda uma relação próxima com reguladores e grupos de trabalho europeus sobre temas de protecção de dados pessoais.

A KPMG coloca à disposição dos seus clientes recursos e metodologias de trabalho provenientes deste Centro de Excelência.



Uma abordagem pragmática, suportada em aceleradores

Como parte das nossas metodologias, utilizamos diversos instrumentos facilitadores, criados pelo nosso Centro de Excelência de Data Privacy, adaptados para a realidade Portuguesa, que permitem aumentar a eficácia e qualidade da colaboração prestada pela KPMG.

Entre estes facilitadores, encontra-se:

- Framework de inventariação RGPD, que contem os elementos necessários para a inventariação e caracterização das actividades de tratamento de dados pessoais.
- Framework de avaliação RGPD, que instancia as diversas obrigações legais em matéria de protecção de dados pessoais em controlos objectivos e pragmáticos, de natureza processual e tecnológica.

Os Nossos Serviços

Os serviços de Data Privacy da KPMG apoiam os nossos clientes a garantir e gerir a conformidade com o RGPD, endereçando as vertentes legais, negócio, sistemas de informação e ciber segurança. Estes serviços baseiam-se em quatro *work-streams*, adaptáveis às necessidades específicas dos nossos clientes.

1 Inventariar

Inventariar e caracterizar as actividades de tratamento de dados pessoais

- Definir o dicionário RGPD
- Definir a taxonomia de dados pessoais
- Caracterizar as finalidade de tratamentos de dados pessoais
- Identificar os repositórios de dados pessoais
- Identificar entidades subcontratadas que fazem tratamentos de dados pessoais e respectivos instrumentos contratuais
- Identificar transferências internacionais de dados pessoais
- Identificar prazos de retenção

2 Avaliar

Definir o programa de transformação

- Identificar áreas de inconformidade com o RGPD
- Avaliar o risco de não conformidade com o RGPD
- Avaliar o custo/benefício das potenciais soluções de conformidade a implementar
- Definir programa de transformação

3 Transformar

Implementar o plano de transformação

- Definir modelo de governo de privacidade
- Definir normativos de protecção de dados pessoais
- Definir requisitos de TI e segurança da informação
- Realizar avaliação de impacto na protecção de dados pessoais
- Realizar acções de formação e sensibilização sobre a utilização e protecção de dados
- Gerir o programa de transformação
- Implementar outras alterações a nível jurídico, processual ou tecnológico

4 Manter

Gerir e monitorizar a conformidade com o RGPD

- Embeber o tema da protecção dados nos processos de criação de novos produtos, serviços, desenvolvimento de sistemas e gestão das alterações
- Definir mecanismos de monitorização do cumprimento do RGPD
- Definir mecanismos de melhoria contínua

Sobre o Estudo

O *Survey* Impacto do Regulamento Geral de Protecção de Dados em Portugal foi uma iniciativa promovida pela KPMG Portugal com o objectivo de tomar o pulso às práticas de protecção de dados pessoais e ao grau de preparação de diferentes sectores de actividade da economia portuguesa para as exigências impostas pelo RGPD.

Foi considerado um total de 7 sectores de actividade: Público, Serviços (energia, telecomunicações, transporte, turismo e electrónica), Seguros, Financeiro, Indústria (automóvel e produtos diversificados), Retalho e Saúde (cuidados de saúde e farmacêutico).

O Estudo, que reflectiu o ponto de vista de 101 organizações, foi conduzido entre Novembro de 2016 e Janeiro de 2017, através de respostas a um questionário *online* utilizando uma plataforma de *Surveys* da KPMG.

A avaliação dos resultados foi realizada pela equipa de especialistas de Data Privacy da KPMG Portugal.

Figura 22 – Dimensão das organizações

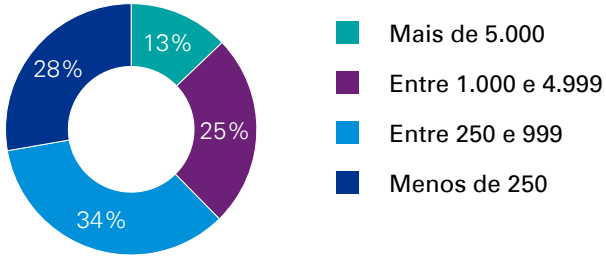
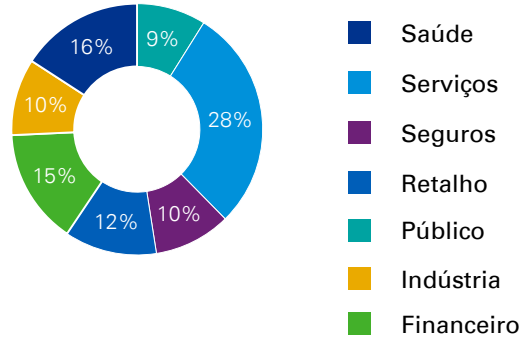


Figura 23 – Participação por sector



kpmg.pt