



Os primeiros passos para o RGPD

Regulamento Geral de Proteção de Dados

Índice

Introdução	03
Conceitos básicos sobre o RGPD	04
Prepare a sua empresa para Maio de 2018	09
A criação do processo RGPD	14
A tecnologia pode ajudar	17
Workshop RGPD na prática	22

Introdução

A privacidade ou falta dela, a globalização, a evolução da tecnologia, as diferentes formas de fazer negócio e a mudança no método de fidelizar clientes, colocaram o tratamento de dados pessoais na agenda da união europeia, com o novo regulamento de proteção de dados.

Hoje em dia, ouvimos falar de "proteção de dados pessoais" e muitas vezes, mal-entendemos o verdadeiro significado do conceito.

É vital ter em conta que o surgimento do RGPD veio ao encontro de uma necessidade social real, originada a partir de um contexto económico, político e cultural, representada em forma de lei pelo novo RGPD.

Atualmente a troca de dados é vital em qualquer negócio. As empresas têm que adotar um modelo operacional mais ágil e rápido para responder às novas exigências de mercado. As fontes de dados e o propósito para o seu processamento sofreram uma profunda alteração ao longo dos tempos, como resposta às novas exigências, permitindo simplificar o nosso dia a dia, mas originando, por outro lado, uma maior dispersão e falta de controlo dos dados.

O novo quadro legal traz algumas mudanças significativas que terão diferente impacto na vida das organizações, consoante a sua natureza, área de atividade, dimensão e tipo de tratamentos de dados pessoais que realizem.

A Arentia neste documento, através da análise de varias fontes de informação, facilita o entendimento do conceito de RGPD e sugerimos alguns dos passos preliminares necessários para estar em conformidade em Maio de 2018.

Capítulo 1

Conceitos iniciais sobre o RGPD

O que é o RGPD?

O Regulamento Geral de Proteção de Dados (RGPD), uniformiza o tratamento de dados pessoais de todos os indivíduos na Europa, inclusive quando esses dados circulam fora da Europa.

O RGPD foi adotado em 27 de Abril de 2016 e entra em vigor em 25 de maio de 2018, substituindo a atual diretiva 95/46 CE.

“Agora essa autorização desaparece e todo o ônus passa para as empresas e entidades públicas. Têm que ser elas a demonstrar que estão a cumprir todas as ordens que vêm no regulamento”

CNPD, Clara Guerra

O que são dados pessoais

Qualquer informação relativa a uma pessoa singular que pode ser identificada, direta ou indiretamente por um identificador, como o nome, número de contribuinte, e-mail, género, fotografia, localização, identificador online, fatores físicos, fisiológicos, culturais ou sociais.

São considerados dados sensíveis, os que revelam origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, associação sindical, dados biométricos e dados sobre saúde ou vida sexual.

Não há distinção entre dados pessoais no contexto pessoal ou profissional, a pessoa é a pessoa. Quanto aos menores de 16 anos, o tratamento só é lícito quando o consentimento é autorizado pelos titulares das responsabilidades parentais da criança.

Os dados podem ser transmitidos de forma verbal ou escrita e armazenados no formato físico (ex. papel) ou digital (ex. suporte informático).

Os primeiros passos para o RGPD



Os direitos das pessoas com o RGPD

1. **O direito ao acesso** - significa que as pessoas têm o direito de solicitar o acesso aos seus dados pessoais e questionar como estão a ser utilizados. A empresa deve fornecer cópia dos seus dados pessoais, gratuitamente, sempre que solicitado.
2. **O direito á portabilidade dos dados** - as pessoas têm o direito de transferir os seus dados de um fornecedor para outro de uma forma automática.
3. **O direito de corrigir a informação** - garantia que as pessoas possam atualizar os seus dados se estiverem desatualizados, incompletos ou incorretos.
4. **O direito de restringir o processamento** - as pessoas podem solicitar que os seus dados não sejam processados, ou seja, o registo pode permanecer na empresa mas não pode ser utilizado.
5. **O direito de objeção** - inclui o direito de não receber informação de marketing direto. Não existem isenções, a partir do momento que o pedido for recebido, os envios de informação devem ser cancelados de imediato.

6. O direito de ser informado

As empresas devem informar sempre de uma forma clara, simples e prévia, qual vai ser a utilização dos dados recolhidos. Além disso, o consentimento nunca deve ser implícito ou a troco de alguma oferta, mas sim livre e gratuito. Isto aplica-se em qualquer tipo de recolha de dados, seja física ou virtual.

7. O direito de ser esquecido

A pessoa pode pedir para ser excluída dos registos da empresa, desde que os dados deixem de ser necessários para o qual foram recolhidos.

8. O direito de ser notificado

Sempre que existir uma violação de dados que comprometa os dados pessoais, a pessoa tem o direito de ser informado no prazo de 72 horas após ter ocorrido.

A quem se aplica

O RGPD aplica-se a todas as empresas que com instalações na UE e/ou que processam e/ou armazenam dados pessoais de pessoas que residem ou viajam na UE.

Mesmo que a empresa esteja fora da EU, mas processe dados pessoais de pessoas que estão na EU, têm de estar conforme.

Coimas

As multas pelo não cumprimento da RGPD são as maiores até hoje. Podem ir desde uma multa até € 20 milhões ou 4% do volume de negócios anual (o que for maior).



Capítulo 2

Prepare a sua empresa para Maio de 2018

Próximos passos (comece ainda hoje)

Uma das palavras chave do RGPD é a privacidade por design, ou seja, exige que a proteção de dados seja pensada e incluída desde início em qualquer processo que inclua tratamento de dados. A proteção de dados deve ser uma preocupação constante na sua empresa.

O primeiro passo é aumentar o grau de conhecimento desta regulamentação ao nível da administração e direção da empresa e identificar qual o atual nível de preparação da sua organização.

Para ajudá-lo neste procedimento temos ao seu dispor um Workshop dedicado à sua empresa, com duração de meio dia, onde poderá esclarecer os conceitos, podendo através da realização de uma pequena avaliação descobrir qual o nível de preparação atual e quais as necessidades da sua organização para estar de acordo com a regulamentação.

Os passos seguintes incluirão:

- a análise da informação de que a sua organização necessita para a sua operacionalidade e a forma como a gere, comunica e armazena;
- a criação de políticas de proteção de dados e de programas para a mudança da cultura dos funcionários;
- a análise da infraestrutura de suporte aos dados;
- a implementação de medidas de segurança;
- a criação de processos de gestão de proteção de dados incluindo, o alinhamento com os seus fornecedores, incluindo-os no processo de gestão de proteção de dados.

Atenção que a terciarização não isenta a sua empresa de responsabilidade.

A importância do suporte informático para o armazenamento e processamento dos dados confere a esta componente uma maior relevância, sendo por isso necessário a implementação de medidas adequadas à confidencialidade, integridade e disponibilidade dos dados. O ponto 49 da RGPD evidencia claramente esta necessidade.



Data protection officer (DPO)

O RGPD introduz uma nova figura que é o Encarregado da Proteção de Dados, que tem como responsabilidade supervisionar e assegurar a implementação e manutenção do RGPD.

O Encarregado da Proteção de Dados, pode ser nomeado internamente (desde que não realize outras tarefas que possam resultar em conflito de interesses), reportando ao mais alto nível da organização, podendo complementarmente recorrer a serviços especializado de aconselhamento para esta matéria.

O DPO é obrigatório para todas as autoridades públicas e onde as atividades principais envolvem o tratamento, armazenamento e monitorização regular e sistemático de dados pessoais em grande escala ou dados sensíveis, que revelam origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, associação sindical, dados biométricos e dados sobre saúde ou vida sexual.

Além das situações previstas em que o DPO é obrigatório, pode decidir ter um encarregado de proteção de dados na sua organização, pelas evidentes vantagens que tal pode significar para o cumprimento das obrigações, tais como: informar e aconselhar os responsáveis pelo processamento de dados nesta matéria, aconselhar os colaboradores e ser o representante da organização para a CNPD e clientes finais, funcionando como ponto único de contato.



Formação

Finalmente e não menos importante, a tecnologia pode ajudar a cumprir, mas de nada vale, se as pessoas na sua empresa não tiverem alinhadas e consensualizadas com a importância do correto tratamento dos dados pessoais.

A formação contínua é de extrema importância para conseguir implementar e assegurar a continuidade do novo RGPD.



Capítulo 3

A criação do processo RGPD

Competências

A Arentia inclui agora na sua oferta, os serviços de consultoria necessários para ajudar a sua organização a criar o processo de gestão de proteção de dados, desde:

- ❖ Análise inicial;
- ❖ Definição de políticas correspondentes;
- ❖ Análise de risco;
- ❖ Definição das medidas de proteção a implementar;
- ❖ Criação de planos de sensibilização e formação internos para a mudança de hábitos dos funcionários;
- ❖ Definição de planos de ensaio de simulação de falha da proteção dos dados;
- ❖ Criação de processo de gestão de incidentes, assim como a ligação do processo a outros absolutamente cruciais para aumentar a resiliência da organização, como o processo de gestão de crise.

A equipa inclui consultores com certificações nos standards de mercado para estas temáticas como ISO 22301, ISO 27001 e DPO e consultor jurídico com especialização nesta matéria.



O serviço de DPO externo também faz parte do nosso portfólio de serviços, permitindo à sua organização um apoio especializado nesta matéria para a gestão continuada do processo, alinhamento constante com alterações internas e/ou de requisitos ou regulamentações, auditorias internas e externas.

Capítulo 4

A tecnologia pode ajudar

A Arentia pode ajudar

A Arentia atua no mercado empresarial de software de gestão e tecnologias de informação. Conta com uma equipa de profissionais qualificada que garante o bom desempenho nas áreas em que atua.

Reunimos um conjunto de boas normas que ajudam a implementar o RGPD, de certeza que muitas delas já fazem parte do seu dia a dia, no entanto é bom recordar.



Atualizações

Sempre que estão disponíveis novas atualizações, principalmente as relacionadas com segurança, devem ser aplicadas o mais rapidamente possível.

Antivírus

Utilize software de antivírus de qualidade e mantenha-o atualizado. Garantir que está atualizado assegura a proteção contra as ameaças mais recentes.

Cifragem de dados pessoais

Mencionado no Artigo 32 do RGPD, além das sugestões já enunciadas, a cifragem é uma das técnicas sugeridas para a proteção de dados pessoais.

Disaster recovery

Recupere os sistemas e os dados da sua organização aconteça o que acontecer. Aplique o plano de recuperação em caso de falha.

Os primeiros passos para o RGPD

Cópias de segurança

Regularmente deve realizar cópias de segurança. Após identificar os dados críticos, faça e mantenha cópias de segurança.

Proteção unificada da rede

Verifique e teste o nível de proteção da sua rede. Normalmente a Firewall é o primeiro nível de proteção. Garanta que só deixa entrar e sair os dados que interessam.

Gestão de acessos

Os ERP's PHC e Primavera, estão a desenvolver soluções que vão permitir um controlo completo de acessos, através de um conjunto de funcionalidades que centralizam o controlo dos seus processos de tratamento de dados e capacidade analítica dos mesmos.



Os primeiros passos para o RGPD



INFORMÁTICA

- Ciências informáticas
- Informática na óptica do utilizador
- Informática - programas não classificados noutra área de formação

Formação

A maior parte das vezes a falha é humana, com o aumento do ransomware é muito importante manter uma cultura de segurança consciente.

Se o colaborador clicar em um link ou abrir um ficheiro mal-intencionado, pode despoletar o ataque.

Na Arentia temos formações específicas ministradas por especialistas que ajudam a desmistificar e a entender estas ameaças de uma forma mais consciente.

Capítulo 5

Workshop RGPD na prática

Marque na sua agenda

Participe no workshop a realizar em Leiria, na presença de consultores certificados nos standards de mercado para estas temáticas como ISO 22301, ISO 27001 e DPO e consultor jurídico com especialização nesta matéria.

RESERVE A DATA

WORKSHOP RGPD NA PRÁTICA

28.02.18

[REGISTE-SE AQUI](#)





Lisboa - Leiria

211 165 266 – 244 882 666

comercial@arentia.pt

www.arentia.pt