E3S

ASSOCIAÇÃO APOIO À EXCELÊNCIA NO 3º SETOR

Secção do puzzle: **Legislação**

Peça: **Regulamento Geral de Protecção de dados – garantir a conformidade**

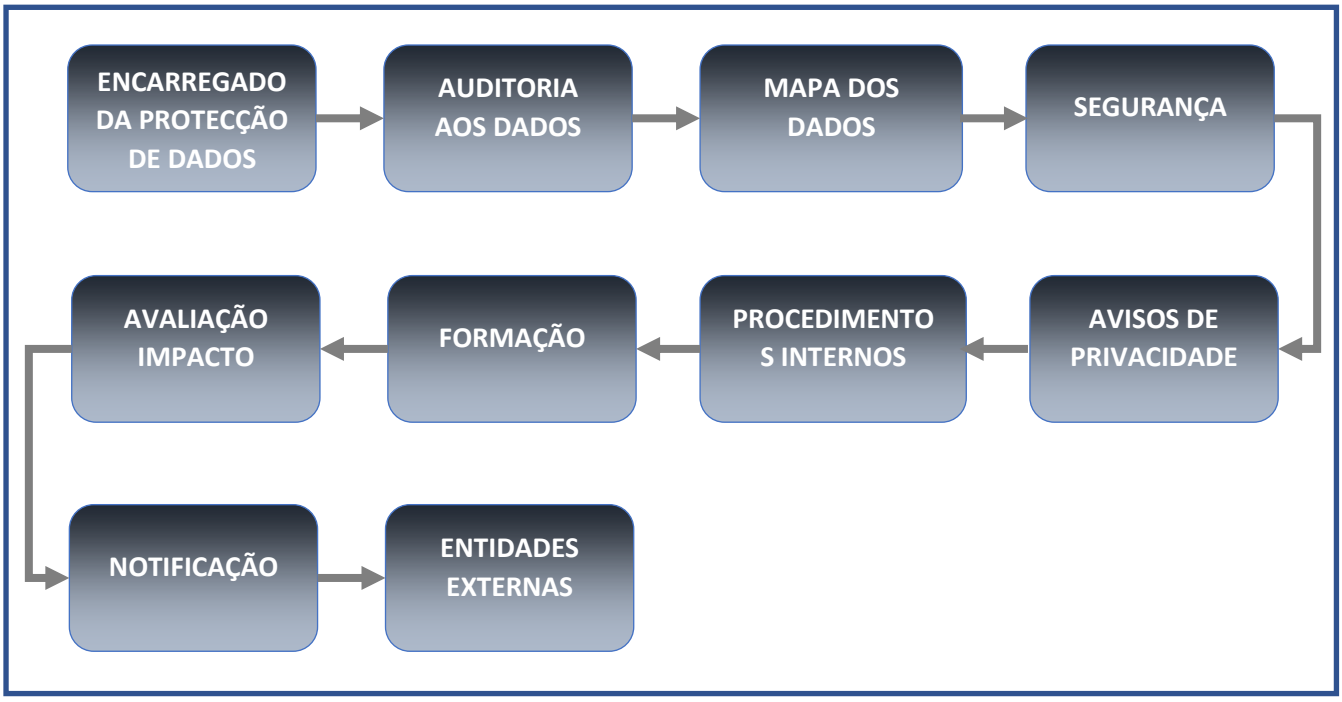
junho 2020

Outras peças relacionadas com este tema:

- Regulamento Geral de Protecção de dados- preparar a conformidade

Índice

Roteiro para a aplicação do RGPD



1. Encarregado da Protecção de dados

Art. 37º - A Organização tem obrigatoriamente de designar um EPD se:

- For uma entidade pública;
- Realizar atividades de monitorização de indivíduos em larga escala (comportamentos online, etc.);
- A actividade core consistir no processamento de categorias especiais de dados em larga escala (estas categorias especiais são, por exemplo, raça, religião, saúde, vida sexual, orientação sexual) ou dados criminais.

Nota: Um EPD pode ter outras funções dentro da Organização

Art. 39º - O que tem o EPD que fazer?

- Assessorar a organização em todos os assuntos relacionados com RGPD e as leis de protecção de dados
- Monitorizar a conformidade com o RGPD
- Prestar apoio nas avaliações de risco sobre protecção de dados
- Gerir os riscos do processamento de dados
- Relacionar-se com os Reguladores
- Ser o ponto de contacto com tudo o que estiver relacionado com proteção de dados

Nota: O EPD tem de operar de forma independente e reportar diretamente à Direcção.

O Regulador e os clientes têm de saber quem é o EPD e como contatá-lo.

2. Auditoria aos Dados

Esta Fase irá permitir efectuar o inventário dos dados, de forma a preparar um mapa dos dados e os diagramas de fluxo.

Os objectivos são:

- Saber onde estão os dados;
- Como são processados;
- Duração do seu armazenamento;
- Nível de segurança;
- Para onde são enviados;
- Quais os suportes legais para o seu processamento;
- Que controlos estão implementados;
- O que é necessário fazer para atingir a conformidade;
- Identificação das áreas/departamentos que recolhem, armazenam e tratam dados e a pessoa responsável;
- Preparar questionários por departamento;
- Envio e preparação (briefings e coaching);
- Sessões de seguimento.

Nota: Os Dados estão relacionados com Clientes, Fornecedores, Terceiros e Empregados.

3. Mapa dos Dados

Depois de inventariar os dados da organização, é necessário registar como os dados são utilizados, nomeadamente com são processados.

Os objectivos desta Fase são:

- Perceber os fluxos de dados dentro da organização
- Como são partilhados
- Quem tem acesso
- Com quem são partilhados
- Para que entidades são enviados

Com o desenho dos fluxos de dados, é efectuada a avaliação de risco com informação sobre a probabilidade de ocorrência de fuga de informação e as acções preventivas a adoptar para minimizar essa probabilidade.

Principais acções:

- Desenhar os fluxos de dados
- Elaborar o relatório de auditoria aos dados
- Elaborar a identificação dos riscos

4. Segurança

O RGPD tem como principal objectivo garantir a segurança e a privacidade dos Dados Pessoais.

- O Regulamento prevê a aplicação de multas avultadas quando as Organizações permitem fugas de informação.
- Os processadores de dados podem ser multados se não tiverem os dados seguros e existe a obrigação de notificação quando existir uma fuga de informação.

Nesta fase são inspecionados os riscos de segurança nas seguintes áreas:

- Edifício
- Sistemas informáticos
- Empregados
- Políticas e procedimentos
- Terceiros (entidades externas que se relacionam com a Organização)

Principais acções:

- Criar a Tabela de Segurança dos Dados (onde estão os dados e como é garantida a segurança)
- Avaliação dos riscos (Sistemas, Terceiros, Trabalhadores, Políticas e Procedimentos)
- Analisar a Ciber segurança
- Criar o Plano de Resposta à Violação dos Dados (o que fazer, quem informar)

5. Avisos de privacidade

O Aviso de Privacidade é a informação a fornecer aos donos dos dados, dando conhecimento sobre a forma e a finalidade com que os seus dados são utilizados pela Organização.

Um Aviso de Privacidade pode ser a "Política de Privacidade" da Organização na página de um website, um Aviso Legal num documento escrito ou uma informação por telefone a dizer que a chamada irá ser gravada.

O que diz o RGPD sobre as Políticas de Privacidade.

De acordo com o Artigo 5º do RGDP os dados pessoais deverão ser:

a) 0bjeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («**licitude, lealdade e transparência**»);

b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades («**limitação das finalidades**»);

c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («**minimização dos dados**»);

d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («**exatidão**»);

e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados («**limitação da conservação**»);

f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («**integridade e confidencialidade**»).

A Organização tem que ser capaz de cumprir com o disposto neste Artigo e tem de poder comprová-lo («**responsabilidade**»).

Política de Privacidade

A Política de Privacidade deve estabelecer a forma como a Organização utiliza os dados pessoais dos seus clientes e dos seus potenciais clientes e deve ser composta pelas seguintes secções:

- Quem é responsável pelo tratamento dos seus dados pessoais
- Como é que recolhemos os seus dados pessoais e que dados pessoais podem ser recolhidos
- Para que finalidades e com que fundamento podem ser utilizados os seus dados pessoais
- Como é que mantemos os seus dados pessoais seguros
- Durante quanto tempo conservamos os seus dados pessoais

- Com quem podemos partilhar os seus dados pessoais e como é que os mantemos seguros
- Como é que pode alterar ou retirar seu consentimento
- Como entrar em contacto connosco, os seus direitos de proteção de dados e o direito de apresentar reclamação junto da sua autoridade de controlo

6. Procedimentos internos

Existe um conjunto de Políticas e Procedimentos que têm que ser implementados ao abrigo do RGPD.

É necessário avaliar as políticas actuais da Organização, adequá-las e descrever as novas políticas.

Estas políticas deverão abranger os seguintes temas:

- Política de protecção de dados
- Política de retenção de dados
- Política de tratamento de incidentes de violação de dados
- Recursos humanos e política de protecção de dados
- Marketing e política de protecção de dados
- Comunicação social e política de protecção de dados
- Definição e implementação dos meios que possibilitarão responder aos pedidos de portabilidade dos dados.

Art. 24.º, 1. - Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

Documentação detalhada do tratamento dos dados pessoais

Todos os processos e atividades relacionadas com o tratamento de dados devem ser documentados de forma detalhada, de modo a que a organização consiga demonstrar o cumprimento de todas as obrigações decorrentes do novo regulamento.

7. Formação

A formação dos colaboradores é uma das fases mais importantes para a aplicação do RGPD

São os colaboradores que vão lidar diariamente com os dados e precisam saber o que fazer para estar em conformidade.

(Um estudo recente revelou que 37% das "violações de dados" foi causada por erro humano)

Será necessário dar formação de base a todos os colaboradores e formação especializada às pessoas com funções mais críticas no acesso e processamento dos dados.

8. Avaliação do impacto

O artigo 35.º introduz o conceito de Avaliação de Impacto sobre a Proteção de Dados (AIPD)

Uma AIPD é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos.

As AIPD ajudam os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas adequadas para assegurar a conformidade com o regulamento.

Por outras palavras, **uma AIPD é um processo que visa estabelecer e demonstrar a conformidade.**

Os objetivos são:

- Detalhar os riscos potenciais de cada projeto
- Listar os cenários de mitigação desses riscos, com recomendações
- Ter um registo confirmando que a pessoa responsável tomou conhecimento desses riscos
- Assegurar que os riscos são monitorizados e que as recomendações são seguidas

9. Notificação

De acordo com o Art. 33º do RGPD, existe uma obrigação legal de as Organizações reportarem as fugas de informação significativas ao Regulador.

Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada. (Art. 34º)

A probabilidade de uma Organização sofrer uma falha na proteção de dados é muito elevada.

É fundamental ter um Plano e a equipa preparada para responder de forma eficaz e conforme o Regulamento, de forma a evitar custos que podem ser muito elevados.

10. Entidades externas

Art. 28.º, 3. - O tratamento em subcontratação é regulado por contrato ou outro ato normativo que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do

tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento. (…)

Quando a Organização partilha informação com uma entidade externa, é necessário verificar se as cláusulas contratuais necessárias para a conformidade com o RGPD estão contempladas.

É necessário avaliar os cenários onde a empresa actua como Controlador de Dados ou como Processador de Dados (em nome de um controlador).

11.Cronograma de implementação

12. Sugere-se que a aplicação deste roteiro se realize com a metodologia de execução de projectos, sendo fundamental a elaboração do respectivo cronograma.

	Fases	Actividades	Dias	Semana 1					Semana 2					Semana 3					Semana 4				
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	Enc. Protecção Dados	Caracterizar, identificar e preparar	1																				
2	Auditoria aos Dados	Identificação das áreas/departamentos e pessoa responsável	1																				
		Preparar questionários por departamento	2																				
		Envio e preparação (briefings e coaching)	1																				
		Sessões de seguimento	1																				
3	Mapa dos Dados	Desenhar fluxos de dados	5																				
		Preparar o relatório de Auditoria aos Dados	2																				
		Preparar o Registo dos Riscos	2																				
4	Segurança	Tabela Segurança dos Dados	5																				
		Avaliação dos riscos (Sistemas, Terceiros, Trabalhadores, Políticas e Procedimentos)	5																				
		Ciber segurança	3																				
		Plano de Resposta à Violação dos Dados	2																				
5	Avisos de Privacidade	Plano de Avisos de Privacidade - AP	3																				
		AP Clientes	1																				
		AP Trabalhadores	1																				
6	Procedimentos internos	Política Protecção de Dados	1																				
		Política Retenção de Dados	1																				
		Política de tratamento de incidentes de violação de dados	1																				
		Recursos humanos e política de protecção de dados	1																				
		Marketing e política de Protecção de Dados	1																				
		Comunicação Social e política de Protecção de Dados	1																				
7	Formação	Definição da Matriz	1																				
		Sessões presenciais	5																				
8	Avaliação impacto	Avaliação de impacto de privacidade	1																				
9	Notificação	Equipa de resposta rápida	1																				
		Plano de resposta à violação de dados	1																				
		Impressos de notficação de violação de dados	2																				
10	Entidades externas	Identificação de terceiros	1																				
		Análise e avaliação	2																				

12. Questionário de auditoria à protecção de dados

Nome:	
Empresa:	
Departamento:	
Função:	

De forma a implementar o Regulamento Geral de Proteção de Dados na empresa é fundamental começar por identificar que dados são guardados e como são utilizados. Este questionário enquadra-se na Fase de Auditoria à Proteção de Dados e o seu preenchimento é a base fundamental para inventariar de forma exaustiva a informação processada na organização.

Procure ser o mais exuastivo e detalhado possível em todas as respostas.

A informação registada neste documento é sensível e deverá ser guardada de forma segura e com acesso restrito.

1. Guarda informação pessoal de que tipos de pessoas (exemplo: clientes, empregados, fornecedores, parceiros, etc.)?

2. Indique que tipo de informação pessoal guarda sobre clientes (exemplo: nome, morada, contato, ocupação, dados médicos, actividades, profissão)

3. Indique que tipo de informação pessoal guarda sobre empregados e/ou outras pessoas

4. Que dados são mantidos em sistemas informáticos?

5. Os dados arquivados em sistemas informáticos estão no seu computador ou num servidor central?

6. Que tipo de mecanismos de segurança existem relativamente aos dados que guarda em sistemas informáticos?

7. Quem tem acesso à informação existente no seu computador?

8. Existe algum registo de quem acede aos dados mantidos no seu computador ou em computadores existentes nas instalações da empresa?

9. As informações existentes nos computadores da empresa alguma vez foram perdidas ou acedidas por pessoas que não deveriam ter tido acesso? Seja o mais detalhado possível.

10. Existe informação mantida em papel? Descreva o tipo de informação com detalhe

11. Onde é guardada a informação em papel?

12. Destrói documentos antigos em papel? Descreva o processo.

13. Por favor descreva em que circunstâncias recolhe dados diretamente de clientes (exemplo: através do preenchimento de formulários online, quando o cliente contata por telefone)

14. Por favor descreva em que circunstâncias recolhe dados de clientes através de terceiros

15. Os clientes recebem alguma informação da empresa sobre como a sua informação será utilizada?

16. O que faz com a informação dos clientes? Descreva cada processo com detalhe

17. Envia informação de marketing ou promoções a clientes? Descreva com exemplos. O cliente pode optar por deixar de receber essa comunicação?

18. É solicitada autorização aos clientes para que lhe sejam enviadas ofertas e promoções?

19. Existe informação enviada para fora da Europa? Se sim, para que países.

20. Por favor descreva como e quando os dados são apagados

21. Tem conhecimento de circunstâncias em que os dados são partilhados com outras empresas?

22. O cliente pode aceder a toda a sua informação se solicitar?

23. Algum cliente apresentou alguma reclamação pela forma como os seus dados estavam a ser utilizados? Essas reclamações são registadas? Qual o procedimento de resposta?

24. Tem conhecimento de normas ou procedimentos na empresa sobre como pode utilizar dados pessoais de terceiros?

25. Recebeu alguma formação sobre como utilizar dados pessoais? Dentro ou fora de empresa.

26. Descreva os aspectos de segurança do edifício/escritório da empresa

27. Indique os aspectos de segurança relacionados com a utilização dos dados que considere estar a precisar de atenção mais urgente

28. Como são atualizados os dados dos clientes? É mantido um histórico de alterações? A data e o autor da alteração ficam registados?

29. Os websites da empresa utilizam cookies? Por favor detalhe informação.