GUIA PRÁTICO

Regulamento Geral de Protecção de Dados

março 2018

E3S
ASSOCIAÇÃO APOIO À EXCELÊNCIA NO 3º SETOR

Este documento tem por objectivo enunciar um conjunto de medidas a adoptar para obter a conformidade com o RGPD e apresentar um roteiro de actividades que permita a sua aplicação.

E3S

ASSOCIAÇÃO APOIO À EXCELÊNCIA NO 3º SETOR

Regulamento UE 2016/679

Regulamento Geral de Protecção de Dados

E3S

ASSOCIAÇÃO APOIO À EXCELÊNCIA NO 3º SETOR

10 MEDIDAS PARA PREPARAR A APLICAÇÃO DO RGPD

10 medidas para preparar a aplicação do RGPD

O Regulamento Geral de Proteção de Dados (RGPD) entra em vigor a 25 de maio de 2018, e substitui a atual lei de proteção de dados pessoais

Neste documento, identificam-se dez áreas principais de atuação para preparar a conformidade com o novo regulamento

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

1. Informação aos titulares dos dados

O regulamento obriga a prestar mais informações do que atualmente, designadamente a base legal para o tratamento de dados, o prazo de conservação dos dados e a possibilidade de apresentar queixa junto da CNPD.

Dentro das exigências de maior transparência, deve ter-se em atenção que as informações devem ser prestadas aos cidadãos de forma concisa, inteligível e de fácil acesso, utilizando uma linguagem clara e simples.

Assim, terão de se reformular impressos, políticas de privacidade e todos os textos que prestem informação aos titulares dos dados.

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

2. Exercício dos direitos dos titulares dos dados

Deverão ser revistos os procedimentos internos de garantia do exercício dos direitos dos titulares dos dados, em especial no que respeita aos prazos máximos de resposta.

Os direitos dos titulares foram alargados em relação à atual lei, passando a existir o direito à **limitação do tratamento**, o direito à **portabilidade**, o direito à **eliminação dos dados** e quanto à notificação de terceiros sobre retificação, apagamento ou limitação de tratamento solicitados pelos titulares.

A organização deve estar preparada para aplicar as novas obrigações, nomeadamente através da **manutenção da informação num formato estruturado, de uso corrente e de leitura automática**, quando aplicável, e de **procedimentos eficazes de comunicação** com as entidades terceiras a quem transmitiu os dados.

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

2. Exercício dos direitos dos titulares dos dados

Tratamento dos dados

Tem de existir fundamento jurídico para o tratamento de dados:

- **Consentimento do titular dos dados**
- **Necessidade de executar um contrato**

É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. (…)

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

2. Exercício dos direitos dos titulares dos dados

Portabilidade

O artigo 20.º do RGPD estabelece um novo direito à portabilidade dos dados, o qual está intimamente ligado ao direito de acesso.

Este direito permite aos titulares dos dados receber os dados pessoais que tenham fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e transmitir esses dados a outro responsável pelo tratamento.

Este direito abrange os **dados fornecidos de forma ativa e consciente** pelo titular dos dados, bem como os **dados pessoais gerados pela sua atividade**.

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

2. Exercício dos direitos dos titulares dos dados

Portabilidade (cont.)

Uma vez que possibilita a transmissão direta de dados pessoais entre dois responsáveis pelo tratamento, o direito à portabilidade facilitará a mudança para diferentes prestadores de serviços.

Os **dados pessoais derivados ou inferidos** a partir dos dados pessoais fornecidos pelo titular dos dados, por exemplo um perfil de utilizador criado através de uma análise de dados, **são excluídos do âmbito** de aplicação do direito à portabilidade dos dados, uma vez que não são fornecidos pelo titular dos dados, mas sim criados pelo responsável pelo tratamento.

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

2. Exercício dos direitos dos titulares dos dados

Portabilidade (cont.)

Prazo de resposta a um pedido de portabilidade.
O responsável pelo tratamento fornece «ao titular as informações sobre as medidas tomadas [...], sem demora injustificada e no prazo de um mês a contar da data de receção do pedido». Este prazo de um mês pode ser alargado até três meses no máximo para os casos complexos.

Possibilidade de indeferir um pedido de portabilidade ou exigir o pagamento de uma taxa?
O artigo 12.º proíbe a exigência de pagamento de uma taxa pelo fornecimento dos dados pessoais, salvo se o responsável pelo tratamento puder demonstrar que os pedidos são manifestamente infundados ou excessivos, «nomeadamente devido ao seu caráter repetitivo»

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

3. Consentimento dos titulares dos dados

Tem de se verificar a forma e circunstâncias em que foi obtido o consentimento dos titulares, quando este serve de base legal para o tratamento de dados pessoais, sendo necessário apurar se o consentimento obtido pelo responsável pelo tratamento respeita todas as novas exigências.

Se assim não for, é imprescindível obter novo consentimento dos titulares dos dados em conformidade com as disposições do RGPD.

Particular atenção deve ser dada ao consentimento dos menores ou dos seus representantes legais, considerando as exigências específicas do regulamento para este efeito.

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

4. Dados sensíveis

Avaliar a natureza dos tratamentos de dados efetuados, a fim de apurar quais os que se podem enquadrar no conceito de dados sensíveis, e consequentemente aplicarem-se condições específicas para o seu tratamento.

O regulamento veio estender o leque das categorias especiais de dados, integrando por exemplo os dados biométricos, que passaram a fazer parte do elenco de dados sensíveis.

Deve também analisar-se o contexto e a escala destes tratamentos de dados, para verificar se daí decorrem obrigações particulares, tais como a designação de um **encarregado de proteção de dados**.

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

5. Documentação e registo de actividades de tratamento

Todas as atividades relacionadas com o tratamento de dados pessoais devem estar documentadas de forma detalhada, não apenas as que resultam diretamente da obrigação de manter um registo, mas também as relativas a outros procedimentos internos, de modo a que a organização esteja apta a demonstrar o cumprimento de todas as obrigações decorrentes do RGPD.

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

6. Contratos de subcontratação

Rever os contratos de subcontratação de serviços realizados no âmbito de tratamentos de dados pessoais, para verificar se contêm todos os elementos exigidos pelo regulamento.

O RGPD veio especificar o conteúdo dos contratos de subcontratação, impondo a introdução de um vasto conjunto de informações. É muito provável que os contratos existentes necessitem de ser modificados para respeitar os termos do regulamento.

Quando houver lugar a sub-subcontratação, compete ao subcontratante verificar se detém as autorizações respetivas dos responsáveis pelo tratamento, exigidas expressamente pelo novo regulamento.

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

7. Encarregado de protecção de dados

Designar o encarregado de proteção de dados que desempenha um papel fulcral para garantir que a organização cumpre todas as obrigações legais.

Deve ser dada especial atenção à posição do encarregado de proteção de dados dentro da organização e ao reporte direto ao mais alto nível, bem como às funções que lhe são atribuídas pelo RGPD.

Mesmo que a organização não se encontre de momento em nenhuma das circunstâncias exigíveis, decidir ter um encarregado de proteção de dados tem evidentes vantagens para o cumprimento das obrigações.

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

8. Medidas técnicas e organizativas e segurança no tratamento

Rever as políticas e práticas da organização à luz das novas obrigações do regulamento, e adotar as medidas técnicas e organizativas adequadas e necessárias para assegurar e poder comprovar que todos os tratamentos de dados efetuados estão em conformidade com o RGPD.

Nessa avaliação, deve ter em conta a natureza, âmbito, contexto e finalidades dos tratamentos de dados, bem como os riscos que deles podem decorrer para os direitos e liberdades dos cidadãos.

Esta apreciação permite ainda tomar as medidas necessárias para confirmar um nível de segurança do tratamento adequado, que garanta designadamente a confidencialidade e a integridade dos dados e que previna a destruição, perda e alterações acidentais ou ilícitas ou, ainda, a divulgação ou acesso não autorizados de dados.

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

9. Protecção de dados desde a concepção e avaliação do impacto

Avaliar rigorosamente o tipo de tratamentos de dados que tenha projetado realizar num futuro próximo, de modo a analisar a sua natureza e contexto e os potenciais riscos que possam comportar para os titulares dos dados, de modo a aplicar com eficácia os princípios da proteção de dados desde a conceção e por defeito.

A fim de decidir sobre as medidas mais ajustadas, seja tendentes à pseudonimização, à minimização dos dados, ao cumprimento dos prazos de conservação da informação ou à acessibilidade dos dados, deve ter em devida conta as características do tratamento e os efeitos que este pode ter nos direitos dos cidadãos; se for suscetível de resultar num elevado risco, deve realizar uma avaliação de impacto sobre a proteção de dados, de modo a adotar as medidas adequadas para mitigar os riscos.

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

9. Protecção de dados desde a concepção e avaliação do impacto

Nota:

Pseudonimização - Tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

Fonte: Comissão Nacional de Protecção de Dados

10 medidas para preparar a aplicação do RGPD

10. Notificação de violações de segurança

Adotar procedimentos internos para lidar com casos de violações de dados pessoais, designadamente na deteção, identificação e investigação das circunstâncias, medidas mitigadoras, circuitos da informação, envolvimento do encarregado de proteção de dados e notificação à CNPD, atendendo aos prazos prescritos no regulamento.

Apenas devem ser reportadas à autoridade de controlo, as violações que sejam suscetíveis de resultar num risco para os direitos dos titulares. Todavia, todas as violações devem ser devidamente documentadas.

Nos casos, em que possa resultar um elevado risco para os titulares, é exigido que estes sejam notificados, pelo que deve ser analisado desde logo o tipo de tratamentos de dados realizados e o potencial risco que pode ocorrer em caso de uma violação de segurança.

Fonte: Comissão Nacional de Protecção de Dados

E3S

ASSOCIAÇÃO APOIO À EXCELÊNCIA NO 3º SETOR

ROTEIRO PARA A APLICAÇÃO DO RGPD

Roteiro para a aplicação do RGPD

Roteiro para a aplicação do RGPD

ENCARREGADO DA PROTECÇÃO DE DADOS

Art. 37º - A Organização tem obrigatoriamente que 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

Notas: Um EPD pode ter outras funções dentro da Organização

Roteiro para a aplicação do RGPD

ENCARREGADO DA PROTECÇÃO DE DADOS

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

Notas: O EPD tem que operar de forma independente e reportar diretamente à Direcção

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

Roteiro para a aplicação do RGPD

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

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

Roteiro para a aplicação do RGPD

AUDITORIA AOS DADOS

Principais Acções:

- 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

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

Roteiro para a aplicação do RGPD

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 adopter para minimizar a probabilidade.

Roteiro para a aplicação do RGPD

MAPA DOS DADOS

Principais acções:

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

Roteiro para a aplicação do RGPD

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.

Roteiro para a aplicação do RGPD

SEGURANÇA

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)

Notas: Depois de identificados os Riscos, os mesmos serão priorizados por nível de criticidade

Roteiro para a aplicação do RGPD

SEGURANÇA

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)

Roteiro para a aplicação do RGPD

AVISOS DE PRIVACIDADE

Os Avisos de Privacidade são a informação prestada aos donos dos dados, sobre a forma e 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.

Roteiro para a aplicação do RGPD

AVISOS DE PRIVACIDADE

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**»);

Roteiro para a aplicação do RGPD

AVISOS DE PRIVACIDADE

O que diz o RGPD sobre as Políticas de Privacidade

De acordo com o Artigo 5º do RGDP, os dados pessoais deverão ser (cont.):

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**»).

Roteiro para a aplicação do RGPD

AVISOS DE PRIVACIDADE

Política de Privacidade

A Politica 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

Roteiro para a aplicação do RGPD

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.

Roteiro para a aplicação do RGPD

PROCEDIMENTOS INTERNOS

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.

Roteiro para a aplicação do RGPD

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.

Roteiro para a aplicação do RGPD

AVALIAÇÃO 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 conformidade.**

Roteiro para a aplicação do RGPD

AVALIAÇÃO IMPACTO

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

Roteiro para a aplicação do RGPD

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.

Roteiro para a aplicação do RGPD

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).

Roteiro para a aplicação do RGPD

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

Exemplo:

Fases		Actividades	Dias	Semana 1					Semana 2				
				1	2	3	4	5	6	7	8	9	10
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										

Roteiro para a aplicação do RGPD

Exemplo:

Fases		Actividades	Dias	Semana 1					Semana 2				
				1	2	3	4	5	6	7	8	9	10
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										
		Total	**55**										

E3S

ASSOCIAÇÃO APOIO À EXCELÊNCIA NO 3º SETOR

ANEXO

QUESTIONÁRIO DE AUDITORIA À PROTEÇÃO DE DADOS (Exemplo)

Nome:	
Departamento:	
Função:	

De forma a implementar o Regulamento Geral de Proteção de Dados na Organização 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.

QUESTIONÁRIO DE AUDITORIA À PROTEÇÃO DE DADOS (Exemplo)

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 Organização?

QUESTIONÁRIO DE AUDITORIA À PROTEÇÃO DE DADOS (Exemplo)

9. A informação existente nos computadores da Organização 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 Organização sobre como a sua informação será utilizada?

QUESTIONÁRIO DE AUDITORIA À PROTEÇÃO DE DADOS (Exemplo)

16. O que faz com a informação dos clientes? Descreva cada processo com detalhe.
17. Envia informação a clientes? Descreva com exemplos. O cliente pode optar por deixar de receber essa comunicação?
18. É solicitada autorização aos clientes para que lhe seja enviada informação?
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 Organizações?
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?

QUESTIONÁRIO DE AUDITORIA À PROTEÇÃO DE DADOS (Exemplo)

24. Tem conhecimento de normas ou procedimentos na Organização sobre como pode utilizar dados pessoais de terceiros?
25. Recebeu alguma formação sobre como utilizar dados pessoais? Dentro ou fora da Organização.
26. Descreva os aspectos de segurança do edifício/escritório da Organização
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?