PROCEDIMENTO

PROTEÇÃO DE DADOS PESSOAIS

PDP.003 (1)

Resposta à Violação de Dados Pessoais (Data Breach)

Verificado por:	***Aprovado por:***
Margarida Novais *Direção Jurídica* *Data:*	*José António Reis Costa* *Administração* *Data:*

Índice

Nº. Alteração	Data	Descrição Sumária das Alterações
00	02 Abr. 2018	Emissão Inicial
01	14-05-2018	Alteração de contactos na página 4

1. OBJETIVO

O presente documento visa servir de orientação aos colaboradores do Grupo ProCME e a terceiros envolvidos numa eventual violação de dados pessoais, permitindo que estes respondam adequadamente a essa violação.

2. ÂMBITO

O presente documento abrange todo o tipo de violações de dados pessoais (incidentes que afetem dados de colaboradores, clientes, prestadores de serviços do Grupo ProCME etc.) e é aplicável a todo o tipo de violações de dados que afetem o Grupo ProCME, independentemente do local do incidente: tanto dentro da rede da empresa como de terceiros, clientes ou prestadores de serviços.

3. DEFINIÇÕES

Não Aplicável.

4. PROCEDIMENTO E RESPONSABILIDADES

O Regulamento Geral sobre a Proteção de Dados ("RGPD") prevê que em caso de violação de dados pessoais, o responsável pelo tratamento deva notificar desse facto a **autoridade de controlo** – em Portugal, a Comissão Nacional de Proteção de Dados ("CNPD") - bem como, em determinadas situações, comunicar essa violação aos **titulares de dados**.[1]

O incumprimento destas obrigações pode resultar na aplicação de uma coima até 10 milhões de Euros ou até 2% do volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.[2]

O conceito de **"violação de dados pessoais"** reporta-se a uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.[3] Os incidentes podem ser categorizados de acordo com os seguintes três princípios de segurança da informação:

(i) Violação da segurança;
(ii) Violação da disponibilidade;
(iii) Violação da integridade.

O documento "Guidelines on Personal data breach notification under Regulation 2016/679", adotado pelo Grupo de Trabalho do Artigo 29 em 3 de outubro de 2017 deve ser considerado na interpretação e aplicação deste Procedimento.[4]

4.1 Instruções

Caso tenha conhecimento de que ocorreu ou poderá ter ocorrido uma violação de dados pessoais, é crucial que a resposta seja rápida.

[1] Artigos 33.º e 34.º do RGPD
[2] Artigo 83 n.º 4 alínea a) do RGPD
[3] Artigo 4.º, 12) do RGPD
[4] Disponível em http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Passo	Ação recomendada	Comentários
1	**Contactar os departamentos / pessoas relevantes** Esteja preparado para contactar as pessoas chave rapidamente, por exemplo via telefone ou e-mail. Deverá contactar de imediato os seguintes departamentos: ▪ Departamento Jurídico ▪ Encarregado da Proteção de Dados – proteção.dados@grupo-procme.com	A ProCME deve organizar uma lista de contactos especial para as situações de violação de dados pessoais. Esta lista deve estar sempre atualizada, deve ser divulgada e estar disponível *on-site* (nos computadores da empresa) e *off-site* (em formato pdf e nos contactos dos telemóveis e outros *devices* móveis da empresa).
2	**Iniciar a investigação da eventual violação de dados pessoais e tomar as primeiras medidas de contenção**	
3	**Identificar as obrigações legais** O Departamento Jurídico, em conjunto com Encarregado da Proteção de Dados – proteção.dados@grupo-procme.com e eventualmente com o auxílio de consultores externos identifica as obrigações legais relevantes, em função dos factos apurados.	Devem ser avaliados os riscos para as pessoas singulares (sem risco, com risco ou com elevado risco) e devem ser informadas as funções / pessoas relevantes da empresa. O Anexo II contém uma listagem não exaustiva de violações de dados pessoais que devem ser notificadas à CNPD. Estes cenários visam auxiliar a ProCME a decidir se deve notificar a CNPD, bem como a identificar diferentes níveis de risco para os direitos e liberdades das pessoas singulares.
4	**Notificar o responsável pelo tratamento (se aplicável)** Nas situações em que a ProCME esteja a agir na qualidade de subcontratante, deve notificar o responsável pelo tratamento sem demora injustificada após ter conhecimento da violação de dados pessoais.[5]	O RGPD prevê que esta notificação deva ser feita sem demora injustificada. Os responsáveis pelo tratamento podem definir contratualmente prazos concretos a cumprir pela ProCME.
5	**Notificar a CNPD (se aplicável)** A notificação deve ser efetuada sem demora injustificada e, sempre que possível, **até 72 horas após ter tido conhecimento da violação de dados pessoais.**[6] A notificação deve, pelo menos: a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa; b) Comunicar o nome e os contactos do encarregado da proteção de dados ou outro ponto de contacto onde possam ser obtidas mais informações; c) Descrever as consequências prováveis da violação de dados pessoais;	A ProCME não está obrigada a notificar a CNPD caso a violação de dados pessoais são seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas à CNPD por fases, sem demora injustificada.[7] Se a ProCME não tiver já comunicado a violação de dados pessoais ao titular dos dados (nos casos em que esta comunicação é obrigatória), a CNPD pode exigir à ProCME que proceda a essa notificação ou dispensá-la, nos casos previstos no artigo 35.º n.º 3.

[5] Artigo 35 n.º 2 do RGPD
[6] Artigo 33 n.º 1 do RGPD
[7] Artigo 33 n.º 4 do RGPD

	d) Descrever as medidas adotadas ou propostas pela ProCME para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.	
6	**Notificar os titulares de dados (se aplicável)** Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares[8], o responsável pelo tratamento comunica também a violação de dados pessoais ao **titular dos dados**, sem demora injustificada. Esta comunicação deve descrever em linguagem clara e simples a natureza da violação dos dados pessoais e fornecer, pelo menos, as seguintes informações e medidas: a) Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações; b) Descrever as consequências prováveis da violação de dados pessoais; c) Descrever as medidas adotadas ou propostas pela ProCME para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.	Uma das finalidades da comunicação aos titulares é limitar os danos que estes possam sofrer. A comunicação não é exigida se for preenchida uma das seguintes condições: a) A ProCME tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem; b) A ProCME tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares já não é suscetível de se concretizar; c) Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.
7	**Documentar a violação de dados pessoais** Este registo deve conter os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada.	Esta documentação deve permitir à CNPD verificar o cumprimento do disposto no art. 33.º do RGPD.
8	**Melhorar os processos internos**	

5. IMPRESSOS

Não Aplicável

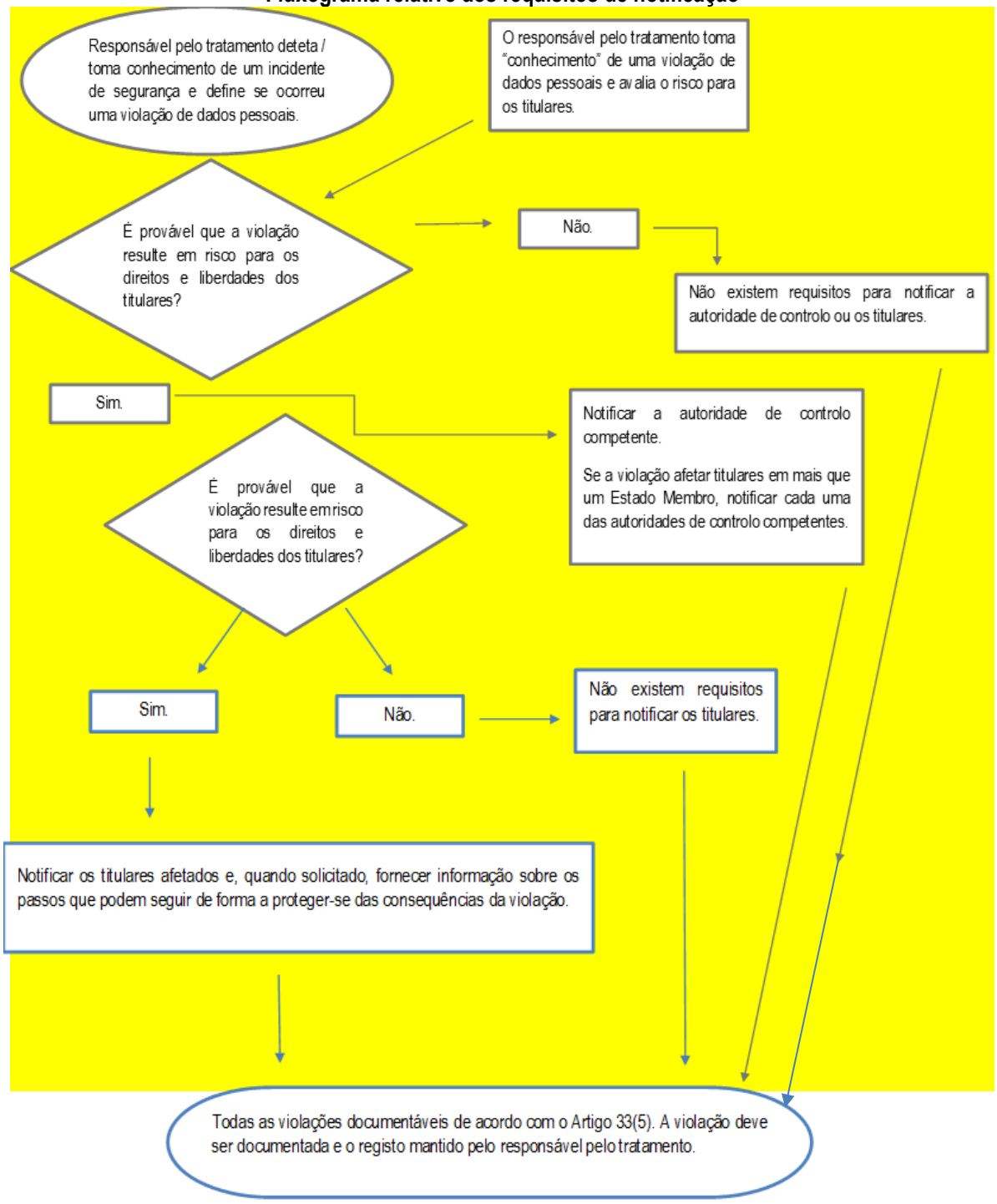
6 ANEXOS

Anexo I – Fluxograma relativo aos requisitos de notificação

Anexo II – Exemplos de violações de dados pessoais

[8] Na interpretação do conceito de "elevado risco" devem ser consideradas as considerações contidas no Capítulo IV (Assessing risk and high risk) das "Guidelines on Personal data breach notification under Regulation 2016/679" adotadas pelo Grupo de Trabalho do Artigo 29

Anexo I
Fluxograma relativo aos requisitos de notificação



Anexo II
Exemplos de violações de dados pessoais

A lista não exaustiva de exemplos que se segue serve para auxiliar os responsáveis pelo tratamento de dados pessoais a determinar se necessitam de notificar uma violação de dados pessoais em diferentes cenários. Estes exemplos podem também ajudar a distinguir entre situações de risco e de alto risco para os direitos e liberdades dos titulares. Estes exemplos são retirados das Guidelines on Personal data breach notification under Regulation 2016/679, adotadas pelo Grupo de Trabalho do Artigo 29.

Exemplo	Notificar a autoridade de controlo?	Notificar o titular dos dados?	Notas / recomendações
i. Um responsável pelo tratamento armazenou um *backup* de um arquivo de dados pessoais encriptado num CD. O CD é roubado durante um arrombamento.	Não.	Não.	Desde que os dados estejam encriptados com um algoritmo de topo, que existam *backups* dos dados e que a única chave não seja comprometida, esta violação poderá não resultar numa notificação. No entanto, se mais tarde a chave for comprometida, é necessário efetuar a notificação.
ii. Dados pessoais de indivíduos são extraídos de um *website* seguro gerido pelo responsável pelo tratamento durante um ataque informático. Os clientes do responsável pelo tratamento estão num único Estado Membro.	Sim, notificar a autoridade de controlo competente se existem potenciais consequências para os titulares.	Sim, notificar os titulares dos dados consoante a natureza dos dados pessoais afetados e se as potenciais consequências para os titulares forem de alta gravidade.	Se o risco não for alto, recomendamos que o responsável pelos dados notifique o titular dos dados, consoante as circunstâncias do caso. Por exemplo, pode não ser necessário notificar se existe uma violação de confidencialidade num boletim informativo relacionado com um programa de televisão, mas pode ser necessário se este boletim informativo levar à divulgação de um ponto de vista político do titular dos dados.
iii. Um breve corte de energia que dure vários minutos numa central de atendimento do responsável pelo tratamento, que leva a que os clientes não consigam telefonar para o responsável pelo	Não.	Não.	Tal não constitui uma violação de dados merecedora de notificação, mas sim um incidente que deve ser documentado ao abrigo do artigo 33(5). O responsável pelo tratamento deve manter um registo adequado.

Exemplo	Notificar a autoridade de controlo?	Notificar o titular dos dados?	Notas / recomendações
tratamento e aceder aos seus registos.			
iv. Um responsável pelo tratamento sofre um ataque de *ransomware* que resulta em todos os dados serem encriptados. Não existem *backups* e os dados não conseguem ser restaurados. Após investigação, torna-se claro que a única finalidade do ransomware era encriptar os dados, e que não havia qualquer outro *malware* presente no sistema.	Sim, notificar a autoridade de controlo competente se existem potenciais consequências para os titulares, tal como esta perda de disponibilidade dos dados.	Sim, notificar os titulares dos dados consoante a natureza dos dados pessoais afetados e dos possíveis efeitos da perda de disponibilidade dos dados, assim como outras possíveis consequências.	Se existisse um *backup* e os dados pudessem ser restaurados em tempo útil, não havia necessidade de notificar a autoridade de controlo e os titulares dos dados já que não existiria perda permanente da disponibilidade dos dados ou violação de confidencialidade. No entanto, a autoridade de controlo poderá considerar efetuar uma investigação de forma a avaliar o cumprimento com os requerimentos gerais de segurança do Artigo 32.
v. Um titular telefone para o centro de atendimento de um banco para reportar uma violação de dados. O titular recebeu uma declaração pertencente a outrem. O responsável pelo tratamento faz uma curta investigação (i.e., completada em menos de 24h) e conclui, com razoável certeza, que ocorreu uma violação de dados pessoais e se foi uma falha sistemática que leve a que outros titulares tenham sido ou sejam afetados.	Sim.	Apenas os titulares afetados devem ser notificados se houver um risco alto e for claro que os outros não foram afetados.	Se, após investigação mais extensa, for concluído que mais titulares foram afetados, a autoridade de controlo deverá ser informada e o responsável pelo tratamento deverá tomar medidas adicionais a fim de notificar outros titulares se o risco for alto para eles.
vi. Uma empresa de *hosting* de *websites* (subcontratante) identifica um erro no código que controla a autorização do utilizador. O efeito da falha leva a que qualquer utilizador possa aceder aos detalhes da conta de qualquer outro utilizador.	Como subcontratante, a empresa deve notificar os seus clientes afetados (os responsáveis pelo tratamento) sem qualquer demora. Assumindo que a empresa conduziu uma investigação própria, os responsáveis pelo tratamento afetados devem confiar razoavelmente que	Se não existe um risco alto para os titulares, estes não precisam de ser notificados.	A empresa de *hosting* de *websites* (subcontratante) deve ter em conta quaisquer outras obrigações de notificação (por exemplo, no âmbito da Diretiva relativa à segurança das redes e da informação). Se não houver indicação de que esta vulnerabilidade é explorada no que toca a

Exemplo	Notificar a autoridade de controlo?	Notificar o titular dos dados?	Notas / recomendações
	sofreram uma violação e é provável que considerem ter "tomado conhecimento" uma vez notificados pela empresa (o subcontratante). O responsável pelo tratamento deve então notificar a autoridade de controlo.		este responsável pelo tratamento em particular, poderá não ter ocorrido uma violação merecedora de notificação, mas sim que deve ser documentada ou uma questão de não cumprimento ao abrigo do Artigo 32.
viii. Os registos médicos de um hospital estão indisponíveis durante 30 horas devido a um ataque informático.	Sim, o hospital é obrigado a notificar já que existir um alto risco para o bem-estar e privacidade dos pacientes.	Sim, notificar os titulares afetados.	
ix. Os dados pessoais de 5000 alunos são enviados, por erro, para uma lista de destinatários errada, com mais de 1000 destinatários.	Sim, notificar a autoridade de controlo.	Sim, notificar os titulares consoante o âmbito e tipo de dados pessoais envolvidos e a gravidade das potenciais consequências.	
x. Um e-mail de *marketing* direto é enviado para destinatários nos campos de "para:" ou "cc:", permitindo assim que cada destinatário veja os endereços de *e-mail* de outros destinatários.	Sim, notificar a autoridade de controlo poderá ser obrigatório se um grande número de titulares for afetado, se foram revelados dados sensíveis (por exemplo, a lista de destinatários de um psicoterapeuta) o se outros fatores apresentarem um alto risco (por exemplo, se o *e-mail* contiver as *passwords* iniciais).	Sim, notificar os titulares consoante o âmbito e tipo de dados pessoais envolvidos e a gravidade das potenciais consequências.	As notificações podem não ser necessários se não foram revelados dados sensíveis e se apenas um pequeno número de endereços de *e-mail* for revelado.