Política de Gestão de Incidentes de Violação de Dados Pessoais

matosinhos

Índice

1. Nota justificativa

A Política de Gestão de Incidentes tem como objetivo oferecer orientações e mecanismos de resposta em caso de incidente com dados pessoais, designadamente, a destruição, perda e alteração ilícita ou acidental, a divulgação ou acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer tipo de tratamento na Câmara Municipal de Matosinhos.

A gestão de um incidente de violação de dados exige, a maioria das vezes, a intervenção de diversos serviços, que se pretende rápida e eficaz.

Para isso, deverá ser criada uma equipa de resposta ao incidente, que terá como objetivo, fazer de cada departamento uma mais-valia em todo o processo de gestão de incidentes, pelo uso do conhecimento técnico especializado de cada um.

2. Âmbito

A presente Política de Gestão de Incidentes de Dados Pessoais é aplicável a todos os trabalhadores da Câmara Municipal de Matosinhos que de qualquer forma tenham acesso a dados pessoais.

3. Definições

3.1 Incidente: qualquer evento adverso que determine uma violação da segurança, que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

3.2 Equipa de resposta ao incidente: equipa responsável pela adoção de medidas de identificação e ações envolvendo qualquer incidente ocorrido com dados pessoais, composta necessariamente por membros das diferentes unidades orgânicas da Câmara Municipal de Matosinhos e pelo Encarregado de Proteção de Dados.

Poderão integrar esta equipa:

-Gabinete de Proteção de Dados/Encarregado de Proteção de Dados

-Departamento de Informática e de Sistemas (DSI)

-Departamento de Recursos Humanos (RH)

- Gabinete de Comunicação e Relações Públicas
- Departamento Jurídico
- Unidade Orgânica atingida
- Arquivo (violação de dados sobre papel)
- Gabinete de Auditoria, Controlo e Excelência
- Executivo Municipal
- Recursos Externos

Responsabilidades:

- Determinar o impacto do acidente
- Identificar os acontecimentos relevantes do incidente ou outras ameaças potenciais decorrentes desse evento ou incidente
- Identificar a causa do incidente
- Coordenar a implementação de estratégias de resposta
- Divulgar informações sobre riscos e estratégias de resposta
- Manter uma base de dados com registo de incidentes e estudar possíveis melhorias de segurança de dados pessoais.

4. Instrumentos de deteção de incidentes de dados pessoais

A Câmara Municipal de Matosinhos deve recorrer a instrumentos de deteção e medidas preventivas de incidentes, designadamente:

Sistema de Segurança da Informação

- Software de blindagem de host e rede
- Software antivírus
- Vigilância de base de dados e de entidades terceiras
- Instrumentos de prevenção de perda de dados

Segurança Interna

- Sistema de correio eletrónico privado
- Sistema de Segurança de dois passos (utilizador/password)

5. Critérios de classificação de impacto de incidentes

Os incidentes de dados pessoais são classificados como de Alto Risco ou Baixo Risco consoante o impacto do risco para os direitos e liberdades das pessoas singulares, designadamente a produção de danos na reputação, na atividade profissional, na família.

6. Procedimento de análise e resposta a incidentes

6.1 Deteção do incidente – logo que detetado, o incidente deverá ser reportado ao encarregado de proteção de dados, com todas as informações recolhidas no serviço onde ocorreu – a natureza do incidente, os titulares afetados, os dados pessoais comprometidos, quem, quando e o que causou o incidente.

6.2 Análise interna do incidente – pelo encarregado de proteção de dados e pela equipa de resposta, se necessário (análise de risco e danos causados)

-Após a deteção da ocorrência do incidente, deverá ser feita a análise relativa à gravidade do incidente e possível resolução dos danos causados.

- Devem ser recolhidas as seguintes informações:
- natureza do incidente (ataque digital, perda de hardware ou desobediência do funcionário, por exemplo);
- número de titulares afetados;
- entidades terceiras envolvidas;
- entidades alheias à Câmara Municipal de Matosinhos que têm conhecimento do incidente;
- informações divulgadas, incluindo categorias de dados ou nomes individuais, se determinável;
- potenciais consequências do incidente;
- medidas tomadas ou a tomar para reverter ou mitigar o impacto do incidente;
- notificações a realizar, por obrigação legal;
- quem teve acesso ou recebeu informações;

Na análise do incidente devem ainda ser considerados alguns fatores, designadamente:

- O risco do impacto do incidente sobre os titulares;
- As circunstâncias do incidente;
- A gravidade do impacto potencial do incidente;

- A natureza, sensibilidade e quantidade de dados pessoais;
- A facilidade de identificação dos titulares relativamente aos dados comprometidos;
- As características especiais dos titulares, como por exemplo, incidentes que afetem crianças ou outros indivíduos vulneráveis;

Caso, e na medida em que, não seja possível comunicar todas estas informações ao mesmo tempo, a notificação inicial deve conter as informações então disponíveis, devendo outras informações, à medida que fiquem disponíveis, ser fornecidas posteriormente sem demora injustificada

Os titulares dos dados devem ser imediatamente notificados se o risco do incidente corresponder a um risco elevado para os seus direitos e liberdades.

O incidente deverá ser tratado como um assunto confidencial.

Para apurar da probabilidade do risco ou dano relevante para os titulares, deverá ser considerado, em acréscimo à regulação aplicável, que a probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver designadamente, dados sensíveis (dados relativos a raça, origem étnica, opinião política, religião ou crenças filosóficas, associação, sindicatos, dados genéticos, dados relativos à saúde, ou dados criminais, representa com alto grau de probabilidade, um risco elevado aos direitos individuais), ou de indivíduos em situação de vulnerabilidade, incluindo crianças, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade.

6.3 Classificação do incidente com base na gravidade e danos apurados, tendo por base as informações prestadas pelas partes interessadas e elementos de prova recolhidos.

6.4 Preenchimento do formulário de incidentes (Anexo I) e registo na base de dados de incidentes (numerado)

6.5 Correção do incidente – informação aos departamentos competentes sobre o incidente e partes interessadas, conforme necessário, para iniciar ações de correção e mitigação de danos eventualmente causados.

6.6 Notificação externa se preenchidos os requisitos legais (à Comissão Nacional de Proteção de Dados (CNPD) e titular dos dados). A comunicação com qualquer pessoa envolvida e a eventual comunicação à CNPD terá de ser aprovada pelo encarregado de proteção de dados (EPD).

6.7 Declaração de incidente finalizado – concluir o incidente e encerrar o processo de resposta.

6.8 Competências do EPD

- Conduzir a avaliação interna do incidente;
- Registar o incidente;
- Solicitar e reunir toda a informação relativa ao incidente;
- Analisar o risco em conjunto com a equipa;
- Notificar o (s) titular (s) dos dados pessoais, entidades terceiras e outras partes interessadas (conforme se justifique de acordo com o previsto nos artigos 33º e 34º do RGPD);
- Elaborar um Relatório de situação com base na informação prestada pelos departamentos afetados. Se se tratar de incidente de segurança digital, o encarregado de proteção de dados solicita a colaboração do DSI na execução do Relatório de situação.

7. Contenção do incidente

No caso de um incidente de segurança, o DSI deve fazer uso dos meios técnicos ao seu dispor para isolar as partes comprometidas da rede ou desativar os dispositivos envolvidos no incidente.

Se o incidente envolver um colaborador da Câmara Municipal de Matosinhos, o encarregado de proteção de dados deve propor a instauração de um inquérito e determinar as opções para limitar as ações de funcionários que possam representar um potencial risco, designadamente:

- Condicionar o acesso do funcionário a certas instalações;
- Condicionar o acesso as áreas reservadas em plataformas digitais;
- Propor a instauração de processos disciplinares

8. Notificação à autoridade reguladora (Comissão Nacional de Proteção de Dados)

– Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente (CNPD), sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação de dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares (artigo 33º do RGPD).

A notificação deve incluir:

- a natureza da violação de dados, as categorias de dados pessoais e o número aproximado de titulares afetados;
- o nome e detalhes de contacto do EPD para efeito de solicitações adicionais de informação;
- as possíveis consequências do incidente de dados pessoais;
- a descrição das medidas propostas a serem adotadas na gestão do incidente, inclusivamente de medidas apropriadas para mitigar os possíveis efeitos adversos;
- a notificação pode ser enviada em partes, de forma a evitar atrasos resultantes da falta de informações precisas e completas;
- se não puder ser realizada dentro do período de tempo previsto legalmente, deve ser enviada o mais rápido possível e acompanhada de uma justificação do atraso.

9. Notificação ao titular dos dados

- Quando a violação dos dados pessoais seja 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 (artigo 34º do RGPD).

Esta comunicação deverá descrever em linguagem clara e simples:

- a natureza da violação dos dados pessoais e fornecer o nome e contactos do EPD ou de outro ponto de contacto onde possam ser obtidas mais informações;
- as consequências prováveis da violação de dados pessoais;
- as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusiva, se for caso disso, medidas para atenuar os seus efeitos negativos.

Em determinadas circunstâncias, poderá ser importante notificar entidades terceiras (prestadores de serviços, subcontratantes).

10. Correção e registo

Após a análise do incidente e efetuadas as notificações se necessário, deverá iniciar-se a gestão da correção e mitigação dos danos causados, desenvolvendo-se as ações a tomar para correção de eventuais falhas.

O encarregado de proteção de dados regista o incidente e mantém atualizada a base de dados de incidentes de dados pessoais.

11. Entrada em vigor

A presente política entra em vigor no 3.º dia útil subsequente à sua publicitação.

Anexo I

Formulário de incidente de segurança de dados pessoais

1 - Designação e descrição do incidente:

- Hora e data do início da violação/do conhecimento da violação

- Forma como foi identificado

- Tipo de violação:

Integridade

Confidencialidade

Disponibilidade

- Natureza:

Equipamento perdido/roubado

Documento perdido/roubado

Correio perdido ou acedido indevidamente

Hacking

Malware

Phishing

Outra

2 - Nome do titular dos dados/prestador de serviços/subcontratantes/outros

Nome:
Empresa:
CC/NIF:

3 - Categorias e quantidade de titulares de dados pessoais envolvidos

Titulares	**Nº de titulares afetados**	**Nº de registos de dados**
Funcionários		
Fornecedores		
Utilizadores/Munícipes		
Menores		
Outros		

Tipo de dados pessoais envolvidos

1- Nome do titular

2 - Número de identificação

3 - Morada

4 - Contactos

5 - Dados de perfil

6 - Dados de saúde e/ou genéticos

7 - Dados de localização

8 - Dados biométricos

9 - Dados financeiros

10 - Dados de recursos humanos

11 - Dados relativos a convicções filosóficas ou filiação partidária

12 - Dados relativos a orientações sexuais

13 - Imagem

14 - Voz

15 - Outros

4 - Causa do incidente

Ato interno não malicioso/malicioso

Ato externo não malicioso/malicioso

Outra

5 - Descrição das consequências prováveis do incidente de dados pessoais

Data provável da ocorrência	Serviço	Utilizador/Funcionário
Data de comunicação	Serviço	Utilizador/Funcionário

Risco (Baixo/Alto)

Data do fecho do Incidente

Reparação total do dado/mitigação

6 – Medidas propostas pela CMM para reparação e/ou mitigação dos efeitos do incidente de dados pessoais

Data: _____/_____/_____

Assinatura: _____