MUNICÍPIO DE SÃO PEDRO DO SUL

Política de Violação de Dados Pessoais

1 - Sumário

As Violações de Segurança com Dados Pessoais são ocorrências cada vez mais frequentes, causadas por erro humano ou por intenção maliciosa. Se, por um lado, à medida que a quantidade de dados e a informação cresce e a tecnologia se desenvolve surgem novas formas pelas quais os dados podem ser violados, por outra, existe uma maior sensibilidade para as questões de privacidade que culminam num reforço das medidas internas relativas à segurança dos dados.

O Regulamento Geral de Proteção de Dados (RGPD) introduziu a obrigação de todas as organizações, de implementarem medidas, técnicas e organizativas, no domínio da segurança para mitigar a probabilidade da ocorrência de incidentes bem como para diminuir os impactos/gravidade.

Para tal, o Município precisa de dotar-se de uma política robusta e de um processo sistemático para detetar, investigar e responder a qualquer violação de dados pessoais. Necessita também de estabelecer um procedimento de comunicação de modo a garantir uma atuação em conformidade com as exigências legais, facilitar as tomadas de decisão e possibilitar a mitigação ao risco da sua ocorrência e do impacto potencial que o mesmo pode gerar.

Uma violação de dados ocorre quando uma organização sofre um incidente de segurança relativo aos dados pessoais pelos quais é responsável e do qual resulte uma quebra de confidencialidade, da disponibilidade ou da integridade dos mesmos.

As obrigações de Notificação constituem medidas para reforçar a transparência, a responsabilização dos Responsáveis pelo Tratamento de Dados bem como promover o aconselhamento e acompanhamento entre as entidades e a Autoridade de Controlo, potencializando um reforço das medidas de prevenção bem como a emergência de um Plano de Ação.

A definição de um Plano de Ação deverá ser pensada como um instrumento de reforço da conformidade em relação à proteção de dados pessoais.

2 - Princípios Básicos e Definição

- **Dados pessoais:** informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

- **Ficheiro:** qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

- **Incidente de Segurança:** Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.

- **Responsável pelo Tratamento:** a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;

- **Subcontratante:** uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;

- **Tratamento:** uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

- **Violação de dados pessoais:** uma violação da 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 - Violação de Dados Pessoais

3.1 - Definição

Uma violação de dados é uma violação da segurança que provoca, 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.

3.1.2 - Destruição, dano perda e tratamento ilícito

O que se entende por «destruição» de dados pessoais deve ser bem claro: refere-se aos dados que deixam de existir, ou deixam de existir num formato que seja de alguma utilidade para o responsável pelo tratamento. O significado de «dano»: trata-se dos dados pessoais que foram alterados, corrompidos, ou já não estão completos. Em termos de «perda» de dados pessoais, tal deve ser interpretado como os dados ainda poderem existir, mas o responsável pelo tratamento perdeu o controlo ou o acesso a eles, ou já não os tem na sua posse. Por último, o tratamento não autorizado ou ilícito pode incluir a divulgação de dados pessoais a (ou o acesso por) destinatários que não estão autorizados a receber (ou a aceder) os dados, ou qualquer outra forma de tratamento que viole o RGPD.

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

3.1.2 - Incidente de segurança VS violação de dados

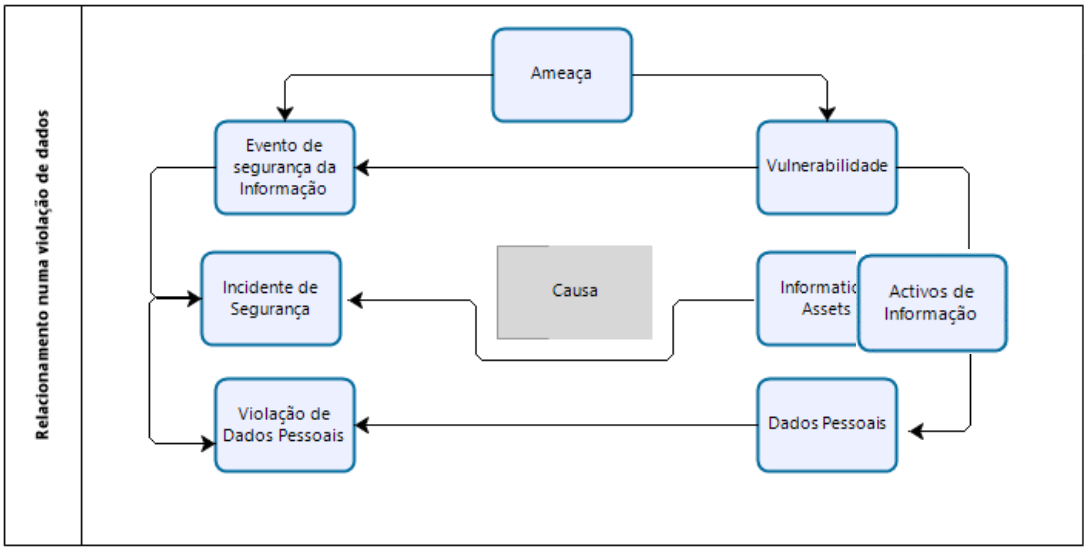
A ocorrência de um incidente de segurança não é classificada como violação de dados. Este só se traduz quando o evento configure uma perda de um ou mais pilares da segurança de informação e esta informação contenha dados pessoais. Assim, uma violação de dados é um tipo de incidente de segurança.

A consequência de tal violação é que o responsável pelo tratamento não poderá assegurar o cumprimento dos princípios relativos ao tratamento de dados pessoais, conforme definido no artigo 5.º do RGPD. Isto realça a diferença entre um incidente de segurança e uma violação de dados pessoais – em essência, enquanto todas as violações de dados pessoais são incidentes de segurança, nem todos os incidentes de segurança são necessariamente violações de dados pessoais.

Uma violação de dados pode ser intencional (desconsiderando-se a tipologia de dolo nas suas diferentes formas e/ou negligência) e pode ser causado por questões técnicas ou não técnicas bem como incidir sobre a informação em suporte físico, ou digital.

3.2 - Princípios Básicos

Uma ameaça que explora uma vulnerabilidade [Digitalmente, por exemplo, no sistemas de informação ou Fisicamente, por exemplo, no processo de armazenamento da informação] pode causar a ocorrência de um incidente de segurança que, por sua vez, pode traduzir-se num incidente de segurança da informação que, por sua vez, contendo dados pessoais, é suscetível de se traduzir numa violação de dados pessoais.



3.3 - Tipos de Violação de Dados Pessoais

As violações podem ser categorizadas de acordo com os três princípios de segurança da informação:

- **Violação da confidencialidade** - quando existe uma divulgação ou acesso acidental, ou não autorizado a dados pessoais. Por exemplo:
  - dados pessoais enviados acidentalmente para alguém (interna ou externamente) que não possui uma necessidade legítima de vê-lo;

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815
Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

- base de dados do cliente comprometido, por exemplo, sendo acedida por outro cliente;
- registo em papel contendo dados pessoais sendo deixados desprotegidos para qualquer um ver, sejam armários desprotegidos, impressora, secretária, entre outros;
- equipa que acede ou divulga dados pessoais fora do âmbito da sua atuação ou autorização;
- ser enganado por terceiros permitindo o acesso indevidamente os dados pessoais de outra pessoa.

- **Violação da integridade** - quando existe uma alteração acidental ou não autorizada dos dados pessoais. Exemplo:
  - A eliminação ou alteração errónea dos números de contacto, ou endereços de email das pessoas.
- **Violação da disponibilidade** - quando existe uma perda de acesso, ou a destruição acidental ou não autorizada de dados pessoais. Importa igualmente notar que, dependendo das circunstâncias, uma violação pode dizer respeito à confidencialidade, à integridade e à disponibilidade de dados pessoais simultaneamente, assim como a qualquer combinação destas. Exemplo:
  - perda ou roubo de computador, dispositivos móveis ou registos em papel contendo dados pessoais;
  - perda de dados pessoais devido a circunstâncias imprevistas, como incêndio ou inundação;
  - quando ocorrer uma perda permanente ou destruição de dados pessoais.

3.4 - Consequências possíveis de Violação de Dados Pessoais

Uma violação pode, potencialmente, ter um leque de efeitos adversos significativos sobre as pessoas bem como sobre as Organizações.

3.4.1 - Titulares dos Dados

Relativamente aos **titulares dos dados** podem resultar em danos físicos, materiais ou imateriais, entre os quais: a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação e a perda de confidencialidade de dados pessoais protegidos por sigilo profissional. Podem incluir igualmente qualquer outra desvantagem económica ou social significativa para essas pessoas singulares.

3.4.2 - Responsável pelo Tratamento

Numa perspetiva do Responsável pelo Tratamento, uma violação de dados poderá culminar num risco reputacional, risco financeiro, risco litigância, entre outros, significando um impacto negativo na atividade, nas relações com terceiros e na segurança sendo que estas consequências deverão ser também ponderadas na definição do risco bem como das mediadas de segurança adotadas.

Compete ao Município, enquanto responsável pelo tratamento, antes de notificar a violação à autoridade de controlo, aferir a probabilidade de observar estes efeitos adversos. Quando existe um risco elevado de ocorrência destes efeitos adversos, o RGPD exige que o responsável pelo tratamento comunique a violação aos titulares afetados logo que seja razoavelmente possível. A importância de ser capaz de identificar uma violação, avaliar o risco para os titulares e, então, proceder à notificação, se necessário, é salientada no considerando 87 do RGPD.

Contudo, a ocorrência das consequências acima referidas não depende apenas da violação em si, mas dos circunstancialismos em que ocorre, em particular, dos controlos técnicos e organizativos no domínio da segurança existentes.

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

Na eventualidade de uma violação de dados, deve o Município:

- Aferir se existiam – técnicas e organizativas- no domínio da segurança para evitar a ocorrência das consequências acima identificadas.
- Aferir se após a ocorrência do incidente são aplicadas as medidas – técnicas e organizativas- no domínio da segurança para evitar a concretização das consequências acima identificadas.
- Aferir as consequências possíveis, verificadas ou com forte hipótese no âmbito da avaliação da gravidade da violação dos dados pessoais. Esta ponderação é essencial para determinar a necessidade da comunicação aos titulares dos dados pessoais.

3.5 - Objetivos na Gestão de Violação de Dados

Como ponto central na gestão de violação de dados, o Município necessita de criar procedimentos e controlos de forma a permitir uma resposta suficiente numa eventual violação de dados pessoais. O principal objetivo numa Organização deverá ser evitar a ocorrência de uma violação, minimizando as potenciais causas e, subsequentemente, dirimir os eventos impactos que desta possam resultar.

A aplicação de medidas de segurança deverão ter em consideração o Impacto- potencial Impacto (Ex. operação de tratamento em causa, tipo de tratamento, etc.) e a gravidade – potencial gravidade (atendendo à tipologia dos dados, quantidade dos dados, quantidade de titulares dos dados afetados).

3.5.1 - Plano de Ação

A estruturação de um Plano de Ação apropriado deverá passar por incluir:

- Que eventos de segurança da informação são detetados e tratados de maneira eficiente, em particular a decisão de quando eles devem ser classificados como incidentes de segurança da informação;
- Que os incidentes de segurança com dados pessoais são detetados e geridos de uma forma eficiente, em particular, na decisão de classificá-los como Violação de Dados Pessoais;
- Que as Violações de Dados Pessoais são detetados e geridos de uma forma eficiente, em particular, na decisão de notificação ou não destes;
- Que as Violações de Dados Pessoais identificados são avaliadas e respondidas da maneira mais apropriada e maneira eficiente;
- Que os efeitos adversos da violação de dados pessoais sobre as Organizações e os titulares dos dados pessoais são minimizado por controlos, técnicos e organizativos, apropriados como parte da resposta a incidentes;
- Existe uma ligação com o Responsável pelo Tratamento dos dados Pessoais – Responsável pela Implementação da Privacidade – Encarregado de Proteção de Dados – Comissão de Segurança;
- As vulnerabilidades de segurança da informação (quando aplicável) são avaliadas e tratadas adequadamente para prevenir ou reduzir incidentes. Essa avaliação pode ser feita pela Comissão de Segurança;
- Melhorar as medidas organizativas e técnicas no domínio da segurança adotadas e a adotar no sentido de diminuir a exposição ao risco da ocorrência de outra violação de dados.

3.5.2 - O que é necessário para atingir os objetivos acima identificados por parte do Município:

- Melhorar, continuamente, as medidas de segurança de informação;

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

- Reduzir a sua exposição risco. Para tal, deverá observar uma abordagem baseada no risco, na definição e implementação aquando dos seus processos internos;
- Proceder, antes do tratamento de dados pessoais, a uma avaliação do impacto sobre a proteção de dados, a fim de avaliar a probabilidade ou gravidade particulares do elevado risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco. Essa avaliação do impacto deverá incluir, nomeadamente, as medidas, garantias e procedimentos previstos para atenuar esse risco, assegurar a proteção dos dados pessoais e comprovar a observância do regulamento;
- Adotar uma abordagem estruturada de gestão de Violações de Dados Pessoais;
- Reforçar o foco na prevenção de incidentes de segurança da informação dentro do Município, incluindo o desenvolvimento de métodos para identificar novas ameaças e vulnerabilidades. A análise de dados relacionados a incidentes permite a identificação de padrões e tendências, facilitando assim um foco mais preciso na prevenção de incidentes e identificação de ações apropriadas para evitar mais ocorrências;
- Melhorar a priorização sempre que possível;
- Assegurar a existência de um registo de Violações de Dados;
- Garantir que os incidentes de segurança da informação são documentados de maneira consistente, usando padrões apropriados para categorização de incidentes, adotando uma classificação normalizada das categorias de incidentes de segurança, violação de dados e categorias de Dados Pessoais;
- Partilhar essas classificações;
- Usando padrões apropriados para categorização de incidentes, classificar e compartilhar para que as métricas possam ser derivadas de dados agregados durante um período, devendo para o efeito definir métricas para valorizar/ categorizar a Violação de Dados em causa;
- Implementar Controlos para Reduzir riscos e proteger a informação;
- Definir competências no âmbito da gestão de violação de dados, estabelecendo responsabilidades neste âmbito bem como meios de comunicação e interseção entre os diferentes sectores responsáveis.

3.5.3 - Considerações a ter na Elaboração de um Plano:

3.5.3.1 - Do ponto de Vista de Segurança:

- **T**amanho, estrutura e natureza do Município, incluindo ativos, processos e processos críticos com dados que devem ser protegidos;
- Escopo de qualquer sistema de gestão de segurança da informação para tratamento de incidentes;
- Risco potencial devido a incidentes;
- Os objetivos da sua atividade.

3.5.3.2 - Do ponto de Vista da Proteção de Dados Pessoais:

- A origem, a natureza e o tipo de tratamento de dados;
- As categorias e o número aproximado de titulares de dados afetados;
- As categorias e o número aproximado de registos de dados pessoais.

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

4 - Fases

Antes do Incidente		Despois do Incidente						
Fases de Processo								
Preventivo		Inicio		Investigação			Encerramento	
Atividades								
Plano	Preparação	Deteção	Reporte	Recolha de informação	Avaliação	Emissão de Parecer	Comunicação	Monitorização

4.1 - Plano e Preparação

Para a efetividade da presente Politica de Violação de dados é necessário:

- Aprovação pelo Executico desta política, da comunicação desta política bem como de qualquer alteração e atualização da mesma;
- Enquadramento e compatibilização com as restantes Políticas de Proteção de Dados, normas e procedimentos do Município;
- Definir o que se enquadra no âmbito da Violação de dados;
- Definir competências de atuação, nomeadamente, a quem compete reportar, investigar, emitir parecer, decidir sobre a comunicação para entidades de controlo, decidir sobre a comunicação aos titulares dos dados pessoais, fazer a ponte entre estes e o Responsável pelo Tratamento de Dados, definir um plano de resposta, implementá-lo, supervisionar a sua implementação e reavaliar de forma a compreender se as mesmas foram eficientes para mitigar a sua probabilidade de ocorrência e gravidade relativamente aos potencias impactos por estas gerados;
- Definir o papel dos intervenientes, Comissão de Segurança da Informação e Privacidade, a ligação com o EPD e Executivo;
- Definir e estabelecer a coordenação interna com terceiros diretamente envolvidos, nomeadamente, subcontratantes;
- Estabelecer e implementar controlos técnicos e organizativos, entre quais, o procedimento no caso de violação de dados pessoais capazes de operacionalizar a presente política;
- Criar e desenvolver ações de sensibilização e formação para explicar as questões consignadas na presente política;
- Testar o procedimento criado para dar resposta à violação de dados.

4.2 - Deteção e Reporte

A segunda fase da Gestão de Violação de Dados Pessoais envolve a deteção e recolha de informações associadas, potencialmente relatórios sobre ocorrências de eventos que podem enquadrar-se como violações de dados para identificar as seguintes questões:

- A origem do incidente;
- Momento em que ocorreu;
- Momento em que foi detetado e reportado;
- Ativos e pessoas envolvidos;
- Quantidade e a natureza dos dados pessoais envolvidos;
- Quantidade e a Tipologia dos titulares de dados envolvidos;

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815
Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

- Detalhes das Ações já tomadas para mitigar e recuperar o nível de segurança/mitigar a gravidade e probabilidade de impacto do incidente.

Para a fase deteção, o Município deve realizar as seguintes atividades:

- Definir competências na avaliação do evento (Comissão de Segurança da Informação e Privacidade,, EPD);
- Definir e disseminar pela Município sobre qual o meio idóneo para a comunicação destes eventos (interna e externamente);
- Disseminar e instruir todos os trabalhadores do Município sobre que informação e quais os prazos para esta comunicação;
- Prever, juntamente com entidades terceiras, que tratem dados do Município ou que possam ter conhecimento de incidente de segurança e/ou potencial violação de dados, formas de alerta. Por exemplo, um trabalhador auxiliar de serviços gerais que verifica que um armário com documentos nos quais constem dados pessoais foi arrombado; entidade terceira na qual os dados pessoais da responsabilidade do Município se encontravam alojados e que foram apagados acidentalmente ou, no caso de dados cifrados de forma segura, ocorra a perda da chave de decifração;.

Para a fase de análise, o Município deve realizar as seguintes atividades:

- Detetar e relatar a ocorrência de um evento de segurança da informação ou a existência de uma vulnerabilidade de segurança (quando aplicável);
- Recolher informações sobre um evento ou vulnerabilidade de segurança da informação (quando aplicável);
- Recolher informações sobre fontes de dados internas e externas, incluindo registos de tráfego e atividades do sistema e da rede, circunstancialismo políticos, sociais e/ou económicos que podem influenciar o impacto da Violação de Dados;
- Tratando-se uma Violação de Dados, que ocorra no meio digital, aferir a existência de evidências respeitando o procedimento de recolhida e armazenamento da mesma, permitindo a conservação de prova, em particular, quando em causa possa estar uma conduta dolosa e, ou até, quando a origem da violação de dados consubstancie um ato com dignidade criminal ou responsabilidade civil;
- Tratando-se uma Violação de Dados, que ocorra no meio físico, aferir a existência de duplicação de informação e indicar o local em que o incidente possa ter ocorrido.

4.3 - Recolha de Informação e Avaliação

4.3.1 Enquadramento

A terceira fase envolve a avaliação da informação associada ao incidente e decisão de classificá-la como uma violação de dados ou não.

Sendo uma violação de dados detetada e reportada por qualquer trabalhador, subcontratante, terceiro..., o Município deve:

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

- Distribuir responsabilidades e competências: A informação deve ser sujeita a uma avaliação por parte da pessoa, entidade, figura (EPD, Comissão de Segurança da Informação e Segurança) que defina os passos necessários à aferição e que remete para quem tem competência para decidir sobre a (in)existência de violação de dados bem como a necessidade ou não de comunicar a violação de dados;
- Providenciar um procedimento de comunicação;
- Seguir padrões de análise e classificação do incidente como violação de dados pessoais.

Para atingir os objetivos acima referidos, o Município deve:

- Recolher toda a informação que possa ser relevante para a tomada de decisão;
- Registar toda a informação recolhida e medidas implementadas;
- Avaliar a informação e a possibilidade da sua subsunção a uma violação de dados pessoais;
- Assegurar o envolvimento de todas as partes pertinentes ao processo de avaliação;
- Assegurar a tomada imediata de medidas – técnicas e organizativas- para mitigar o impacto do incidente bem como a probabilidade da sua repetição;
- Designar competências para o cumprimento das referidas tarefas;
- Assegurar que a informação é devidamente analisada;
- Assegurar que todas as evidencias- factos e controlos – são registados e mantidos como evidencias;
- Assegurar que o procedimento é cumprido.

4.3.2 - Quando é que existe uma Violação de Dados Pessoais?

Uma violação de dados ocorre quando uma organização sofre um incidente de segurança relativo aos dados pelos quais é responsável que resulta numa violação da confidencialidade, da disponibilidade ou da integridade dos dados. Se tal ocorrer, e se a violação for suscetível de representar um risco para os direitos e as liberdades de uma pessoa, a organização tem de notificar a autoridade de controlo sem demora injustificada e, o mais tardar, no prazo de 72 horas após tomar conhecimento. Se a organização for um subcontratante, tem de notificar todas as violações de dados ao responsável pelo tratamento.
Se a violação de dados representar um elevado risco para as pessoas afetadas, estas devem também ser informadas (a menos que existam medidas de proteção técnicas e organizativas eficazes ou outras medidas destinadas a garantir que não é provável que o risco se volte a concretizar).

4.3.3 - Risco

Ao avaliar o Risco resultante de um incidente com dados pessoais deverão ser considerados os **riscos apresentados pelo incidente de segurança em si tais como:**

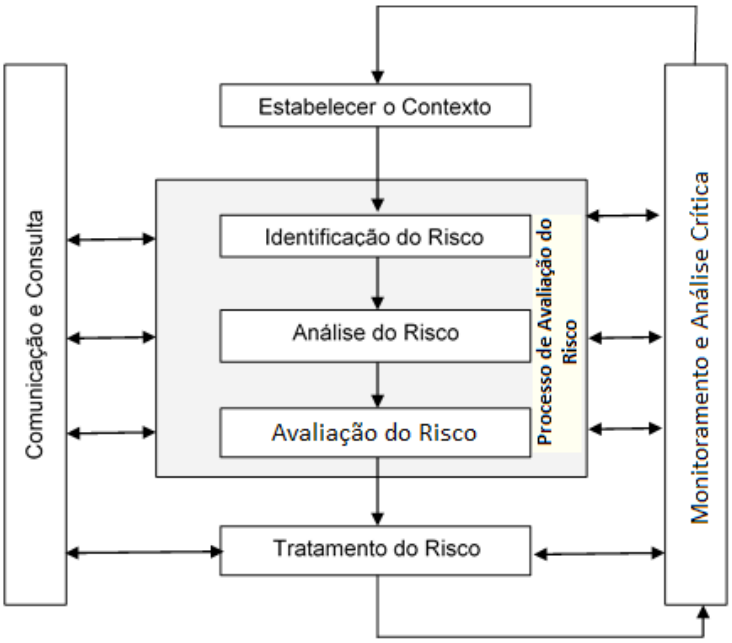
- A destruição, perda e alteração acidental ou ilícita dos dados;
- A divulgação ou acesso não autorizado a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a danos físicos;

E, ainda, deverão ser considerados **os riscos inerentes ao tratamento de dados em causa**:

- Devassa da vida privada, a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação e a perda de confidencialidade de dados pessoais protegidos por sigilo profissional

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt



Todo o processo de avaliação deverá ser devidamente documentado de forma a permitir demonstrar à Autoridade de Controlo o cumprimento das exigências dos artigos 32.º e 33.º do RGPD.
Para aferir o risco é necessário avaliar a situação casuisticamente, sendo o **Município** capaz de:

4.3.3.1 - Estabelecer o Contexto:

- **Circunstancialismo:** como, quando ocorreu e partes envolvidas;
- **Ativos em causa:** São designados ativos da informação, sistemas, portais, servidores, base de dados, equipamentos de comunicação, contratos que devem ser identificados;
- **Determinação do Valor da Informação**: Para cada ativo de informação identificado, é efetuada a classificação no que se refere à confidencialidade, integridade e disponibilidade.

4.3.3.2 - Identificação do Risco

- **Identificar os dados pessoais em causa:**
  - Natureza dos dados;
  - Quantidade de dados pessoais;
  - Natureza dos titulares;
  - Quantidade de titulares.
- **Identificar o(s) tratamento(s) de dados pessoais em causa;**
- **Identificar os riscos apresentados pelo tratamento, em concreto, em particular, que possam resultar da violação de dados (Ponto 4.3.1).**

4.3.3.3 - Análise do Risco

- **Identificar os Controlos- medidas técnicas e organizativas:** Identificar e ponderar as medidas existentes ou aplicáveis após a deteção da Violação de Dados com vista a mitigar o impacto da ocorrência do mesmo;

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815
Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

- **Analisar e ponderar a gravidade e a probabilidade dos riscos atendendo à Violação de dados em concreto.**

4.3.3.4 - Avaliação do Risco

- **Qual a probabilidade de a violação resultar um risco para o(s) Individuo(s)?**

A Probabilidade expressa a possibilidade de ocorrer um risco. Depende principalmente do nível de vulnerabilidades dos ativos de suporte quando sob ameaça e do nível de recursos das fontes de risco para explorá-los.
Pode ser equacionada em 3 ou 5 graus consoante a variabilidade e complexidade de uma organização;
A título de exemplo num modelo de 5 graus:

Não envolve	A não envolvência ou não representação deve aplicar-se no caso de uma violação de dados, por exemplo, já transformados para efeitos [Estatísticos], não sendo possível a sua reversão;
Improvável	Não parece possível que as fontes de risco existentes materializem as ameaças explorando as propriedades de ativos de suporte (por exemplo, roubo de documentos em papel armazenados em uma sala protegida por um leitor de crachá e código de acesso);
Limitada	Parece difícil para as fontes de risco selecionadas materializar a ameaça explorando as propriedades dos ativos de suporte;
Provável	Parece possível que as fontes de risco selecionadas materializem a ameaça explorando as propriedades de ativos de suporte;
Muito Provável	Parece extremamente fácil para as fontes de risco selecionadas materializar a ameaça, explorando as propriedades de ativos de suporte.

Para a sua avaliação, **o Município** deve:

- Aferir a aplicação de medidas de proteção adequadas (técnicas e organizativas) aos dados pessoais afetados pela violação que tornem os dados pessoais incompreensíveis ou inacessíveis para terceiros não autorizados, tais como cifragem, anonimização;
- Aferir a implementação de medidas de partição de dados de modo a reduzir a possibilidade de que os dados pessoais possam ser correlacionados e que uma violação de todos os dados pessoais possa ocorrer;
- Aferir a implementação dos seguintes controlos nos dados pessoais:
    - Filtragem e remoção;
    - Redução da sensibilidade por conversão;
    - Redução da natureza de identificação dos dados;
    - Redução da acumulação de dados;
    - Restrição do acesso a dados.

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

- Aferir a implementação de controlos Lógicos, quando aplicável, especificando regras aplicáveis à definição de perfis e às senhas (duração mínima, caracteres necessários, duração da validade, número de tentativas falhadas antes que o acesso à conta seja bloqueado, etc.);
- Aferir a existência de Controlos Físicos, quando aplicável;
- Aferir a existência de Controlos Organizacionais.

4.3.3.5 - Existe um risco elevado para os direitos e liberdades dos titulares?

Haverá, com toda a certeza, vários níveis de suscetibilidade de verificação de risco para os Direitos, Liberdades dos Titulares dos Dados Pessoais. À luz das obrigações do RGPD, bastará a existência de um risco mínimo para ser necessário o cumprimento da obrigação de notificação.

O conceito de "elevado risco" deve ter em consideração:

- A inexistência de medidas de proteção adequadas (técnicas e organizativas) aos dados pessoais afetados na violação, especialmente medidas acima identificadas (anonimização, partição, cifragem, etc.);
- A não adoção de medidas subsequentes que garantam a impossibilidade de concretização do elevado risco para os Direitos e Liberdades dos Titulares dos dados pessoais; ou
- O esforço desproporcional que a comunicação aos titulares pode implicar. Neste ponto a comunicação poderá ser feito por comunicação pública ou algo semelhante.

Os termos do n.º 3 do artigo 34.º permitem um auxílio no preenchimento deste conceito:

- A aplicação de medidas de proteção adequadas (técnicas e organizativas) aos dados pessoais afetados pela violação, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem:
  - Deve ter-se em consideração a aplicação originária de medidas técnicas e organizativas de proteção de dados;
  - Deve ter-se em consideração a aplicação subsequente, de resposta, de medidas técnicas e organizativas para mitigar/diminuir a probabilidade de violação de dados;
- A adoção pelo Responsável pelo Tratamento de Dados Pessoais de medidas subsequentes que garantam a impossibilidade de concretização do elevado risco para os direitos e liberdades dos titulares dos dados.

4.3.3.6 - Emissão de Parecer

Nesta terceira fase deve proceder-se a avaliação da informação associada com a ocorrência ao evento. Para tal, o Município deverá:

- Definir a responsabilidade no âmbito da gestão de violação de dados e de comunicação;
- Definir um procedimento de comunicação;
- Recorrer às orientações de segurança da informação e gestão de incidentes.

4.3.3.6.1 - E se não possuir todas as informações necessárias?

O RGPD reconhece que nem sempre é possível investigar uma violação completamente no prazo de 72 horas para entender exatamente a ocorrência e o que precisa ser feito para mitigá-la. Portanto, o n.º 4 do artigo 33º prevê que a recolha de

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

informação seja realizada por fases fases, desde que não implica uma demora indevida. Neste período, os controladores priorizam a investigação fornecendo os recurso adequados.

O Município deve notificar a Autoridade de Controlo sobre a violação, disponibilizando todas as informações necessários. Caso o Município não consiga fornecer detalhes completos em 72 horas, deverá notificar a Autoridade, justificar o atraso bem como indicar uma previsão para a conclusão.

4.3.3.7 - Notificações

- A imposição legal de comunicar a Violação de Dados pessoais reside na premissa que esta violação seja suscetível de "causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares." (Cf. Considerando(8);
- Existe a obrigação de notificar a Autoridade de Controlo se a violação de dados pessoais for suscetível de resultar **num risco** para os direitos e liberdades das pessoas singulares;
- Subsiste a obrigação de notificação aos titulares dos Dados Pessoais se a violação de dados pessoais for suscetível de resultar num **elevado risco** para os direitos e liberdades das pessoas singulares.

O Município deve:

- Avaliar se violação é suscetível de "causar danos físicos, materiais ou imateriais às pessoas singulares" e, em caso positivo, aferir quais os danos em causa;
- Caso considere ser suscetível, então deverá proceder à comunicação na Autoridade de Controlo Competente;
- Avaliar se violação é suscetível de representar um risco elevado para os direitos e liberdades das pessoas singulares;
- Caso considere que é, deverá comunicar aos titulares, aferindo qual o meio mais idóneo de o fazer.

Caso o Município decida pela notificação aos titulares:

- Deverá descrever a natureza da violação de dados pessoais e dirigir recomendações à pessoa singular em causa para atenuar potenciais efeitos adversos;
- Deverá ser efetuada logo que seja razoavelmente possível, em estreita cooperação com a autoridade de controlo e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes.

Obrigações de comunicação em caso de subcontratante:

- A obrigação de notificação de Violação de Dados é extensiva ao subcontratante que deve notificar o responsável pelo tratamento de dados após ter conhecimento de uma violação de dados pessoais para que, este último, possa cumprir a obrigação de comunicação junto da autoridade de controlo;
- O prazo de 72h não se encontra previsto para o subcontratante. Contudo, esta comunicação deverá ser feita no mais curto espaço de tempo, atento ao conceito de demora injustificável aplicável a ambos bem como a premência de o responsável notificar tal violação à autoridade de controlo.

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

4.3.3.8 - Monitorização do Incidente e Encerramento

Independentemente de uma violação necessitar ou não de ser notificada à autoridade de controlo, o responsável pelo tratamento deve proceder à conservar da documentação de todas as violações, como on.º 5 do artigo 33.º explica: *«O responsável pelo tratamento documenta quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à autoridade de controlo verificar o cumprimento do disposto no presente artigo*.»

O presente prende-se com o cumprimento do princípio da responsabilidade do RGPD (*accountability*), constante no n.º de 2 do artigo 5º e no artigo 24º, sendo que a autoridade de controlo pode exigir a consulta destes registos.
O Município deve:

- Criar e manter um registo interno de violações, independentemente de terem de notificar ou não;
- Deve fixar um método e estrutura a ser utilizar na documentação de uma violação;
- Nesse registo deve conter as informações relativas à violação, que devem incluir as suas causas, o que aconteceu e os dados pessoais afetados. Deve também incluir os efeitos e consequências da violação, juntamente com a medida de reparação adotada pelo responsável pelo tratamento:
  - Deve estabelecer um prazo de conservação dessa documentação;
  - Quando esses registos contiverem dados pessoais, caberá ao Município determinar o período apropriado de conservação em conformidade com os princípios relacionados com o tratamento de dados pessoais e atender a uma base legal para o tratamento;
  - Será necessário conservar a documentação de acordo com o n.º 5 do artigo 33.º, na medida em que pode ser chamado a fornecer prova do cumprimento do disposto nesse artigo ou, de um modo mais geral, com o princípio da responsabilidade, à autoridade de controlo. Se os próprios registos não contiverem dados pessoais, então, o princípio da limitação da conservação do RGPD não se aplica.
- Deve documentar a sua fundamentação para as decisões tomadas em resposta a uma violação. Em especial, se uma violação não for notificada, deve ser documentada a justificação para essa decisão. Isto deve incluir as razões pelas quais o Município considera que a violação não é suscetível de resultar num risco para os direitos e liberdades das pessoas singulares;
- Deve fornecer prova adequada quando o Município considera que se encontra preenchida qualquer uma das condições que constam do n.º 3 do artigo 34.º.

4.3.3.9 - Aprendizagem

Para dotar o Município de capacidade para responder face a uma violação de dados pessoais é necessário:

- Que entenda o conceito de violação de dados pessoais;
- Que prepare um plano de resposta para solucionar quaisquer violações de dados pessoais que ocorram;
- Que atribua a responsabilidade de gestão de violações a uma pessoa ou equipe dedicada;
- Que conheça a tramitação no caso da suspeita de Violação de Dados Pessoais.

4.3.3.10 – Avaliação

Na avaliação devem verificar-se os seguintes requisitos:

- O Município implementou um processo para avaliar o risco provável para as pessoas como resultado de uma violação;

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815
Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

- O Município sabe quem é a autoridade supervisora relevante para nossas atividades de processamento;
- O Município tem um processo para notificar a de uma violação dentro de 72 horas após tomar conhecimento, mesmo que ainda não possua todos os detalhes:
  - O Município sabe quais informações devemos fornecer à OIC sobre uma violação;
  - O Município tem um processo para informar as pessoas afetadas sobre uma violação quando é provável que isso resulte em um alto risco para seus direitos e liberdades;
  - O Município sabe que deve informar as pessoas afetadas sem demora injustificada;
  - O Município sabe quais informações sobre uma violação que deve fornecer aos indivíduos e que deve fornecer orientações para a sua proteção;
  - O Município tem um processo de documentação de todas as violações, mesmo que elas não requeiram relato, e monitoriza a sua existência.

Anexos

Anexo 1

Procedimento para Violação de Dados Pessoais.

Anexo 2

Formulário para a participação de Violação

Anexo 3

Registo de Violação de Dados

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

MUNICÍPIO DE SÃO PEDRO DO SUL

Anexo 1

Política de Violação de Dados – Procedimento

Introdução

- O Município procede ao tratamento de dados pessoais, constituindo este um ativo valioso que precisa ser adequadamente protegido;
- São tomadas as medidas técnico-organizativas, no domínio da segurança para proteger os dados pessoais de incidentes (acidental ou deliberados) de forma a evitar violações de dados pessoais
- Para tal, o Município precisa de dotar-se de uma política robusta e de um processo sistemático para responder a qualquer violação de dados pessoais, detetar, investigar bem como estabelecer um procedimento de comunicação de modo a garantir uma atuação em conformidade com as exigências legais, facilitar as tomadas de decisão e a mitigação do risco da sua ocorrência e do impacto potencial que o mesmo pode gerar;
    - Uma violação de dados ocorre quando uma organização sofre um incidente de segurança relativo aos dados pelos quais é responsável que resulta numa violação da confidencialidade, da disponibilidade ou da integridade dos dados;
    - Parte dessas medidas passa por elucidar todos os seus trabalhadores, prestadores de serviço, terceiros sobre contexto, conteúdo e respetivo procedimento em caso de incidente de segurança com dados pessoais.

Finalidade e âmbito

- Nos termos da legislação de proteção de dados, o Município é obrigado a implementar medidas para garantir a segurança de todos os dados pessoais durante seu ciclo de vida, incluindo definir competências e responsabilidades nesta matéria;
- Esta política estabelece as diretrizes a ser seguir para garantir uma abordagem consistente e eficaz, face a uma violação de dados aplicável a todo o Município, estabelecendo as obrigações relativas ao reporte de violação de dados pessoais, responsabilidades e respetivos procedimentos;
- Esta política aplica-se a todos os dados pessoais sujeitos a qualquer tratamento de dados na ou por conta do Município, independentemente do formato;
- Esta política aplica -se a todos os trabalhadores, independentemente do vínculo contratual, fornecedores, consultores, prestadores de serviço ou terceiros que tenham acesso a dados pessoais por conta da relação com o Município;
- O objetivo desta política é mitigar a ocorrência de violação de dados, diminuindo o risco associado e estabelecer as ações para evitar outras violações.

Definições

- **Dados pessoais:** informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, iden-

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

tificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

- **Incidente de Segurança:** Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.

- **Responsável pelo tratamento:** a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;

- **Violação de dados pessoais:** Uma violação de dados é uma violação da 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.

Reporte de um Incidente

- Qualquer pessoa que trate dados pessoais em nome e por conta do Município é responsável por reportar um eventual ou suspeito incidente de segurança com dados pessoais imediatamente à Comissão de Segurança de Informação e Privacidade, através de formulário próprio ou mensagem de correio eletrónico destinada a rgpd@cm-spsul.pt.
- Se a violação ocorrer ou for descoberta fora do horário normal de trabalho, ela deve ser relatada assim que é praticável;
- A Comunicação deverá incluir os detalhes completos e precisos do incidente, quando a violação ocorreu (datas e horários), quem os está a reportar, que dados pessoais poderão estar em causa e a respetiva quantidade, quantos e qual a natureza dos titulares dos dados a que os dados respeitam.
- Tal informação deverá constar de um Formulário de Relatório de Incidente que deve ser preenchido como parte do processo de reporte;
- Todos os trabalhadores deverão estar cientes sobre o que é uma violação de dados e qual o procedimento a seguir no caso da sua ocorrência.

Mitigação e recuperação

- O Município poderá estabelecer, de acordo com o Encarregado de Proteção de Dados (EPD), a Comissão de Segurança da Informação e Privacidade medidas de implementação imediatas para mitigar o evento e minimizar os efeitos da violação.

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

- Uma avaliação inicial será feita pelo EPD em contacto com o (s) serviço (s) relevante (s) para estabelecer a gravidade da violação. A coordenação da investigação da violação poderá ser atribuída à Comissão de Segurança da Informação e Privacidade ou até o próprio EPD.

Investigação e Avaliação do Risco

- Uma investigação será realizada pelo Município, sempre que possível, num prazo de 24 horas da violação após identificada/relatada;
- Os serviços deverão auxiliar os trabalhos de investigação, procedendo ao apoio suscitado pelo Município para analisar e avaliar o evento;
- Os serviços deverão apurar, entre outras informações:
  - A origem do incidente;
  - Momento em que ocorreu;
  - Momento em que foi detetado e reportado;
  - Ativos e pessoas envolvidos;
  - Quantidade e a tipologia dos dados pessoais envolvidos;
  - O tipo e a quantidade de titulares de dados envolvidos.;
  - Detalhes das ações tomadas para mitigar e recuperar o nível de segurança/mitigar a gravidade e probabilidade impacto.

Notificação

- Compete ao Município, após consulta e parecer do EPD, estabelecer se deverá ou não proceder à notificação da Autoridade de Controlo e aos titulares dos dados pessoais;
- Nesse caso, o Município tem 72h após a tomada de conhecimento da violação para proceder à comunicação à Autoridade de Controlo;
- Todos os incidentes deverão ser avaliados casuisticamente e deverão ser considerados os seguintes elementos:
  - Se a violação é suscetível de implicar um risco para os direitos e liberdades dos titulares dos dados pessoais;
  - Se a notificação poderá auxiliar a mitigação do risco, nomeadamente, do uso indevido de informação;
  - Se existem obrigações legais e contratuais de reporte.
- Compete ao Município, após esta deliberação, notificar a Autoridade de Controlo;
- Compete ao EPD, salvo outras funções atribuídas, cooperar com a Autoridade de Controlo;
- No âmbito desta cooperação poderão ser necessárias a averiguação de mais informação bem como a determinação de novas medidas pelo que devem os trabalhadores, no âmbito das suas funções cooperarem com o Município e com o EPD para a implementação das mesmas,
- Deverá ser mantido um registo de todas as ações resultantes do evento, independentemente da existência ou não de notificação.

Avaliação e Resposta

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt

- Uma vez contido o incidente inicial, o EPD deverá:
  - Realizar uma revisão completa das causas da violação;
  - Verificar a eficácia da(s) resposta(s);
  - Avaliar se há alterações introduzir nos sistemas, políticas e procedimentos.
- Os controlos existentes deverão ser revistos para determinar sua adequação e se alguma ação corretiva
- devem ser tomada para minimizar o risco de ocorrência de incidentes semelhantes;
- A revisão poderá ter em consideração:
  - Competências e responsabilidades;
  - Processos de tratamento de dados;
  - Meios de comunicação, transmissão ou armazenamento dos dados;
  - Os controlos técnicos e organizativos;
  - Respeito pelos princípios de tratamento de dados, em especial, de minimização e exatidão;
  - Consciencialização e dotação de ferramentas para os trabalhadores;
  - Revisão do plano de violação de dados e identificação de responsáveis.
- Se considerado necessário, um relatório recomendando qualquer alteração nos sistemas, políticas e procedimentos deverá ser elaborado pela Município;
- Os controlos existentes deverão ser revistos para aferir da sua adequação e se alguma ação corretiva deve ser tomada para minimizar o risco de ocorrência de incidentes semelhantes.

9.Revisão da Política

- Esta política será atualizada conforme se mostre necessário para refletir as melhores práticas garantir a conformidade com quaisquer alterações legislativas relevante.
- Esta política foi revista pela última vez em 09/06/2022.

Largo de Camões
3660-436 São Pedro do Sul
NIF 506 785 815

Telef (+351) 232 720 140
Fax (+351) 232 723 406
www.cm-spsul.pt
geral@cm-spsul.pt