Controlo de versões:

Nº DA REVISÃO	DESCRIÇÃO DA ALTERAÇÃO	DATA DE ENTRADA EM VIGOR	EMISSOR
01/00	DOCUMENTO INICIAL	21/12/2022	GDP
01/01	ATUALIZAÇÃO - NOTIFICAÇÃO ELETRÓNICA	__/07/2024	GDP

O C.A. aprova

PRESENTE À SESSÃO DO
C. A. DE 02/10/2024
O Presidente Carlos Neves Martins
O Dir. Clínico ACSH Rui Tato Marinho
A Dir. Clínica ACSP Eunice Carrapiço
O Vogal Miguel Guimarães
O Vogal Francisco Matoso
A Enfª Directora Carla Martins Ribeiro
ATA Nº 46/2024

ELABORADO POR:	VERIFICADO POR:	APROVADO POR:
GABINETE DE PROTEÇÃO DE DADOS (GDP)	ENCARREGADA DE PROTEÇÃO DE DADOS (EPD)	CONSELHO DE ADMINISTRAÇÃO (CA)
ASSINATURA Dulce Maria Freire Afonso	ASSINATURA Ana Vidigal	ASSINATURA
DATA: 27/05/2024	DATA: 05/07/2024	DATA:

Índice

ENQUADRAMENTO

É obrigação do Responsável pelo Tratamento (RT) de dados pessoais notificar a Comissão Nacional de Proteção de Dados (CNPD) sempre que ocorra uma violação de dados pessoais que seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares, nos termos do artigo 33º do Regulamento Geral de Proteção de Dados (RGPD) e deve manter um registo documentado de todos os incidentes de violação de dados, tenham estes sido notificados ou não à CNPD e aos titulares.

Entende-se «**violação de dados pessoais**» como qualquer 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[1].

Essa notificação à autoridade de controlo competente deve ocorrer sempre que se conclua que a violação pode resultar num **risco** para os direitos e liberdades das pessoas singulares, devendo esta ocorrer até **72 horas** após o conhecimento pelo responsável da violação de dados.

Além disso, nos casos em que se verifique existir um **risco elevado** para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deverá igualmente comunicar a violação de dados ao titular dos dados sem demora injustificada, nos termos do artigo 34º do RGPD.

Pretende-se com este procedimento criar as condições para o cumprimento dessas obrigações legais e para que sejam tomadas as medidas necessárias e adequadas no sentido de apurar, o mais rapidamente possível, a existência de uma violação de dados pessoais e informar, imediatamente, a Autoridade de Controlo e o titular dos dados – caso se determine que estas comunicações são exigíveis, no contexto da violação de dados pessoais que venha a ocorrer na ULSSM.

O presente procedimento substitui o procedimento anterior, aprovado pelo Conselho de Administração e em vigor desde 21.12.2022, cessando os seus efeitos na data da entrada em vigor deste.

[1] Definição do n.º 12 do artigo 4.º do RGPD.

1 ÂMBITO

Este procedimento é aplicável a todos os profissionais, estudantes ou estagiários que exercem funções ou desenvolvem qualquer atividade na ULSSM, independentemente da relação de trabalho ou vínculo jurídico existente.

No caso de violação de dados pessoais comunicadas por **Subcontratantes**, o presente procedimento também deve ser aplicado.

Entendem-se fora do âmbito deste procedimento os incidentes de segurança não relacionados com dados pessoais.

2 FINALIDADE DO DOCUMENTO

- Fornecer as orientações necessárias para saber como atuar no caso de ocorrer um incidente de violação de dados pessoais;
- Definir funções e responsabilidades dos intervenientes na resposta a um incidente de violação de dados pessoais;
- Definir o fluxo de notificação de um incidente de violação de dados pessoais e garantir uma resposta atempada;
- Garantir a notificação atempada às partes interessadas relevantes.

3 CALENDARIZAÇÃO

Este procedimento deverá ser do conhecimento de todos os profissionais da ULSSM assim que for divulgado, e deverá ser consultado sempre que seja identificado um possível incidente de violação de dados pessoais.

4 ESTRUTURA DO PROCEDIMENTO

4.1 Pré-requisitos

Deverão ser assegurados **os seguintes pré-requisitos, antes deste procedimento ser implementado:**

i. Deve estar nomeada a Equipa de Resposta a Incidentes (ERI) para dar suporte ao GPD e/ou EPD na resposta à violação de dados (a identificação dos membros deste grupo será contextual à situação);

ii. A equipa de resposta deve ter formação prévia do funcionamento da plataforma HER+;

iii. A equipa de resposta deve compreender como funciona a atividade de tratamento de dados pessoais, ser capaz de caracterizar uma violação de dados pessoais e determinar a gravidade da mesma.

4.2 Fases de Implementação

1. **Deteção do incidente de segurança**
    a. Ocorrência e deteção do incidente de segurança por colaborador ou entidade externa.

2. **Caracterização**: esta fase ocorre após a deteção de um incidente de segurança, em que será necessário confirmar se o incidente implica uma violação de dados pessoais e inclui:
    a. Análise preliminar pelo **Gabinete de Proteção de Dados (GDP)**;
    b. Convocação da **Equipa de Resposta a Incidentes (ERI);**
    c. Caracterização da violação de dados.

3. **Avaliação**: após a caracterização da violação de dados, será necessário avaliar o seu impacto para determinar a sua gravidade. **Atendendo ao prazo para a notificação de uma violação de dados pessoais (72h)**, recomenda-se que a avaliação, se necessário, ocorra em duas etapas: avaliação preliminar e avaliação detalhada.

4. **Notificação à CNPD, se aplicável**: dependendo dos riscos para os direitos e liberdades das pessoas singulares, pode ser necessário notificar a **Comissão Nacional de Proteção de Dados (CNPD)** da violação de dados pessoais;

5. **Comunicação aos titulares de dados, se aplicável**: face à gravidade da violação, poderá existir a obrigação de notificar os titulares dos dados pessoais afetados pela violação.

6. **Resolução**: nesta fase deverão ser definidas e implementadas medidas técnicas e organizativas que permitam resolver a violação de dados pessoais.

7. **Registo**: deve proceder-se ao registo da violação de dados pessoais e atualizá-lo sempre que sejam efetuadas alterações às medidas adotadas ou sejam adotadas novas medidas.

4.3 Fluxo do circuito de notificação

A representação das etapas a seguir no processo de notificação de um incidente de violação de dados encontra-se no **Anexo I.**

4.4 DESCRIÇÃO DAS FASES DE IMPLEMENTAÇÃO

FASE I – DETEÇÃO DO INCIDENTE DE SEGURANÇA

O procedimento inicia-se a partir do momento em que qualquer pessoa que exerça funções ou desenvolva qualquer atividade na ULSSM detete (ou suspeite) de um incidente de violação de dados pessoais **passível de configurar uma violação de dados pessoais**.

O incidente de violação de dados pessoais poderá ser detetado internamente ou reportado por entidades externas. Independentemente da forma de deteção, este deve ser reportado o mais rapidamente possível, por forma a minimizar o impacto decorrente do mesmo, devendo ser adotados os procedimentos abaixo descritos para efeitos de notificação/reporte na ULSSM do incidente.

i) Notificação por entidades externas:

a. Notificação por **SUBCONTRATANTE** ou **ENTIDADE** que atue em **RESPONSABILIDADE CONJUNTA** com a ULSSM pelo tratamento de dados possivelmente afetado pela violação, por deteção do incidente na sua origem e conforme definido nos respetivos acordos de tratamento de dados pessoais.

b. Notificação por **ENTIDADES TERCEIRAS** recebida por um colaborador da ULSSM, ficando este com o dever de notificar o **GPD** e a **EPD** da ULSSM, assim que tomar conhecimento

da notificação do incidente. Nestas situações, o GPD, com o apoio da EPD, deverá fazer a ponte de contacto com a entidade externa em questão, solicitando a informação necessária para cumprimento do presente procedimento.

ii) Notificação interna por colaboradores da ULSSM:

a. Os colaboradores da ULSSM (independentemente do vínculo profissional) deverão reportar internamente qualquer incidente de que tenham conhecimento e seja passível de configurar uma violação de dados, independentemente do modo como tomaram conhecimento do mesmo.

b. Sempre que o **Serviço de Sistemas de Informação (SSI)** seja notificado ou detete a ocorrência de um incidente de segurança que possa configurar uma violação de dados pessoais por outra via, deverá reportar a mesma, sem demora injustificada, ao **GPD** e **EPD**.

c. Uma vez detetado o incidente de violação de dados pessoais, o colaborador deve proceder **imediatamente** ao seu **registo** na plataforma de gestão de violações de dados pessoais - "**HER+"** disponibilizada**,** que funciona em ambiente Web e é acessível através da intranet, seguindo os seguintes passos:

intranet ➲ Proteção de Dados ➲ Notificação de violação de dados pessoais ➲ Notificação de Violação de Dados ➲ Formulário Notificação de Violação de Dados.

FASE II -CARACTERIZAÇÃO

Uma violação de dados pessoais tem, normalmente, origem num incidente de segurança. No entanto, nem todos os incidentes de segurança configuram uma violação de dados pessoais. Como tal, após a deteção do incidente será necessário determinar se este implica, ou não, uma violação de dados pessoais.

Após receber a notificação do incidente, o **GPD** com o apoio do **EPD,** deverá reunir a informação disponível e proceder à **análise preliminar** da ocorrência com vista a determinar se o incidente de segurança

reportado configura, ou não, uma violação de dados pessoais. A caraterização do incidente implica a averiguação:

i. da origem;
ii. da tipologia da violação de dados pessoais;
iii. da natureza de dados pessoais envolvidos; e,
iv. do alcance do incidente.

Caso se conclua pela análise preliminar, que o incidente de segurança é passível de configurar uma violação de dados pessoais ou não seja possível descartar essa hipótese, o **GPD** com o apoio do **EPD,** deverá reportar ao Conselho de Administração a situação, devendo este órgão convocar a **EQUIPA DE RESPOSTA A INCIDENTES (ERI)** para que esta realize uma análise forense detalhada e identifique as ações adequadas para a resolução da situação. A composição da equipa será contextual à situação e poderá incluir:

MEMBROS	FUNÇÕES E RESPONSABILIDADES
Gabinete de Proteção de Dados (GPD)	• Responsável pela condução do procedimento de resposta a violações de dados pessoais
Encarregado da Proteção de Dados (EPD)	• Aconselhar o GPD ao longo de todo o procedimento; • Aconselhar o Conselho de Administração acerca da notificação da violação de dados pessoais à Autoridade de Controlo e titulares envolvidos; • Participar na definição e adoção de medidas de reação face a uma violação de dados pessoais; • Ser o ponto de contacto entre a ULSSM e a CNPD.
Elemento designado pelo Serviço de Sistemas de Informação/Responsável pela segurança	• Apoio na análise do impacto e consequências prováveis da violação de dados pessoais no âmbito das TI; • Emitir parecer sobre as consequências do incidente e participar na avaliação do risco; • Emitir parecer sobre medidas de contenção e reparação a adotar; • Auxiliar na identificação e adoção atempada de medidas de reação ao incidente.
Elemento designado pelo Gabinete Jurídico	• Apoio na análise do impacto e consequências prováveis da violação de dados pessoais;

	• Emitir parecer sobre implicações legais do incidente e ações subsequentes a adotar (por ex., eventuais queixas-crime); • Auxiliar na identificação e adoção atempada de medidas de reação ao incidente.
Conselho de Administração	• Decisor de várias etapas do presente processo, nomeadamente no aval para efetuar a notificação à CNPD e/ou comunicar as violações de dados aos titulares.
Responsável (eis) do (s) Serviço (s) Afetado(s)	• Colaborar na investigação; • Auxiliar na identificação e adoção atempada de medidas de reação ao incidente.
Elemento designado pelo Gabinete de Comunicação e Relações Públicas	• Para a eventualidade da realização de comunicações aos titulares de dados e/ou público em geral e/ou meios de comunicação social. • Avaliar o impacto do ocorrido nos meios de comunicação social e público em geral; • Decidir o nível, a frequência e o conteúdo das comunicações ao exterior; • Auxiliar na identificação e adoção atempada de medidas de reação ao incidente.
Elemento designado pelo Gabinete de Segurança	• Avaliar impacto e consequências prováveis da violação de dados pessoais na respetiva área de conhecimento.
Outros Serviços de Apoio	• Sempre que se justificar e se aplicável na sua área de intervenção, serão chamados a integrar a equipa de resposta a incidentes elementos de outros Serviços de Apoio, designadamente, Serviço de Recursos Humanos, Serviço de Saúde Ocupacional, Serviço de Instalações e Equipamentos, Gabinete de Risco e Serviço Social/Gabinete do Cidadão.

Uma vez constituída a **ERI**, esta procurará recolher toda a informação disponível sobre o incidente, de forma a proceder à sua **caracterização** e concluir efetivamente se o incidente de segurança **configura, ou não**, uma violação de dados.

i) Origem do incidente de segurança

Para caracterizar o incidente de segurança, será importante proceder ao levantamento da informação que permita identificar a sua origem. Para o efeito, podem ser utilizadas as seguintes questões:

- Como foi detetado o incidente que esteve na sua origem? (ex. e-mail, site, comunicação direta)

- A comunicação da violação de dados foi interna ou externa?
- O autor do incidente de segurança na origem da violação de dados é interno ou externo?
- O incidente foi acidental ou intencional?

ii) Tipologia da violação de dados pessoais

Consoante a origem do incidente, a violação de dados pessoais pode ter a seguinte tipologia:

Violação de confidencialidade	Quando existe uma divulgação ou acesso acidental ou não autorizado a dados pessoais.
Violação de integridade	Quando existe uma alteração acidental ou não autorizada dos dados pessoais.
Violação de disponibilidade	Quando existe uma perda de acesso ou a destruição acidental ou não autorizada de dados pessoais.

De 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.

iii) Natureza dos dados pessoais

Para a caracterização do incidente, será ainda importante identificar a natureza dos dados pessoais envolvidos no incidente, nomeadamente:

- A que tratamento/processo está associado? (por ex., processamento de salários, ficha de cadastro, processo clínico);
- A que categorias de titulares de dados pessoais respeita? (por ex., utentes, estagiários, trabalhadores);
- Quais as categorias de dados pessoais que estão em causa? (por ex., dados de identificação e contacto, dados de menores ou incapazes, categorias especiais de dados);
- Os titulares estão identificados ou são identificáveis?

iv Alcance do incidente

Deverá, ainda, ser recolhida informação que permita perceber qual o alcance da violação de dados:

- Estimativa do número de titulares de dados pessoais afetados pela violação de dados pessoais;
- Início e duração da violação de dados;
- Consequências da violação de dados (permanentes ou temporárias).

Fase III - AVALIAÇÃO DA GRAVIDADE DO INCIDENTE

Nesta fase, e dependendo da complexidade do incidente, a análise e avaliação da gravidade da violação de dados pessoais pela **ERI** não deverá ultrapassar as **72 horas** após o conhecimento do incidente. Recomenda-se, por isso, que esta avaliação ocorra em duas fases:

i. **Avaliação preliminar**: O **GPD** faz uma avaliação preliminar do incidente, tendo em consideração que esta deverá ser concluída em **48h** e que deverá assumir o pior cenário possível;
ii. **Avaliação detalhada**: A **ERI** complementa a avaliação preliminar com informação suficiente que permita concluir a avaliação prevista, de acordo com as regras definidas no presente capítulo.

Para avaliação da gravidade da violação de dados, o **GDP** deverá utilizar o **modelo de avaliação de violações de dados pessoais,** "**Avaliar risco: Avaliação da Severidade de Violações de Dados**", elaborado de acordo com a matriz da ENISA[2], com a colaboração da restante **Equipa de Resposta a Incidentes**.

Para fazer esta avaliação da severidade da violação de dados, o **GDP** deverá utilizar a seguinte metodologia no preenchimento do formulário indicado:

I) Critérios

Na avaliação da gravidade da violação de dados pessoais deverão ser considerados os seguintes critérios, como referência:

- Contexto do tratamento de dados (**DPC** – *Data Processing Context*): tipo de violação de dados pessoais e natureza de dados pessoais e tratamentos envolvidos;
- Facilidade na identificação (**EI** – *Ease of Identification*): grau de facilidade da identificação do titular de dados pessoais face aos dados envolvidos na violação;

[2] Disponível em: https://www.enisa.europa.eu/publications/dbn-severity

- Circunstâncias da violação (**CB** – *Circumstances of Breach*): circunstâncias relacionadas com o tipo de violação de dados pessoais, incluindo, entre outros, a intencionalidade da violação de dados pessoais.

II) Pontuação dos critérios

A pontuação dos critérios indicados, **DPC**, **EI** e **CB**, deverá ser feita de acordo com os seguintes passos:

a) Critério DPC:

Os dados pessoais envolvidos na violação de dados deverão ser identificados e categorizados num dos seguintes tipos:

- Dados simples: caracterizam um titular de dados pessoais (*por ex.,* dados biográficos, contactos, nome completo, informação familiar, experiência profissional).
- Dados comportamentais: gerados pelo comportamento dos titulares de dados pessoais (*por ex.,* dados de geolocalização, dados de tráfego, dados referentes a preferências ou hábitos).
- Dados financeiros: qualquer tipo de dados financeiros (*por ex.,* renda, transações financeiras, extratos bancários, investimentos, cartões de crédito, faturas).
- Dados de elevada sensibilidade: incluem os dados pertencentes às categorias especiais de dados pessoais, os dados pessoais relacionados com condenações penais e infrações, e os dados de menores.

A existência de fatores que possam aumentar ou diminuir a criticidade associada à categoria de dados pessoais deverá ser avaliada.

Se os dados associados ao incidente de violação de dados pessoais corresponderem a mais do que uma categoria, deverá ser considerada aquela que tiver o valor mais alto.[3]

a) Critério EI:

[3] **Por exemplo:** se for divulgada inadvertidamente uma lista de nomes e moradas de utentes oncológicos de um Hospital, estarão em causa dados simples e dados de elevada sensibilidade. Neste caso, deve prevalecer para a determinação do critério DPC a categoria de dados de elevada sensibilidade, que tem um valor mais alto de criticidade associado.

A atribuição de um valor ao critério **EI** depende da facilidade de identificação dos titulares face aos dados pessoais afetados pela violação, em que:

- Dados associados diretamente a um titular, identificando-o **–** deve ser atribuído ao critério **EI** o valor de **1**;
- Vários tipos de dados que, se combinados, tornam o titular mais fácil de identificar (por ex., a conjugação da morada, data de nascimento e sexo do titular) – deve ser atribuído ao critério **EI** o valor de **0,75**;
- Dados pessoais suficientemente genéricos para tornar difícil a identificação do titular, por pertencerem a muitos indivíduos – deve ser atribuído ao critério **EI** o valor de **0,5**;
- Muito pouca informação associada ao titular, tornando a identificação do titular de dados pessoais bastante improvável – deve ser atribuído ao critério **EI** o valor de **0,25**.

Nota: Este critério está dependente do contexto da violação de dados pessoais e não depende do facto da informação estar cifrada, ou não, podendo este ser um complemento à gravidade da violação.

b) Critério CB:

O critério **CB** terá um valor dependente da circunstância em que ocorreu a violação de dados pessoais, incluindo as propriedades (confidencialidade, integridade e disponibilidade) de segurança da informação que foram violadas e a intencionalidade da violação (acidental ou propositada/maliciosa):

- Perda de confidencialidade: a extensão da perda de confidencialidade varia de acordo com o (potencial) número de terceiros que possam aceder a dados pessoais de forma não autorizada.
- Perda de integridade: a gravidade varia consoante as (potenciais) consequências que a alteração de dados pessoais possa causar aos respetivos titulares.
- Perda de disponibilidade: a gravidade varia consoante o tempo durante o qual os dados pessoais estão indisponíveis, e como consequência máxima, caso a perda seja permanente.
- Intencionalidade maliciosa: pretende medir se a violação foi praticada intencionalmente (desejada) e com o propósito de causar dano aos titulares (e/ou à Instituição) ou se ocorreu acidentalmente (não foi prevista nem provocada).

Nota: contrariamente aos outros critérios, no qual se aplica o valor máximo de entre várias possibilidades, o critério **CB** é cumulativo nas várias circunstâncias da mesma violação.

III) Cálculo da gravidade

A **gravidade** (SE – *Severity*) será calculada relacionando os critérios da seguinte forma:

SE = DPC × EI + CB

DPC *(Contexto do tratamento de dados)*	Avalia a criticidade dos dados pessoais e respetivo contexto de tratamento.
EI *(Facilidade na identificação)*	Atenua o **DPC** com base na facilidade com que se identificam titulares de dados pessoais (por ex., se os titulares dos dados estiverem identificados, então a criticidade será máxima; se não existirem dados que permitam a identificação dos titulares, então a criticidade será mínima).
CB *(Circunstâncias da violação)*	Quantifica as circunstâncias específicas associadas à violação.

O resultado do cálculo da gravidade da violação de dados pessoais deve interpretar-se da seguinte forma:

SE < 2 gravidade **baixa**	Violações de dados que não afetam os titulares de dados pessoais, ou que apenas representem algum constrangimento para os mesmos, passíveis de resolução sem dificuldade (*por ex.,* os dados alvos de violação são passíveis de serem encontrados facilmente na Internet).
2 ≤ SE < 3 gravidade **média**	Violações de dados nas quais os titulares de dados pessoais sofrem maior incómodo para ultrapassar as consequências da violação (*por ex.,* alguns custos financeiros, situações de *stress* ou medo, usurpação de contas associado a serviços de menor sensibilidade).

3 ≤ SE < 4 gravidade **alta**	Violações de dados com consequência graves, que os titulares de dados pessoais ultrapassam com sérias dificuldades (*por ex.,* apropriação indevida de fundos, dano patrimonial, perda de emprego, intimação, usurpação de contas de áreas como a saúde ou serviços financeiros).
4 ≤ SE gravidade **crítica**	Violações de dados com consequências graves e irreversíveis para os titulares de dados pessoais (*por ex.,* dívida substancial, inabilidade de encontrar emprego, danos psicológicos ou físicos de longa duração, morte).

IV) Complementos

- Primeiro complemento: **risco associado ao processo e/ou finalidades** associadas aos dados pessoais envolvidos na violação de dados pessoais. Este complemento poderá ser útil numa fase preliminar da avaliação da gravidade, podendo ajudar no processo de decisão de notificação à CNPD.
- Segundo complemento: **número estimado de titulares de dados pessoais afetados** pela violação. Por exemplo, um número elevado de titulares de dados pessoais afetados poderá incrementar a facilidade com que terceiros acedem aos dados pessoais envolvidos na violação.
- Terceiro complemento: a considerar se a **informação está protegida**. Se a avaliação da violação indicar que tem gravidade máxima, mas os dados pessoais se encontrarem cifrados, então o impacto que a violação possa ter para os titulares de dados pessoais afetados poderá diminuir substancialmente (neste caso, apesar de os dados cifrados representarem segurança para os titulares dados pessoais, também representam um potencial risco da tecnologia usada para cifrar os dados se tornar obsoleta ou haver um comprometimento das chaves criptográficas utilizadas);
- O valor da gravidade (SE) poderá ser complementado com outra informação associada à violação de dados pessoais. Ainda que possa não ter impacto na pontuação final, o **SE** deve ser considerado na avaliação final.

V) Considerações Finais

- A avaliação de uma violação de dados pessoais deve ser suportada por evidências (*por ex.,* relatório de análise forense).
- A recolha de evidências para suportar a avaliação da violação de dados pessoais é da responsabilidade do **GPD** e da **ERI.**
- Os critérios de classificação de violações de dados pessoais são revistos anualmente pelo **GDP** e ajustados na medida do necessário.
- Após documentar as medidas de segurança e mitigação em resposta à violação dos dados, considerando adicionalmente os complementos da secção anterior, o **Conselho de Administração** sob proposta da **ERI,** deve considerar a sua eficácia na redução da probabilidade dos impactos se materializarem, de acordo com a **Tabela 1.**

Tabela 1 – Impacto das medidas adotadas

Redução Máxima	A lista de medidas de mitigação é suficiente para evitar os riscos associados à violação de dados.
Alta Redução	Há uma elevada redução, mas alguns titulares poderão ainda estar afetados.
Média Redução	A probabilidade é reduzida face às medidas aplicadas.
Baixa Redução	Pouco ou nenhum benefício nas medidas aplicadas.

- Considerando todas as medidas de resolução em vigor, analisar em que medida é reduzida a probabilidade dos impactos se materializarem, de acordo com a seguinte matriz de risco:

Tabela 2 – Probabilidade de resolução face às medidas adotadas

		Probabilidade – considerando medidas de resolução			
		Redução Máxima	Alta Redução	Média Redução	Baixa Redução
Gravidade	Baixa	Sem risco	Sem risco	Risco	Risco
	Média	Sem risco	Risco	Risco	Risco elevado
	Alta	Risco	Risco	Risco	Risco elevado
	Muito Alta	Risco	Risco elevado	Risco elevado	Risco elevado

FASE IV e FASE V - NOTIFICAÇÃO E COMUNICAÇÃO

O EPD deverá emitir parecer quanto à necessidade de proceder à notificação:

- À CNPD
- Aos titulares de dados afetados

O parecer do **EPD** deve ser comunicado ao **Conselho de Administração**, que **decidir**á pela realização, ou não, das notificações em questão.

Caberá ainda ao **Conselho de Administração**, a decisão sobre a notificação da violação de dados pessoais às seguintes entidades, com o apoio dos Serviços internos competentes:

- Ao Ministério Público ou às autoridades policiais;
- Ao Centro Nacional de Cibersegurança (CNCS)[4];
- À SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E.[5];
- A outras entidades, como seguradoras, em caso de necessidade.

I) Notificação à CNPD

Confirmando-se a violação de dados pessoais e decidindo o **Conselho de Administração** realizar a notificação à **CNPD**, porque resulta num risco para os direitos e liberdades dos titulares dos dados, a mesma deverá ser realizada num **prazo de 72 horas**, incluindo, pelo menos:

- Uma descrição da natureza da violação de dados pessoais, incluindo sempre que possível, as categorias e número aproximado de titulares de dados afetados e as categorias e número aproximado de registos de dados pessoais afetados;
- A identificação e detalhes de contacto do representante do **RT** e do **EPD**;
- Uma descrição das possíveis consequências da violação de dados pessoais;
- Uma descrição das medidas tomadas ou propostas pelo **RT** para suster a violação de dados pessoais, incluindo, se aplicável, as medidas tomadas para mitigar possíveis efeitos negativos.

[4] Nos termos do DL 65/2021, de 30/07.
[5] Nos termos do Despacho 1348/2017 SES, publicado em DR – II série, n.º 28, e CI n.º 1 SPMS de 15/02/2017.

O risco deverá estar associado à avaliação da gravidade da violação de dados pessoais, sendo recomendável notificar a CNPD sempre que esta seja **de grau médio** ou **superior** (**SE > 2**).

A notificação à **CNPD** é feita através da submissão de um formulário eletrónico acessível na respetiva página, em https://www.cnpd.pt/organizacoes/obrigacoes/violacao-de-dados-ou-data-breach/.

Não sendo possível fornecer todas as informações ao mesmo tempo, poderão ser fornecidas de forma faseada, desde que sem demora injustificada.

Se, após a notificação à CNPD, se concluir que não existe risco para os titulares de dados pessoais, poderá solicitar-se à CNPD que considere sem efeito a notificação inicialmente feita, indicando os respetivos motivos justificativos.

Após a resolução do problema, o **RT**, através do **EPD**, deverá informar a **CNPD** sobre as medidas corretivas adotadas.

II) Comunicação ao Titular dos Dados

Decidindo o **Conselho de Administração** que deve realizar a notificação, esta deverá ser comunicada, **sem demora injustificada,** ao(s) titular(es) dos dados, sempre que a violação de dados resultar num **risco elevado** para os seus direitos e liberdades.

- Fatores a considerar na decisão de comunicar aos titulares afetados:
  - As obrigações legais;
  - Que riscos comporta para os direitos e liberdades das pessoas (*por ex., comprometimento da sua identidade ou dados de identificação, causando danos físicos, materiais, de reputação ou outros*);
  - Até que ponto os danos produzidos são irreversíveis e os possíveis prejuízos futuros podem ser evitados ou mitigados;
  - O risco deverá estar associado à avaliação da gravidade da violação de dados pessoais, devendo os titulares ser notificados sempre que esta seja de grau médio ou superior (**SE ≥ 3**).

- A comunicação aos titulares afetados não será necessária quando:
  - Tiverem sido aplicadas medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pelo incidente, especialmente medidas

que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem;

- Tiverem sido tomadas medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados pessoais já não é suscetível de se concretizar; ou
- Implicar um esforço desproporcionado. Caso em que será feita uma comunicação pública ou tomada uma medida semelhante, através da qual os titulares dos dados pessoais são informados de forma igualmente eficaz.

- A informação a comunicar aos titulares de dados pessoais deverá incluir:
  - O nome e o contacto do EPD ou o ponto de contacto da ULSSM com quem poderão ser obtidas mais informações;
  - A descrição da violação de dados pessoais, incluindo que tipos de dados pessoais foram comprometidos e como foram comprometidos;
  - Quais os serviços disponibilizados pela ULSSM, se existirem, para que o titular de dados pessoais possa mitigar os efeitos adversos da violação, e/ou os passos que os titulares de dados pessoais devem considerar tomar para reduzir o risco associado à violação (*por ex., alterar a password de um determinado serviço*).

- Poderá, ainda, ser útil comunicar:
  - Quais os dados pessoais que foram comprometidos (*por ex., no caso de uma morada, indicar qual é a que foi comprometida*);
  - Os possíveis impactos e consequências para os titulares;
  - As medidas de mitigação já planeadas e/ou implementadas pela ULSSM;
  - As medidas preventivas para mitigar futuras violações de dados pessoais.

FASE VI – RESOLUÇÃO DO INCIDENTE

A **ERI,** com o apoio do **EPD,** deverá garantir a implementação de um plano de ação corretivo, evitando ocorrências futuras.

O **GPD** é responsável por manter um registo de evidências das ações corretivas implementadas (*por ex., as notificações à CNPD e aos titulares, relatório de testes que confirmem que a vulnerabilidade que deu origem à violação de dados pessoais foi corrigida, resultados de auditorias, etc.*).

FASE VII – REGISTO DOS INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

A **ULSSM** conserva um **registo interno** contendo toda a documentação das violações de dados ocorridas, nos termos do artigo 33º/5 do RGPD, com todos os factos relacionados com as violações, os respetivos efeitos e a medidas de reparação adotadas, de forma a permitir à autoridade de controlo verificar o cumprimento daquela obrigação legal.

Cada violação de dados pessoais deve ser numerada, de forma sequencial e única, para efeitos de inventário e gestão de documentação.

O registo interno será mantido, sob a responsabilidade do **GPD,** na **plataforma Her+**, na qual serão anexados os formulários "**Formulário CNPD**" e "**Avaliação da Severidade de Violações de Dados**", e toda a documentação de suporte que tenha sido produzida no decorrer na análise e resolução, incluindo o(s) parecer(es) do EPD.

Este arquivo de registos de violação de dados pessoais é informação confidencial da **ULSSM** e a sua divulgação a terceiros só é permitida mediante aprovação explícita do **Conselho de Administração**, exceto se a **CNPD** o solicitar. A retenção dos registos de violações de dados pessoais, e respetivas evidências, deverá ser acordada com a **CNPD**.

5 AVALIAÇÃO E PLANO DE AÇÃO

O **GDP**, assim que os passos acima indicados tiverem sido concluídos, contida a violação de dados e notificadas todas as partes interessadas, efetuará uma análise completa das causas da violação de dados, da eficácia das medidas tomadas em resposta e da necessidade de adoção de medidas adicionais, para evitar a repetição de situações semelhantes, considerando, nomeadamente:

- Onde são conservados e como são armazenados os dados;

- Quais as medidas de segurança técnicas e organizativas adotdas para proteger os dados e os riscos e possíveis fragilidades dessas medidas;
- Os métodos de transmissão de dados, tanto físicos como digitais e se tais métodos são ou não seguros;
- O nível de partilha de dados existente e se esse nível é ou não necessário;
- Se é necessário realizar ou atualizar quaisquer avaliações do impacto sobre a proteção de dados;
- A sensibilização e formação do pessoal em matéria de proteção de dados.

O **EPD** emitirá um parecer sobre o relatório realizado.

6 DIVULGAÇÃO E SENSIBILIZAÇÃO

Após aprovação pelo Conselho de Administração, este procedimento será divulgado a **todos os colaboradores da Unidade Local de Saúde Santa Maria (ULSSM)** através de **Infomail** e ficará acessível na página da **Intranet** em ***Proteção de Dados/Violação de dados pessoais***.

7 EXEMPLOS DE VIOLAÇÃO DE DADOS PESSOAIS

Evento	Confidencialidade	Disponibilidade	Integridade
Divulgação verbal de dados pessoais	x		
Papel perdido ou subtraído ou deixado em local inseguro	x	x	
Correio perdido ou aberto	x	x	
Eliminação incorreta de dados pessoais em papel		x	
Dados pessoais enviados por engano (postal ou eletrónico)	x		
Dados pessoais apagados/destruídos		x	
Abuso dos privilégios de acesso pelo utilizador (por exemplo, colaborador)para extrair, reenviar ou copiar dados pessoais	x		
Lixo digital (e-Waste), dados pessoais ainda presentes em dispositivos obsoletos	x		
Publicação não intencional	x		
Envio de correio eletrónico a múltiplos destinatários sem cópia cega ou numa lista de distribuição visível	x		
Dispositivo perdido ou roubado	x	x	
Incidente cibernético: Dispositivo encriptado / *Ransomware*	x	x	

Incidente cibernético: *Phishing* / compromisso de conta de utilizador ou administrador	x	x	x
Incidente cibernético: Acesso não autorizado a dados pessoais num sistema de informação, quer corporativo quer de um serviço de Internet	x	x	x
Incidente técnico com corrupção de dados		x	x
Modificação de dados não autorizada			x
Dados pessoais apresentados ao indivíduo errado	x		
Circunstâncias imprevistas, tais como incêndio ou inundação		x	x

8 REVISÃO

Esta política deve ser revista sempre que ocorrer alguma das seguintes situações:

- A adoção da política evidenciar erros ou omissões no respetivo conteúdo.
- Quando outra política, estratégia ou orientação emitida pela ULSSM entrar em conflito com a informação constante desta política.
- Quando o enquadramento estratégico da ULSSM evoluir ou se alterar carecendo o mesmo de revisão.
- Decorridos três anos após aprovação da atual versão.

A. GLOSSÁRIO

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." (Cfr. Art. 4.º RGPD)
Dados especiais	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.
Tratamento de dados	"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." (Cfr. Art. 4.º RGPD)
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». (Cfr. Art. 4.º RGPD)
Incidente de segurança da informação	Um ou vários eventos inesperados e indesejáveis com significante probabilidade de comprometer as operações de negócios e ameaçar a segurança da informação, percebida como a preservação da confidencialidade, integridade ou disponibilidade da informação (Norma ISO/IEC 27000:2016).
Destruição de dados pessoais	Quando os dados deixam de existir ou deixam de existir num formato que seja de alguma utilidade para o Responsável pelo tratamento.
Dados pessoais danificados	Dados pessoais que foram alterados, corrompidos ou já não estão completos.
Perda de dados pessoais	Dados pessoais que podem ainda existir, mas o Responsável pelo tratamento perdeu o controlo ou o acesso a eles, ou já não os tem em sua posse.
Responsável pelo tratamento de dados	"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." (Cfr. Art. 4.º RGPD).
Equipa de resposta a incidentes	**Equipa de Resposta a Incidentes** convocada ao abrigo do presente procedimento para efeitos da análise e resposta de um incidente de segurança passível de configurar uma violação de dados pessoais.

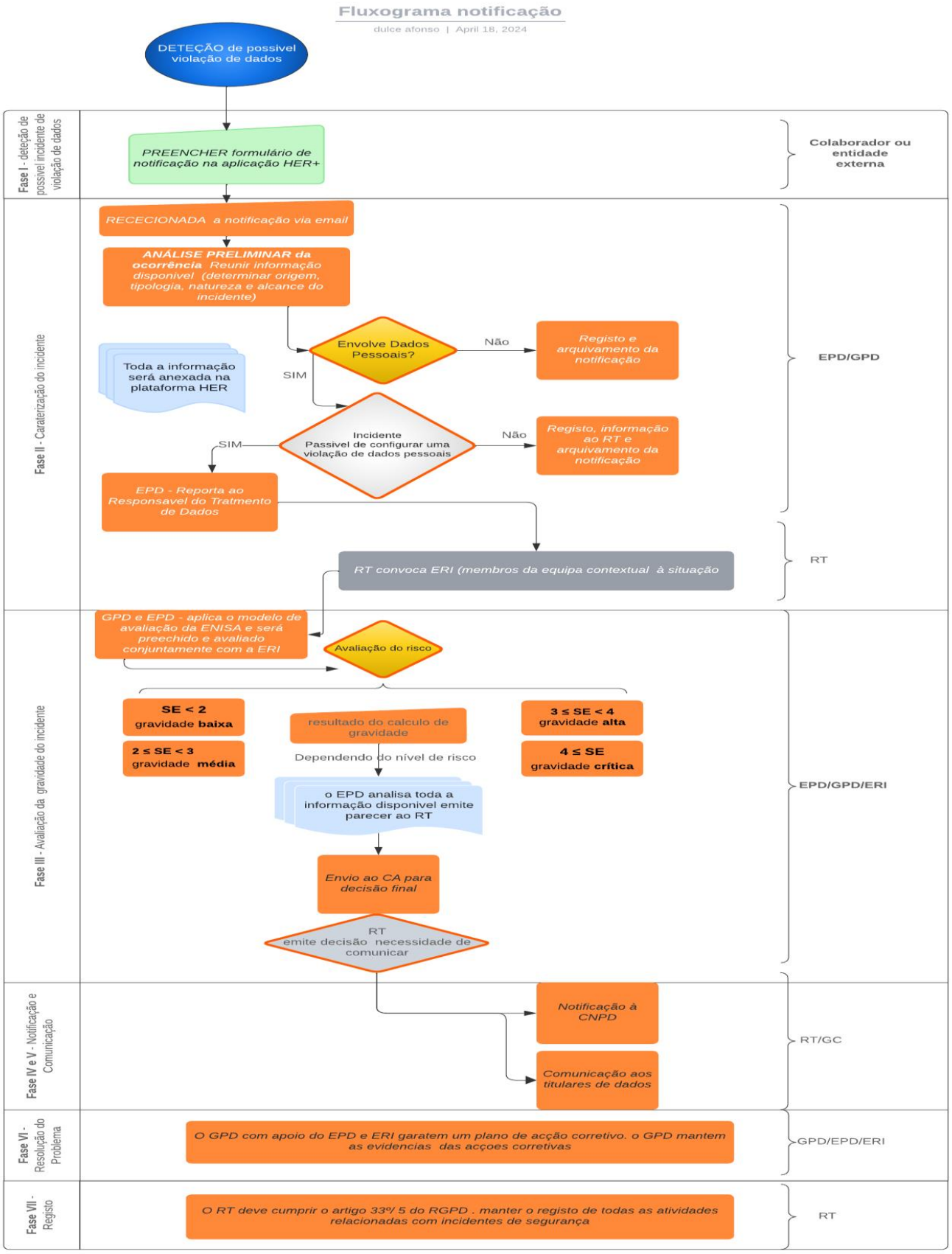
B. ANEXOS

Anexo I – Fluxo do Circuito de Notificação de Incidentes

Anexo II - Matriz de Ações e Responsabilidades (RACI)

Anexo III - Formulário de registo de incidente (HER+)

ANEXO I – Fluxo do Circuito de Notificação de Incidentes



ANEXO II – Matriz de Ações e Responsabilidades (RACI)

AÇÕES	RESPONSÁVEIS								
	Colaborador/notificador	CA	EPD	GPD	ERI			Serviço(s) envolvido(s)	Outros Serviços[6]
					SSI	GJ	GC		
Registar o Incidente HER+	R								
Preencher formulário (aplicação HER+)	R								
Fazer a avaliação prévia do Incidente			C	R					
Reportar ao CA a tipologia do incidente			C	R					
Convocar equipa de resposta ERI		A/R	C						
Caracterizar incidente e Avaliar risco com base na gravidade e probabilidade do dano, com base no formulário "avaliar risco" e outras informações disponíveis		A	C	R	R	R	R	R	R
Definir medidas de contenção e mitigação do risco		A	C	R	R	R	R	R	R
Notificar a CNPD		A/R	C						
Notificar os titulares de dados		A/R	C					R	
Comunicar interna e externa mente		A	C				R	R	
Documentar incidente		A	C	R					

Legenda

(R) – Responsável (quem é o responsável por executar a tarefa)
(A) – Autoridade (quem tem autoridade para tomar a decisão)
(C) – Consultado (quem deve ser consultado para participar na atividade)
(I) – Informado (quem deve receber informações sobre as atividades)
(CA) – Conselho de Administração (Responsável tratamento)
(EPD) – Encarregado de Proteção de Dados
(SSI) – Serviço de Sistemas de Informação
(GJ) - Gabinete Jurídico
(GC) – Gabinete de Comunicação

[6] Sempre que se justificar na sua área de intervenção, serão chamados a integrar a equipa de resposta a incidentes.

Anexo III - Formulário de registo de incidente (HER+)

Dados do Incidente	
Data do incidente	
Declarante	
Local de Deteção	
Descrição **Dados do Notificante**	
Nº mec	
Serviço	
contatoTelefone:	
Contacto eletrónico:	
Tipo de Comunicação	
☐ inicial	
☐ Complementar	
Informação Geral do Incidente	
Quando tomou conhecimento	
Local/serviço da ocorrência	
Tipo de tratamento	Físico ☐ Eletrónico ☐
Envolvidos dados pessoais no incidente	☐ Sim ☐ Não

Breve descrição do incidente

Descrever a natureza do incidente de violação 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.*

contexto do Incidente Sobre os Dados Pessoais

Tipo de Dados Pessoais		
1 Dados Simples		
☐ Dados básicos de identificação *(Ex.: nome, sobrenome, data de nascimento, morada, matrícula)*	☐ Número de documento de identificação oficial.	☐ Dados de contato. (*Ex.: telefone, endereço, e-mail*)
☐ Documentos de identificação oficial. *(Ex.: CC, BI, Passaporte)*	☐ Outros. (descrever)	
2 Dados comportamentais e profissionais		
☒ Dado de geolocalização. *(Ex.: coordenadas geográficas)*	☐ Dados de preferências e hábitos pessoais	☐ Dados protegidos por sigilo profissional/legal.
☐ Dados relativos a atividade formativa	☐ Dados de autenticação de sistema. (*Ex.: senhas, PIN ou tokens)*	☐ Dados Profissionais ☐ Outros. *(descrever)*
3 Dados financeiros		
☒ Dados de meios de pagamento. *(Ex.: cartão de crédito/débito)*	☐ Dados financeiros ou económicos.	☐ Dados de faturação ☐ Outros. *(descrever)*
4 Dados Sensiveis		
☐Origem racial ou étnica. ☐Referente à saúde. ☐Referente à vida sexual.	☐Convicção religiosa. ☐Biométricos. ☐Filiação a organização sindical, religiosa, filosófica ou política.	☐Opinião política. ☐Genéticos.
☐Imagens/Áudio /Vídeo		☐ Outros. *(descrever)*

Circustâncias do incidente	
De que forma o incidente afetou os dados pessoais:	
☐ Confidencialidade quando existe uma divulgação ou acesso acidental ou não autorizado a dados pessoais	**Houve acesso não autorizado aos dados, violando seu sigilo.**
☐ Integridade quando existe uma alteração acidental ou não autorizada dos dados pessoais	**Houve alteração ou destruição de dados de maneira não autorizada ou acidental.**
☐ Disponibilidade quando existe uma perda de acesso ou a destruição acidental ou não autorizada de dados pessoais	**Houve perda ou dificuldade de acesso aos dados por período significativo**.
☐ Intenção maliciosa	

Circunstâncias do Incidente – Qual o tipo de incidente (em função da quebra de Confidencialidade, Disponibilidade e Integridade)

☐ Divulgação verbal de dados pessoais (C)	☐ Papel perdido ou roubado ou deixado em local inseguro (C) (D)
☐ Correio perdido ou aberto (C) (D)	☐ Eliminação incorreta de dados pessoais em papel (D)
☐ Dados pessoais enviado por engano (postal ou eletrónico) (C)	☐ Dados pessoais apagados/destruídos (D)
☐ Abuso de privilégios de acesso pelo membro (exemplo: empregado) para extrair, reenviar ou copiar dados pessoais (C)	☐ e-*Waste*, dados pessoais ainda presentes em dispositivos obsoletos (C)
☐ Publicação não intencional (C)	☐ Envio de correio eletrónico a múltiplos destinatários sem cópia cega ou numa lista de distribuição visível (C)
☐ Dispositivo perdido ou roubado (C) (D)	☐ Incidente cibernético: Dispositivo encriptado / *Ransomware* (C) (D)
☐ Incidente cibernético: *Phishing*/Compromisso de conta de utilizador ou administrador (C) (D) (I)	☐ Incidente cibernético: Acesso não autorizado a dados pessoais num sistema de informação, quer corporativo quer de um serviço de Internet (C) (D) (I)
☐ Incidente técnico com corrupção de dados (D) (I)	☐ Modificação de dados não autorizada (I)
☐ Dados pessoais apresentados ao indivíduo errado (C) (D) (I)	☐ Circunstâncias imprevistas, tais como incêndio ou inundação
☐ Outro tipo de incidente *(descrever)*	

Circunstâncias do Incidente - Explique, resumidamente, a causa do incidente (identifique a causa raiz, se conhecida)

Circunstâncias do Incidente - Que medidas adotou no imediato para corrigir o incidente?

Riscos e Consequências para os Titulares dos Dados

Quais as categorias de titulares que foram afetadas pelo incidente?

☐ Funcionários. (Nº de titulares afetados)	☐ Utentes. (Nº de titulares afetados)	☐ Utentes menores (Nº de titulares afetados)
☐ Cidadãos. (Nº de titulares afetados)	☐ Utentes vulneráveis (Nº de titulares afetados)	☐Prestadores de serviços. (Nº de titulares afetados)
☐ Estudantes/Alunos. (Nº de titulares afetados)	☐Ainda não identificadas. (Nº de titulares afetados)	☐ Outras: _____

Riscos e Consequências para os Titulares dos Dados - Quais as prováveis consequências do incidente para os titulares?

☐ Danos morais.	☐ Danos materiais.	☐ Violação à integridade física

☐ Discriminação social.	☐ Danos reputacionais.	☐ Roubo de identidade.
☐ Engenharia social / Fraudes.	☐ Limitação de acesso a um serviço.	☐ Exposição de dados protegidos por sigilo profissional/legal.
☐ Restrições de direitos.	☐ Perda de acesso a dados pessoais.	☐ Outras: _____

Riscos e Consequências para os Titulares dos Dados - A ocorrência do incidente foi comunicada aos titulares?

☐ Sim, foi comunicado aos titulares dos dados	☐ Não, mas vão ser informados	☐ Não vão ser informados
☐ Outro		

O que é que acontece a seguir?

Pretende ser informado da evolução deste processo?

(Deve ler as nossas orientações para determinar as medidas que deve tomar.)

☐ Sim ☐ Não

Com base nas informações que forneceu, contactá-lo-emos no prazo de sete dias úteis para o informarmos sobre os passos seguintes. Se esta for a sua denúncia inicial, dar-lhe-emos um número de referência do caso que poderá consultar na plataforma HER+.

Se esta notificação estiver relacionada com um processo preexistente, juntá-la-emos a esse processo para que o responsável pelo mesmo a possa analisar.

Se precisar de ajuda ou tiver alguma dúvida para preencher este formulário, descreva-o nos campos do formulário ou contacte-nos através do email **dpo@ulssm.min-saude.pt**.

Para informações sobre o que fazemos com os seus dados pessoais, consulte a nossa declaração de privacidade.