POLÍTICA GERAL DE PROTEÇÃO DE DADOS PESSOAIS

ORPEA Ibérica

Versão: 2.0
Data: maio 2019

INTRODUÇÃO

No Grupo ORPEA Portugal e nas entidades que fazem parte do mesmo (doravante "ORPEA Portugal" ou simplesmente "ORPEA"), estamos empenhados em desenvolver a nossa atividade com o máximo respeito pela privacidade dos nossos funcionários, residentes e pacientes. Este compromisso está refletido no nosso Código de Conduta, cujo segundo princípio estabelece que *"O Grupo ORPEA compromete-se a respeitar rigorosamente os dados pessoais e a legislação vigente sobre proteção de dados"*.

Neste sentido, desde a entrada em vigor do Regulamento Geral de Proteção de Dados (RGPD), foram estabelecidas uma série de obrigações que devem ser cumpridas para nos adaptarmos ao que o novo enquadramento exige de nós.

Uma das principais novidades que o Regulamento inclui é o princípio da responsabilidade proativa (*accountability*). Este princípio exige que apliquemos medidas de segurança técnicas e organizacionais para garantir o cumprimento das normas e proteger os dados pessoais.

Portanto, todos que fazemos parte da ORPEA devemos promover ativamente a cultura de proteção de dados, garantindo que todos conhecemos os nossos direitos e obrigações.

O objetivo desta Política é estabelecer os objetivos de gestão da privacidade, orientar e informar acerca dos vários aspetos que precisamos saber sobre a proteção de dados pessoais na ORPEA.

ÂMBITO DE APLICAÇÃO

As regras e diretrizes contidas e desenvolvidas nesta política são aplicáveis a todo o pessoal, às equipas e aos sistemas relacionados com tratamentos, utilizações ou meios do Grupo ORPEA Portugal que contenham dados pessoais.

Estão particularmente vinculados a esta política:

a. todos os funcionários ou pessoas que ajam em nome e em representação da ORPEA que se encontrem envolvidos em qualquer operação ou conjunto de operações realizadas em dados pessoais ou conjuntos de dados pessoais, seja através de procedimentos automatizados ou não, envolvendo recolha, registo, organização, estruturação, conservação, adaptação ou alteração, extração, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de autorização de acesso, recolha ou interligação, limitação, supressão ou destruição de dados pessoais.

b. todos os recursos dos sistemas de informação através dos quais se pode aceder aos ficheiros, tratamentos ou utilizações que contêm dados pessoais, bem como todos os dispositivos que realizam qualquer processo de tratamento ou armazenamento de dados pessoais.

Qualquer violação desta política pode expor a ORPEA, os seus funcionários e/ou terceiros que ajam em seu nome a importantes sanções administrativas, criminais e/ou disciplinares.

DEFINIÇÕES

Dado pessoal:	Um dado pessoal é qualquer informação que identifique ou torne um indivíduo identificável.
Dado de saúde:	Os dados de saúde ou "dados sanitários" são todos os dados relativos ao estado de saúde física ou mental, presente, passada ou futura, de um indivíduo. Alguns exemplos são: 1) dados de doença. 2) dados de incapacidade. 3) a história clínica 4) qualquer relatório médico. 5) os tratamentos médicos. 6) o estado fisiológico ou biomédico da pessoa. 7) o risco de sofrer de doenças. 8) qualquer número, símbolo ou dado atribuído a um indivíduo que o identifique, inequivocamente, para efeitos sobre a saúde.
Afetado/interessado	É o indivíduo titular dos dados que são objeto de tratamento.
Tratamento:	Um tratamento é qualquer operação ou conjunto de operações realizadas em dados pessoais, por exemplo: a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a extração, a consulta, o uso, a comunicação por transmissão, a divulgação ou qualquer outra forma de autorização de acesso, recolha ou interligação, limitação, supressão ou destruição. Através de nossa própria atividade, a ORPEA trata "*dados pessoais de saúde*" que, de acordo com a regulamentação atual, são especialmente protegidos.

PRINCÍPIOS DE TRATAMENTO NA ORPEA

Na ORPEA seguimos uma política de **transparência, lealdade e legalidade dos dados:**

a. **Legalidade**: Trataremos apenas dados pessoais para finalidades específicas, explícitas e legítimas, protegidos por algumas das bases legais permitidas pela legislação e sem poderem ser tratados posteriormente de forma incompatível com os referidos fins.

b. **Transparência**: Só processaremos os dados pessoais se as partes interessadas foram informadas. Esta informação deverá cobrir o propósito do tratamento, a sua base legal e a possibilidade de exercer os seus direitos.

c. **Minimização de dados e proporcionalidade**: Temos que assegurar-nos que só tratamos os dados pessoais necessários, adequados e pertinentes e não excessivos para o objetivo do tratamento.

d. **Precisão**: os dados pessoais devem ser precisos e mantidos completos e atualizados de modo a permitir o cumprimento das finalidades para as quais foram recolhidos.

e. **Retenção e eliminação**: Manteremos os dados pessoais apenas pelo tempo necessário em relação aos propósitos do tratamento. Os dados pessoais que já não forem necessários, após os prazos legais ou estabelecidos para o tratamento, serão eliminados.

f. **Confidencialidade e segurança de dados**: Somos obrigados a aplicar as regras estabelecidas para proteger os dados pessoais que tratamos, tanto do ponto de vista da segurança técnica quanto da segurança da organização. Assim, aplica-se o princípio de "necessidade de saber" de modo que somente podemos aceder às informações pessoais que forem necessárias para o desempenho adequado das nossas funções, sendo proibido usar dados pessoais para fins particulares ou comerciais, para os divulgar ou disponibilizar a terceiros de qualquer outra forma. Esta obrigação permanecerá em vigor mesmo após o término da nossa relação profissional.

DATA PROTECTION OFFICER (DPO)

A ORPEA nomeou um *Data Protection Officer* a nível de Grupo em conformidade com o art. 37 do Regulamento Europeu de Proteção de Dados.

A fim de garantir que as partes interessadas (tanto dentro como fora da organização) e as autoridades de supervisão possam entrar facilmente em contacto com o DPO, de forma direta e confidencial, em conformidade com o Artigo 37 do RGPD, a ORPEA comunicou os dados de contacto do DPO às autoridades supervisoras correspondentes e publica a identidade e os dados de contacto do DPO:

Nome:	Alma Benzaïd.	**Telefone:**	+ 33 1 47 75 60 22.
***E-mail*:**	DPO-pt@orpea.net	**Morada:**	12 rue Jean Jaurès, 92 813 Puteaux Cedex, Paris, França.

MEDIDAS DE PROTEÇÃO DE DADOS PESSOAIS

Na ORPEA adotámos uma série de medidas técnicas e organizacionais para salvaguardar a confidencialidade e segurança da informação que tratamos. Estas medidas são:

A) Medidas de segurança informática

O Departamento de IT estabeleceu uma série de regras para garantir a segurança dos sistemas e meios informáticos da Orpea que todos deverão cumprir. Algumas delas são:

- É estritamente proibida a utilização de memórias ou discos externos (USB) sem autorização prévia.
- Exige-se a observância das licenças de *software* e está proibida a utilização de *software* não autorizado.
- O *software* antivírus é executado com uma frequência definida para verificar se os computadores e os meios apresentam algum dos vírus conhecidos.
- O *software* e o conteúdo dos dados dos sistemas são revistos regularmente e verifica-se a existência de ficheiros falsos ou alterações não autorizadas.
- Todos os meios removíveis (discos, CDs, cartões de memória, etc.) devem ser testados antes de serem usados.
- O suporte de IT deve ser informado imediatamente de qualquer ataque de vírus.
- Anexos e *hiperlinks*, de qualquer natureza, de um correio eletrónico devem ser sempre tratados como suspeitos.
- O correio deve ser eliminado sem abrir os anexos ou o *link*, sempre que um correio eletrónico chegue da parte de alguém desconhecido.
- Deve contactar-se o remetente de um correio eletrónico para confirmar o conteúdo dos anexos/*links* antes de o abrir, no caso de se tratar de um contacto profissional que normalmente não envia anexos/*links* ou de quem não se esperavam dados em anexo/*links*.

B) Medidas de segurança dos dados pessoais em suporte de papel

- Os processos e as pastas devem ser arquivados e organizados de forma a garantir a sua correta conservação, localização e consulta;

- Devem ser arquivados em elementos ou dispositivos (armários, arquivadores, etc.) com mecanismos que impeçam a sua abertura.
- Quando não estiverem arquivados nos elementos acima mencionados, a pessoa responsável protegerá e impedirá sempre o acesso não autorizado.

Na ORPEA seguimos uma Política de "*Clean Screen & Desks*" (Ecrãs e Secretárias Limpas); de forma que:

- Cada vez que abandonamos o computador, devemos bloquear o ecrã (pressionando Ctr + l).
- No final do dia, todos os documentos e processos devem ser devidamente arquivados ou mantidos à chave para evitar a sua perda ou roubo.

C) Funções do DPO

- Controlar o cumprimento do RGPD pela ORPEA.
- Dar apoio à ORPEA para a realização das avaliações de impacto da proteção de dados.
- Considerar devidamente o risco associado às atividades de tratamento, levando em consideração a natureza, o alcance, o contexto e os propósitos do tratamento.
- Manter o registo das operações de tratamento, de responsabilidade da ORPEA, a fim de realizar as funções de controlo do cumprimento, da informação e assessoria.
- Cooperar com a autoridade de controlo.
- Atuar como ponto de contacto da autoridade de controlo para questões relacionadas com o tratamento.

D) Funções e obrigações do pessoal

- Todo o pessoal autorizado a aceder aos sistemas de informação ou ficheiros que contenham dados pessoais, é obrigado a cumprir os regulamentos de segurança incluídos nesta Política e qualquer outra que a ORPEA possa adotar.

DIREITOS RELATIVOS AOS DADOS PESSOAIS

Os funcionários, residentes, pacientes e todas as outras pessoas cujos dados pessoais são processados pela ORPEA podem exercer os seus direitos de acesso, retificação, oposição, exclusão, limitação do tratamento, portabilidade no caso de não serem objeto de decisões individualizadas.

Direito de aceso: A parte interessada tem o direito de solicitar e obter, gratuitamente, as informações sobre os dados pessoais submetidos ao tratamento, à origem desses dados, bem como às comunicações realizadas ou que se preveem fazer a partir deles. Deve-se informar:

a. Do propósito do tratamento dos seus dados
b. Das categorias (básicos, bancários, saúde... etc.)
c. Dos destinatários a quem se vai comunicar.
d. Do prazo da sua conservação.
e. Como solicitar ao responsável o exercício dos direitos.
f. Do direito de apresentar uma reclamação à autoridade de controlo.
g. Qualquer informação sobre a origem dos dados.
h. Transferências internacionais.
i. Dos tratamentos e decisões automatizadas sobre os seus dados.

Direito de retificação: O interessado tem o direito de obter a retificação dos dados pessoais que sejam imprecisos, sem atrasos injustificados.

Direito de oposição: O interessado tem o direito de se opor ao processamento dos seus dados em alguns casos avaliados.

Direito de supressão: O interessado tem o direito à eliminação dos dados pessoais quando ocorrer qualquer das circunstâncias legalmente avaliadas.

Da mesma forma, todas as partes interessadas podem exercer os seus direitos sobre a portabilidade de dados, a limitação do tratamento ou para retirar o consentimento previamente concedido.

Para exercer os seus direitos, a parte interessada deverá enviar um correio eletrónico para protecçaodedados@orpea.net, indicando o direito que pretende exercer e identificando-se inequivocamente através do seu documento de identificação ou documento semelhante, legalmente válido. Em todos os casos, as solicitações realizadas serão arquivadas com a data e cópia da resposta enviada ao interessado.

Se o interessado considera que o tratamento realizado aos seus dados pessoais não se encontra em conformidade com a lei ou que a sua solicitação não foi devidamente aceite, pode apresentar uma reclamação à Comissão Nacional de Proteção de Dados (www.cnpd.pt/) nos termos indicados por esta.

REGISTO E NOTIFICAÇÃO DE INCIDÊNCIA DE SEGURANÇA

Considera-se por incidência qualquer facto ou circunstância que, quando ocorre, gera ou pode gerar qualquer tipo de risco ou dano que afete a segurança, a confidencialidade ou a integridade dos dados pessoais processados pela ORPEA, como, por exemplo, *hacking*, roubo de informação, envio indevido de dados pessoais para terceiros, perda de dados pessoais, etc.

Devemos estar atentos a estas ocorrências e informar acerca delas o mais rápido possível. Qualquer funcionário que tenha conhecimento de qualquer incidente fica direta e pessoalmente responsabilizado de o notificar sem demora ao Departamento de IT através de *ticket* na ferramenta SNOW e ao Departamento de *Compliance* no seguinte endereço: protecçaodedados@orpea.net.

O DPO documentará qualquer violação de segurança de dados, incluindo os factos relacionados com a mesma, os seus efeitos e as medidas de segurança implementadas. A referida documentação permitirá que a autoridade de controlo verifique o cumprimento do disposto no artigo 33 do RGPD.

Em caso de violação de segurança que afete seriamente os direitos e liberdades das partes interessadas, o DPO notificará sem demora a autoridade de controlo competente num prazo máximo de 72 horas. A comunicação aos afetados deve ser clara e simples.

CONTROLOS PERIÓDICOS E AUDITORIA

Serão realizados controlos periódicos para a verificação correta do cumprimento das medidas, normas e procedimentos estabelecidos nesta Política, de tal forma que possam detetar qualquer anomalia que afete a segurança, integridade ou disponibilidade dos dados pessoais contidos nos ficheiros.

As datas de controlos e as medidas a serem auditadas serão aprovadas anualmente pelo Departamento de IT e pelo Departamento de *Compliance*.

FORMAÇÃO E TRANSMISSÃO DA INFORMAÇÃO:

Esta política ou qualquer outra relacionada com a proteção de dados está acessível ao pessoal e será entregue uma cópia da mesma, nas matérias que lhes dizem respeito, a qualquer utilizador que a solicitar.

O pessoal deve ser sensibilizado nesta questão através da informação, de comunicações internas ou formação específica.

O não cumprimento das obrigações relativas à proteção de dados pode ser considerado como uma violação da boa-fé contratual. Se o não cumprimento for de natureza fraudulenta, serão tomadas as ações legais correspondentes para o devido apuramento de responsabilidades.