



Sindicato dos Médicos da Zona Centro

Rua de Tomar, n.º 5 • 3000-401 COIMBRA

Telef.: 239 827737 Fax: 239 837788 Tlm.: 91 3626493 E-Mail: geral@smzc.pt

**POLÍTICA DE PRIVACIDADE
E
REGULAMENTO GERAL DE
PROTECÇÃO DE DADOS**

**SINDICATO DOS MÉDICOS DA ZONA CENTRO
SMZC**



PROTECÇÃO DE DADOS PESSOAIS

ÍNDICE

INTRODUÇÃO.....	3
I. OBJECTIVO E ÂMBITO.....	4
II. REGRAS E PROCEDIMENTOS.....	4
III. DEFINIÇÃO DE DADOS PESSOAIS.....	5
IV. TRATAMENTO DE DADOS PESSOAIS.....	5
V. APAGAR E “CONGELAR” INFORMAÇÃO.....	7
VII. DIREITOS DOS TITULARES DOS DADOS.....	7
VIII. GESTÃO DE DADOS DOS COLABORADORES.....	8
IX. DIVULGAÇÃO E CONTRATUALIZAÇÃO.....	9
X. INFORMAÇÃO E FORMAÇÃO.....	9
XI. DISPONIBILIZAÇÃO DE DADOS PESSOAIS A TERCEIROS.....	9
XII. PRESTADORES EXTERNOS DE SERVIÇOS (SUBCONTRATANTES).....	10
XIII. PROTECÇÃO DE DADOS E MEDIDAS DE SEGURANÇA.....	10
XIV. VIOLAÇÃO DE DADOS.....	11
XV. DÚVIDAS.....	11
XVI. POLÍTICA DE COOKIES.....	12
ANEXO I.....	13



INTRODUÇÃO

- a. A utilização pelo Sindicato da informação disponível no âmbito da sua atividade deverá ter sempre presente as disposições legais em vigor em território Português, nas quais assenta a Política de Proteção de Dados, adiante designada por PPDP.
- b. A PPDP regula a utilização de informação relativa aos dados pessoais no exercício da atividade do Sindicato.
- c. A PPDP não tem um carácter de confidencialidade, mas baseia-se numa lógica “*need to know*” no que respeita à utilização interna e externa de dados pessoais, sempre em consonância com as disposições legais aplicáveis.
- d. É neste contexto que o Sindicato, elaborou a sua Política de Proteção de Dados Pessoais (PPDP) aplicável a todos os que no âmbito da sua atividade, se relacionam com o Sindicato.

OBJECTIVO E ÂMBITO

O objetivo desta Política é o de garantir um determinado nível de proteção de dados pessoais que:

- a. Esteja de acordo com as disposições legais aplicáveis sobre proteção de dados pessoais;
- b. Esteja de acordo com as necessidades dos clientes, parceiros e dos trabalhadores;
- c. Permita realizar os processos de negócio de forma eficaz;
- d. Permita ao Sindicato manter uma imagem externa positiva no mercado.



REGRAS E PROCEDIMENTOS

- a. Todos os colaboradores ou unidades do Sindicato que utilizem dados pessoais são individualmente responsáveis pelo cumprimento das disposições legais e regulamentares aplicáveis.
- b. Os membros da Direção, além de estarem obrigados ao cumprimento das regras e procedimentos relativos à PPDP, têm a incumbência de implementar estruturas e garantir recursos adequados ao bom funcionamento da PPDP.
- c. Os colaboradores têm a obrigação de garantir a confidencialidade dos dados como parte indissociável das suas funções previstas no contrato de trabalho. Deverão também proceder em conformidade com toda a informação e formação recebida, bem como cumprir todas as orientações definidas na PPDP. O não cumprimento destas obrigações pode ter consequências disciplinares, e todas as falhas no âmbito da PPDP devem ser reportadas à Direção.
- d. Consideram-se colaboradores, para efeitos da Política de Proteção de Dados Pessoais, os que tenham com o Sindicato uma relação de trabalho, estágio, prestação de serviço ou outra equiparável.
- e. À Direção incumbe zelar pelo cumprimento da regulamentação de proteção de dados pessoais, através do fornecimento de informação a todos os colaboradores do Sindicato neste domínio.
- f. A Direção será também responsável pela identificação de riscos e proposta de oportunidades de melhoria relacionadas com a PPDP.
- g. A Direção pode, no âmbito das suas funções, determinar a implementação de medidas PPDP em qualquer área do Sindicato,



devendo para este fim, dispor de controlos e acessos adequados.

DEFINIÇÃO DE DADOS PESSOAIS

Consideram-se dados pessoais todas as 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 (E-mail) ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

TRATAMENTO DE DADOS PESSOAIS

- a. Por tratamento de dados pessoais entende-se qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição.
- b. A informação pessoal deverá ser recolhida, processada e utilizada:

Na base de uma relação contratual e confidencial com a pessoa em causa;

Com o consentimento por escrito das pessoas implicadas;

Com o detalhe que é legalmente possível ou requerido.



- c. Todos os procedimentos para tratamento de dados pessoais deverão cumprir os requisitos impostos pelas normas aplicáveis. (Vide Anexo)
- d. Qualquer alteração ao método de recolha e tratamento de dados pessoais deverá ser comunicado à Direção para verificar a sua viabilidade e conformidade com as normas aplicáveis.
- e. A recolha de dados deverá ser efetuada para finalidades determinadas e estar limitada à informação necessária para o processo da finalidade em causa, não podendo incidir, a não ser com o consentimento prévio do titular dos dados, sobre dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária e sindical, fé religiosa, vida privada, origem racial ou étnica, saúde ou vida sexual.
- f. Os dados pessoais recolhidos deverão ser exatos e deverão ser atualizados se necessário, devendo ser tomadas as medidas adequadas para que sejam apagados ou retificados os dados inexatos e incompletos.
- g. Dentro do possível e quando for considerado vantajoso a informação deverá ser anónima e podem ser utilizados pseudónimos.
- h. Em caso de transferência de informação pessoal e/ou dos respetivos suportes deverão ser tomadas medidas especiais de segurança.

APAGAR E “CONGELAR” INFORMAÇÃO

- a. Quando os dados não forem necessários para um determinado propósito, ou quando os fins que motivaram o seu armazenamento tiverem sido cumpridos, a informação deve ser apagada.



- b. No caso de ser necessário reter os dados por um determinado período, a informação deverá ser “congelada”.
- c. Neste último caso, o acesso a informação “congelada” carece de autorização específica da Direção.

I. PROCESSAMENTO DE INFORMAÇÃO PESSOAL POR OUTRA EMPRESA DO GRUPO

O processamento de dados pessoais por outro Sindicato ou empresa apenas será possível mediante autorização das pessoas implicadas.

DIREITOS DOS TITULARES DOS DADOS

- a. O Sindicato deverá estabelecer procedimentos que visam proteger os direitos dos titulares dos dados pessoais no que se refere a:
 - b. Conformidade com o objetivo específico da recolha dos dados, ou seja, os dados pessoais não podem ser utilizados para fins diferentes dos que motivaram a sua recolha, e dos quais o titular dos dados foi devidamente informado;
 - c. Fornecimento da informação ao titular dos dados sobre o armazenamento dos seus dados, sobre o respetivo conteúdo e sobre o seu direito à consulta e correção da informação;
 - d. Retificação, eliminação ou bloqueio de dados, e a sua notificação, caso possível, aos terceiros que hajam tido conhecimento desses dados;
 - e. Oposição, sempre com fundamento em razões ponderosas e legítimas relacionadas com a sua situação particular, ao tratamento dos dados de que seja titular;



- f. Notificação quando a informação é armazenada pela primeira vez por outro método distinto do original;
- g. Não utilização de dados pessoais para fins de publicidade, marketing direto ou qualquer outra forma de prospeção comercial, bem como a sua não comunicação a terceiros para os mesmos fins, salvo com o consentimento prévio do titular dos dados.

GESTÃO DE DADOS DOS COLABORADORES

- a. Os dados pessoais dos colaboradores serão tratados de acordo com a política de proteção de dados pessoais, levando em consideração os direitos e os requisitos operacionais do Sindicato.
- b. Os dados pessoais dos colaboradores são tratados exclusivamente nos termos constantes dos contratos de trabalho.
- c. O tratamento de dados pessoais do colaborador no âmbito de uma relação de laboral tem subjacente o mesmo procedimento de tratamento de dados que um qualquer sócio.
- d. O acesso a esta informação deverá estar regulamentado no Regulamento Interno.

DIVULGAÇÃO E CONTRATUALIZAÇÃO

- a. A PPDP será divulgada e afixada nas instalações do Sindicato.
- b. A obrigação de confidencialidade por parte dos colaboradores do Sindicato, relativamente aos dados pessoais a que tiverem acesso por força das suas funções, deve constar dos contratos de trabalho, mantendo-se em qualquer caso em vigor mesmo após o termo das respetivas funções ao serviço do Sindicato.



INFORMAÇÃO E FORMAÇÃO

Deverá a ser disponibilizada informação e formação adequadas sobre a PPDP a todos os colaboradores do Sindicato.

DISPONIBILIZAÇÃO DE DADOS PESSOAIS A TERCEIROS

- a. Os dados pessoais só podem ser disponibilizados a entidades externas quando tal se encontre especificamente previsto na Lei, ou por consentimento expresso do titular dos dados.
- b. Antes de ser fornecida qualquer informação por telefone deverá ser realizada uma adequada identificação do requerente da informação mediante contraste de dados pessoais específicos.
- c. O requerente deve ser previamente informado de que as informações solicitadas para efeito de contraste configuram uma medida de proteção dos seus próprios dados pessoais.
- d. O fornecimento de dados pessoais a cônjuges ou legalmente equiparados das pessoas cujos dados pessoais são recolhidos seguirá as mesmas regras que a prestação de informação a terceiros.
- e. Em caso de exigência de dados pessoais por auditores ou autoridades externas, o seu fornecimento será limitado ao estritamente necessário para que essas entidades possam executar adequadamente as tarefas e funções que por via da lei ou de contrato lhes estão cometidas.
- f. No caso de dúvida sobre direitos de acesso a informação, a Direção deverá ser consultada.



PRESTADORES EXTERNOS DE SERVIÇOS (SUB-CONTRATANTES)

Os contratos com prestadores externos deverão incluir exigências específicas adequadas em matéria de PPDP.

PROTECÇÃO DE DADOS E MEDIDAS DE SEGURANÇA

- a. Deverão ser implementadas medidas que visem uma adequada política de proteção de dados evitando a sua divulgação indevida, accidental ou intencional.
- b. Os dados deverão ser classificados de acordo com o seu nível de confidencialidade.
- c. O rigor das medidas de proteção deve ser proporcional ao nível de confidencialidade dos dados a proteger.

XIV. VIOLAÇÃO DE DADOS

- a. O Sindicato está obrigado a notificar a entidade de controlo de segurança dos dados pessoais, que na presente data é a Comissão Nacional de Proteção de Dados, de todas as violações de dados com risco para o seu titular.
- b. Esta comunicação tem de ser realizada no prazo de 72h.
- c. A notificação tem que conter a descrição da natureza da violação de dados pessoais, incluindo o número de pessoas em causa, e registos de dados pessoais em questão, o nome e dados de contacto do responsável da proteção de dados, a descrição das consequências prováveis da violação de dados pessoais, e a



descrição das medidas propostas pelo responsável de tratamento de dados, para reparação dos direitos violados.

- d. Quando a violação de dados for suscetível de causar prejuízo ao seu titular, designadamente, quando possa representar um alto risco para os direitos e liberdades, deve o titular ser informado, de forma clara e sem demora.

DÚVIDAS

No caso de dúvida sobre direitos de acesso a informação, sobre exigências específicas a impor a terceiros ou outras que respeitem à PPDP, a Direção deverá ser consultada, e, sempre que for caso disso, recorrerá aos Serviços Jurídicos para obter o enquadramento jurídico das respetivas decisões.

POLÍTICA DE COOKIES

São utilizados cookies para melhorar a experiência do utilizador do site e o desempenho do site. O SMZC utiliza cookies para recolher e guardar informação no âmbito da utilização do site. A cada visitante corresponde um cookie individual, garantindo desta forma a privacidade e a segurança dos dados. A sua utilização limita-se aos seguintes fins:

- Permitir ao SMZC saber qual do fuso horário do visitante e em caso de login de sócio identificá-lo.
- Permitir ao SMZC estimar os níveis de utilização dos serviços que disponibiliza



ANEXO I

Regime jurídico da Proteção de Dados (Principais diplomas)

➤ Proteção de Dados Pessoais

- Artigo 35º da Constituição da República Portuguesa - utilização da informática;
- Lei n.º 67/ 98, de 26 de outubro - Lei da Proteção de Dados Pessoais;
- Lei n.º 43/ 2004, de 18 de agosto - Lei da organização e funcionamento da CNPD Saúde;
- Lei n.º 12/2005, de 26 de janeiro - Informação genética pessoal de saúde.

➤ Comunicações eletrónicas

- Lei n.º 41/2004, de 18 de agosto - Regula a proteção de dados pessoais no sector das Comunicações Eletrónicas;
- Decreto-Lei n.º 7/2004, de 7 de janeiro - transpõe a Diretiva do Comércio Eletrónico e o artigo 13º da Diretiva das Comunicações Eletrónicas;
- Lei n.º 32/2008, de 17 de julho - Regula a conservação de dados no contexto dos serviços de comunicações eletrónicas ou dos serviços públicos de comunicações.

➤ Videovigilância

- Decreto-Lei n.º 35/2004 - utilização de sistemas de videovigilância pelos serviços de segurança privada e de autoproteção;
- Lei n.º 1/2005, de 10 de janeiro - utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum.

➤ Trabalho

- Lei n.º 99/ 2003, de 27 de agosto - aprova o Código do Trabalho;



Sindicato dos Médicos da Zona Centro

Rua de Tomar, n.º 5 • 3000-401 COIMBRA

Telef.: 239 827737 Fax: 239 837788 Tlm.: 91 3626493 E-Mail: geral@smzc.pt

- Lei n.º 35/ 2004, de 29 de julho - regulamenta o Código do Trabalho .

➤ **Criminalidade informática**

- Lei n.º 109/ 91, de 17 de agosto - Lei da criminalidade informática.

REGULAMENTO GERAL DE PROTECÇÃO DE DADOS

Em cumprimento do RGPD (Regulamento Geral de Proteção de Dados), o Sindicato dos Médicos da Zona Centro (SMZC), informa que todos os dados pessoais dos nossos sócios, fornecedores e parceiros, serão processados e armazenados informaticamente. Os dados serão conservados de forma a permitir a identificação dos titulares até que por vontade própria queiram cancelar os seus dados pessoais, o que podem fazer para o Email: rgpd@smzc.pt, aos cuidados do Sr. Dr. Miguel Monteiro. Os dados pessoais serão tratados exclusivamente pelos serviços administrativos do sindicato e serão utilizados na solicitação de qualquer informação ou contato única e exclusivamente no âmbito da relação entre este sindicato e as entidades já mencionadas.

IDENTIFICAÇÃO DO RESPONSÁVEL DE DADOS

Proteção de Dados Pessoais

INFORMAMOS QUE NOS TERMOS DO RGPD, o Responsável de Dados do Sindicato dos Médicos da Zona Centro é:



Sindicato dos Médicos da Zona Centro

Rua de Tomar, n.º 5 • 3000-401 COIMBRA

Telef.: 239 827737 Fax: 239 837788 Tlm.: 91 3626493 E-Mail: geral@smzc.pt

Luís Miguel Torres Monteiro,

Morada: Rua de Tomar, n.º 5-A, 3000-401 COIMBRA

Telefone/Telemóvel: 239 827737

Email: rgpd@smzc.pt

DECLARAÇÃO DO RESPONSÁVEL DE DADOS

Proteção de Dados Pessoais

Luís Miguel Torres Monteiro, na qualidade de Responsável de Dados do Sindicato dos Médicos da Zona Centro declara para os devidos e legais efeitos que a aplicabilidade e o respeito total pelo cumprimento do Regulamento Geral de Proteção de Dados em vigor, obrigando-se a executar as medidas técnicas e/ou organizativas adequadas, à salvaguarda dos direitos dos titulares de dados.

Mais se obriga a:

- a) Proceder ao tratamento dos dados pessoais, segundo as diretrizes do Regulamento, designadamente em tudo o que respeite à transferência de dados para outros países salvo disposição de direito comunitário a que se encontre sujeito, exceto se a informação for proibida por motivos legítimos de interesse público.
- b) Certificar que o tratamento dos dados pessoais está a ser efetuado com a devida autorização, por pessoas que assumiram um compromisso de confidencialidade ou que estão subordinadas a obrigações legais de confidencialidade;



- c) Adotar as medidas de segurança no tratamento dos referidos dados, em cumprimento do disposto no n.º1 do Art.32.º do Regulamento (UE) 2016/679, de 27 de Abril de 2016, nomeadamente:
1. A pseudonomização e a cifragem de dados pessoais;
 2. A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
 3. Capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada, em situações de incidente físico ou técnico;
 4. Ter um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.
- d) Somente recorrerá a subcontratantes se estes cumprirem todas as obrigações de tratamento de dados pessoais decorrentes do RGPD;
- e) Prestar assistência ao SMZC pelo tratamento de dados a fim desta assegurar o cumprimento das obrigações de segurança no referido tratamento, notificando a autoridade de controlo e aos respetivos titulares, em caso de violação de dados pessoais.
- f) Efetuar avaliações de impacto sobre a protecção de dados e consulta prévia, quando tal se justifique.
- g) Apagar ou devolver, dependendo dos dados em causa, todos os dados pessoais depois de decorrido o prazo de guarda dos mesmos, obrigando-se a eliminar as cópias existentes, salvo se tal conservação for legalmente obrigatória.



- h) Disponibilizar aos titulares dos dados, comprovativos do cumprimento das suas obrigações enquanto Responsável de Dados.
- i) Facilitar e apoiar a elaboração de auditorias e inspeções a realizar no SMZC.
- j) Informar no prazo máximo de 72h a CNPD em caso de violação do RGPD ou outras disposições em matéria de proteção de dados.
- k) A notificação tem que conter a descrição da natureza da violação de dados pessoais, incluindo o número de pessoas em causa, e registos de dados pessoais em questão, o nome e dados de contacto do responsável da proteção de dados, a descrição das consequências prováveis da violação de dados pessoais, e a descrição das medidas propostas pelo responsável de tratamento de dados, para reparação dos direitos violados.
- l) Quando a violação de dados for suscetível de causar prejuízo ao seu titular, designadamente, quando possa representar um alto risco para os direitos e liberdades, deve o titular ser informado, de forma clara e sem demora.