



Living
Care

Regulamento Interno
Proteção de Dados Pessoais

Setembro 2026

Índice

Preâmbulo	4
Capítulo I. Disposições Gerais	4
Artigo 1º. Objeto	4
Artigo 2º. Âmbito de Aplicação	4
Artigo 3º. Objetivos	5
Artigo 4º. Definições	5
Capítulo II. Princípios Gerais do Tratamento de Dados	5
Artigo 5º. Princípio da Licitude, Lealdade e Transparência	5
Artigo 6º. Princípio da Limitação das Finalidades	6
Artigo 7º. Princípio da Minimização dos Dados	6
Artigo 8º. Princípio da Exatidão	6
Artigo 9º. Princípio da Limitação da Conservação	6
Artigo 10º. Princípio da Integridade e Confidencialidade	6
Artigo 11º. Princípio da Responsabilidade	6
Capítulo III. Organização da Proteção de Dados	7
Artigo 12º. Responsável pelo Tratamento	7
Artigo 13º. Encarregado da Proteção de Dados	7
Artigo 14º. Responsabilidade da Direção	7
Artigo 15º. Responsabilidade das Chefias	7
Artigo 16º. Deveres dos Colaboradores	8
Artigo 17º. Prestadores de Serviços, Voluntários e Estagiários	8
Artigo 18º. Subcontratantes	8
Capítulo IV. Tratamento de Dados Pessoais	9
Artigo 19º. Categorias de Dados Pessoais Tratados	9
Artigo 20º. Finalidades do Tratamento	9
Capítulo V. Tratamento de Categorias Especiais de Dados	9
Artigo 21º. Dados Relativos à Saúde	9
Artigo 22º. Dados Biométricos	10
Artigo 23º. Dados de Natureza Social e Financeira	10
Capítulo VI. Videovigilância	10
Artigo 24º. Finalidade	10
Artigo 25º. Funcionamento do Sistema	10
Artigo 26º. Acesso às Imagens	10
Artigo 27º. Conservação das Gravações	11
Artigo 28º. Cedência de Imagens	11
Capítulo VII. Partilha e Comunicação de Dados Pessoais	11

Artigo 29º. Princípios Gerais	11
Artigo 30º. Comunicação a Entidades Públicas	11
Artigo 31º. Comunicação a Familiares e Representantes Legais	11
Artigo 32º. Comunicação a Subcontratantes	11
Capítulo VIII. Direito dos Titulares dos Dados	11
Artigo 33º. Direito à Informação	11
Artigo 34º. Direito ao Acesso	12
Artigo 35º. Direito de Retificação	12
Artigo 36º. Direito ao Apagamento	12
Artigo 37º. Direito à Limitação do Tratamento	12
Artigo 38º. Direito de Portabilidade	12
Artigo 39º. Direito de Oposição	12
Artigo 40º. Retirada de Consentimento	13
Artigo 41º. Exercício dos Direitos.....	13
Artigo 42º. Reclamações	13
Capítulo IX. Conservação e Eliminação dos Dados Pessoais	13
Artigo 43º. Conservação.....	13
Artigo 44º. Eliminação Segura.....	13
Capítulo X. Confidencialidade e Segurança da Informação	13
Artigo 45º. Dever da Confidencialidade	13
Artigo 46º. Segurança da Informação.....	13
Artigo 47º. Boas Práticas	14
Capítulo XI. Gestão de Incidentes	14
Artigo 48º. Comunicação.....	14
Capítulo XII. Formação e Sensibilização.....	14
Artigo 49º. Formação	14
Capítulo XIII. Auditoria e Melhoria Contínua.....	14
Artigo 50º. Monitorização	14
Capítulo XIV. Incumprimento	14
Artigo 51º. Responsabilidade.....	14
Capítulo XV. Disposições Finais	15
Artigo 52º. Documentos Complementares	15
Artigo 53º. Revisão	15
Artigo 54º. Entrada em Vigor	15
Artigo 55º. Casos Omissos.....	15
Artigo 56º. Publicitação	15

Preâmbulo

A Associação Living Care, enquanto Instituição Particular de Solidariedade Social (IPSS), dedica-se à prestação de cuidados e serviços de apoio a pessoas em situação de dependência, desenvolvendo a sua atividade com respeito pela dignidade humana, pela confidencialidade da informação e pela proteção dos direitos fundamentais dos seus utentes, colaboradores e demais titulares de dados pessoais.

No exercício da sua missão, a Associação procede diariamente ao tratamento de dados pessoais, incluindo categorias especiais de dados, designadamente dados relativos à saúde, cuja proteção assume particular relevância atendendo à natureza dos cuidados prestados.

O respeito pela privacidade e pela proteção dos dados pessoais constitui um princípio estruturante da atividade da Associação, sendo entendido não apenas como uma obrigação legal, mas como um compromisso ético para com todos aqueles que nela depositam a sua confiança.

O presente Regulamento Interno estabelece os princípios, normas e procedimentos aplicáveis ao tratamento de dados pessoais realizado pela Associação, assegurando o cumprimento do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – RGPD), da Lei n.º 58/2019, de 8 de agosto, e da demais legislação nacional e europeia aplicável.

Pretende-se igualmente promover uma cultura organizacional assente na responsabilidade, confidencialidade, segurança da informação e melhoria contínua, garantindo que todos os colaboradores, prestadores de serviços, voluntários, estagiários e demais intervenientes conhecem as suas responsabilidades relativamente ao tratamento de dados pessoais.

O cumprimento do presente Regulamento é obrigatório para todas as pessoas que, no exercício das suas funções ou da sua relação com a Associação, tenham acesso a dados pessoais tratados pela instituição.

Capítulo I. Disposições Gerais

Artigo 1º. Objeto

- a) O presente Regulamento estabelece as regras os princípios, normas e procedimentos relativos à recolha, utilização, conservação, transmissão, acesso, proteção e eliminação de dados pessoais tratados pela Associação.
- b) O Regulamento define igualmente os direitos e deveres dos titulares dos dados, dos colaboradores e dos restantes intervenientes que, por qualquer motivo, tenham acesso a dados pessoais tratados pela Associação.
- c) O presente Regulamento constitui o instrumento interno de referência da Associação em matéria de proteção de dados pessoais.

Artigo 2º. Âmbito de Aplicação

- a) O presente Regulamento aplica-se a todas as atividades de tratamento de dados pessoais realizados pela Associação, independentemente do respetivo suporte, formato ou tecnologia utilizada.
- b) O Regulamento aplica-se, designadamente, ao tratamento de dados relativos a:
 - i) Utes, familiares e representantes legais;
 - ii) Colaboradores;
 - iii) Prestadores de serviços;
 - iv) Candidatos a procedimentos de recrutamento;

- v) Voluntários;
- vi) Estagiários;
- vii) Membros dos órgãos sociais;
- viii) Fornecedores;
- ix) Parceiros institucionais;
- x) Visitantes;
- xi) Quaisquer outras pessoas singulares cujos dados sejam tratados pela Associação.

Artigo 3º. Objetivos

- a) Constituem objetivos do presente Regulamento:
 - i) Garantir o cumprimento da legislação aplicável em matéria de proteção de dados;
 - ii) Salvaguardar os direitos, liberdades e garantias dos titulares dos dados;
 - iii) Assegurar a confidencialidade, integridade, disponibilidade e autenticidade da informação;
 - iv) Promover uma cultura organizacional de proteção da informação;
 - v) Definir responsabilidades claras relativamente ao tratamento de dados pessoais;
 - vi) Estabelecer procedimentos uniformes para toda a organização;
 - vii) Reduzir o risco de incidentes de segurança e de violações de dados pessoais;
 - viii) Promover a confiança dos utentes, colaboradores, parceiros e restantes titulares de dados.

Artigo 4º. Definições

- a) Para efeitos do presente Regulamento entende-se por:
 - i) Dados pessoais: qualquer informação relativa a uma pessoa singular identificada ou identificável.
 - ii) Titular dos dados: a pessoa singular a quem os dados pessoais dizem respeito.
 - iii) Tratamento: qualquer operação efetuada sobre dados pessoais, designadamente recolha, registo, organização, conservação, consulta, utilização, comunicação, limitação, apagamento ou destruição.
 - iv) Categorias especiais de dados: os dados pessoais que revelem origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos destinados a identificar uma pessoa de forma inequívoca, dados relativos à saúde ou à vida sexual.
 - v) Responsável pelo tratamento: a Associação, que determina as finalidades e os meios do tratamento dos dados pessoais.
 - vi) Subcontratante: a pessoa singular ou coletiva que trate dados pessoais por conta da Associação.
 - vii) Violação de dados pessoais: qualquer incidente de segurança que provoque, de forma accidental ou ilícita, a destruição, perda, alteração, divulgação não autorizada ou acesso indevido a dados pessoais.
 - viii) Encarregado da Proteção de Dados (DPO): a pessoa designada pela Associação para acompanhar e assegurar o cumprimento das obrigações legais em matéria de proteção de dados pessoais.

Capítulo II. Princípios Gerais do Tratamento de Dados

Artigo 5º. Princípio da Licidade, Lealdade e Transparência

- a) Todos os tratamentos de dados pessoais realizados pela Associação devem assentar numa base jurídica válida prevista na legislação aplicável.
- b) Os dados pessoais são tratados de forma transparente, garantindo aos respetivos titulares informação clara, acessível e compreensível sobre a forma como os seus dados são utilizados.

- c) A Associação compromete-se a tratar os dados pessoais de forma leal, respeitando os direitos, expectativas legítimas e interesses dos respetivos titulares.

Artigo 6º. Princípio da Limitação das Finalidades

- a) Os dados pessoais apenas podem ser recolhidos para finalidades determinadas, explícitas e legítimas.
- b) É proibida a utilização dos dados pessoais para finalidades incompatíveis com aquelas que justificaram a sua recolha, salvo quando exista fundamento legal para o efeito.

Artigo 7º. Princípio da Minimização dos Dados

- a) Apenas serão recolhidos os dados pessoais estritamente necessários para a prossecução das finalidades identificadas.
- b) Sempre que possível, deverão ser privilegiados procedimentos que reduzam a quantidade de dados pessoais tratados.
- c) Os colaboradores devem abster-se de solicitar ou conservar informação que não seja necessária ao exercício das respetivas funções.

Artigo 8º. Princípio da Exatidão

- a) A Associação adota medidas adequadas para garantir que os dados pessoais tratados são exatos, completos e atualizados.
- b) Sempre que sejam detetadas inexatidões, os dados deverão ser corrigidos ou atualizados com a maior brevidade possível.

Artigo 9º. Princípio da Limitação da Conservação

- a) Os dados pessoais são conservados apenas durante o período necessário para o cumprimento das finalidades que justificaram a sua recolha ou pelo período exigido por disposição legal.
- b) Findo o prazo de conservação, os dados pessoais serão eliminados ou anonimizados de forma segura, salvo quando devam ser conservados por obrigação legal ou para defesa de direitos da Associação.

Artigo 10º. Princípio da Integridade e Confidencialidade

- a) A Associação implementa medidas técnicas e organizativas adequadas para proteger os dados pessoais contra destruição, perda, alteração, divulgação ou acesso não autorizado.
- b) Todos os colaboradores e demais pessoas abrangidas pelo presente Regulamento encontram-se obrigados ao dever permanente de confidencialidade relativamente aos dados pessoais de que tenham conhecimento no exercício das suas funções.
- c) O dever de confidencialidade mantém-se mesmo após a cessação da relação laboral, contratual ou funcional com a Associação.

Artigo 11º. Princípio da Responsabilidade

- a) A Associação compromete-se a demonstrar, a todo o momento, o cumprimento das obrigações legais em matéria de proteção de dados pessoais.
- b) Para efeitos do número anterior, a Associação adota políticas, procedimentos internos, ações de formação, mecanismos de monitorização e medidas de segurança adequadas ao risco inerente aos tratamentos realizados.
- c) Todos os colaboradores devem cooperar na implementação das medidas previstas no presente Regulamento, contribuindo para uma cultura de proteção de dados e segurança da informação.

Capítulo III. Organização da Proteção de Dados

Artigo 12º. Responsável pelo Tratamento

- a) A Associação é a responsável pelo tratamento dos dados pessoais recolhidos e tratados no âmbito da sua atividade institucional.
- b) Compete à Associação determinar as finalidades e os meios do tratamento dos dados pessoais, assegurando que todas as operações realizadas cumprem a legislação aplicável em matéria de proteção de dados.
- c) Enquanto responsável pelo tratamento, a Associação compromete-se a:
 - i) Assegurar a licitude dos tratamentos efetuados;
 - ii) Implementar medidas técnicas e organizativas adequadas à proteção dos dados pessoais;
 - iii) Garantir que apenas são tratados os dados estritamente necessários para cada finalidade;
 - iv) Promover a formação e sensibilização dos seus colaboradores;
 - v) Disponibilizar mecanismos que permitam aos titulares exercer os seus direitos;
 - vi) Avaliar periodicamente a eficácia das medidas de segurança adotadas.

Artigo 13º. Encarregado da Proteção de Dados

- a) A Associação designa um Encarregado da Proteção de Dados (DPO), nos termos da legislação aplicável.
- b) O DPO exerce as suas funções com independência e autonomia técnica.
- c) Compete ao DPO, designadamente:
 - i) Informar e aconselhar a Direção Executiva e os colaboradores relativamente às obrigações decorrentes da legislação sobre proteção de dados;
 - ii) Acompanhar o cumprimento do presente Regulamento;
 - iii) Promover ações de sensibilização e formação;
 - iv) Emitir pareceres sobre novos tratamentos de dados pessoais;
 - v) Cooperar com a Comissão Nacional de Proteção de Dados;
 - vi) Constituir o ponto de contacto entre a Associação e os titulares dos dados relativamente às matérias de proteção de dados;
 - vii) Acompanhar a gestão de incidentes e violações de dados pessoais.
- d) O DPO poderá ser contactado através do endereço eletrónico institucional disponibilizado pela Associação: dpo@livingcare.pt

Artigo 14º. Responsabilidade da Direção

- a) Compete à Direção da Associação:
 - i) Aprovar as políticas e procedimentos internos em matéria de proteção de dados;
 - ii) Disponibilizar os recursos humanos, técnicos e financeiros necessários ao cumprimento das obrigações legais;
 - iii) Garantir que os sistemas de informação utilizados oferecem níveis adequados de segurança;
 - iv) Promover uma cultura organizacional baseada na proteção da informação;
 - v) Avaliar os riscos associados ao tratamento de dados pessoais;
 - vi) Assegurar que os contratos celebrados com subcontratantes incluem as cláusulas legalmente exigidas em matéria de proteção de dados.

Artigo 15º. Responsabilidade das Chefias

- a) As chefias intermédias desempenham um papel fundamental na implementação do presente Regulamento.
- b) Compete às chefias:
 - i) Garantir que os colaboradores sob sua coordenação conhecem e cumprem o presente Regulamento;

- ii) Controlar os acessos à informação necessária ao desempenho das funções;
- iii) Comunicar imediatamente quaisquer incidentes de segurança ou suspeitas de violação de dados;
- iv) Promover boas práticas de confidencialidade no respetivo serviço;
- v) Colaborar com o DPO na implementação de medidas corretivas.

Artigo 16º. Deveres dos Colaboradores

- a) Todos os colaboradores são responsáveis pela proteção dos dados pessoais a que tenham acesso no exercício das suas funções.
- b) Constituem deveres dos colaboradores:
 - i) Tratar apenas os dados necessários ao desempenho das respetivas funções;
 - ii) Respeitar o dever de sigilo profissional;
 - iii) Utilizar exclusivamente os sistemas e equipamentos autorizados pela Associação;
 - iv) Manter confidenciais as credenciais de acesso aos sistemas informáticos;
 - v) Comunicar imediatamente qualquer incidente de segurança ou suspeita de violação de dados pessoais;
 - vi) Participar nas ações de formação promovidas pela Associação.

Artigo 17º. Prestadores de Serviços, Voluntários e Estagiários

- a) Os prestadores de serviços, voluntários, estagiários e demais colaboradores externos encontram-se igualmente vinculados às obrigações previstas no presente Regulamento.
- b) Sempre que tenham acesso a dados pessoais, deverão assinar compromisso de confidencialidade e cumprir as instruções transmitidas pela Associação.
- c) Os acessos concedidos serão limitados às funções efetivamente desempenhadas e cessarão imediatamente após o termo da respetiva colaboração.

Artigo 18º. Subcontratantes

- a) Sempre que o tratamento de dados pessoais seja efetuado por entidades externas em nome da Associação, deverá existir contrato escrito contendo as cláusulas previstas no artigo 28.º do Regulamento Geral sobre a Proteção de Dados.
- b) Os subcontratantes apenas poderão tratar dados pessoais mediante instruções documentadas da Associação.
- c) Os subcontratantes deverão implementar medidas técnicas e organizativas adequadas que garantam um nível de segurança compatível com os riscos do tratamento.
- d) A Associação poderá solicitar evidências documentais do cumprimento das obrigações assumidas pelos subcontratantes.
- e) Os dados podem ser tratados, mediante necessidade legal ou contratual, com as seguintes entidades:
 - i) Gestão e Auditoria;
 - ii) Seguros;
 - iii) Advogados;
 - iv) Saúde e Segurança no Trabalho;
 - v) Medicina do Trabalho;
 - vi) Entidades Oficiais;
 - vii) Laboratórios de Análises Clínicas;
 - viii) Fornecedores de Equipamentos de Ventiloterapia e Oxigenoterapia;
 - ix) Outros fornecedores de equipamentos.

Capítulo IV. Tratamento de Dados Pessoais

Artigo 19º. Categorias de Dados Pessoais Tratados

- a) A Associação trata apenas os dados adequados, pertinentes e limitados ao necessário para cada finalidade.
- b) Consoante a natureza da relação estabelecida, poderão ser tratados, entre outros, os seguintes dados:
 - i) Dados de identificação;
 - ii) Dados de contacto;
 - iii) Dados fiscais;
 - iv) Dados da Segurança Social;
 - v) Dados bancários;
 - vi) Dados profissionais;
 - vii) Dados académicos;
 - viii) Dados biométricos destinados ao controlo de acessos ou assiduidade, quando legalmente admissível;
 - ix) Dados relativos à saúde;
 - x) Dados relativos à situação socioeconómica dos utentes;
 - xi) Imagens recolhidas pelos sistemas de videovigilância;
 - xii) Registos de acesso aos sistemas informáticos.
- c) O tratamento de categorias especiais de dados apenas será realizado quando exista fundamento legal adequado e observadas as garantias previstas na legislação aplicável.

Artigo 20º. Finalidades do Tratamento

- a) Os dados pessoais tratados pela Associação destinam-se, designadamente, às seguintes finalidades:
 - i) Para os dados recolhidos junto aos utentes, familiares e representantes legais:
 - 1) Prestação de cuidados de saúde e apoio social;
 - 2) Gestão administrativa dos utentes;
 - 3) Elaboração e execução de planos individuais de cuidados;
 - ii) Para os dados recolhidos junto aos trabalhadores e prestadores de serviço:
 - 1) Gestão contratual;
 - 2) Gestão de recursos humanos;
 - 3) Processamento salarial;
 - 4) Cumprimento de obrigações fiscais, laborais e contributivas;
 - 5) Recrutamento e seleção;
 - 6) Gestão da formação;
 - 7) Segurança de pessoas e bens;
 - 8) Controlo de acessos;
 - 9) Cumprimento de obrigações legais;
 - 10) Exercício ou defesa de direitos em processos judiciais ou administrativos;
 - 11) Comunicação institucional, quando exista fundamento legal para o efeito.

Capítulo V. Tratamento de Categorias Especiais de Dados

Artigo 21º. Dados Relativos à Saúde

- a) Atendendo à natureza da atividade desenvolvida pela Associação, o tratamento de dados relativos à saúde constitui uma atividade essencial para a prestação de cuidados aos utentes.

- b) Os dados relativos à saúde apenas poderão ser tratados por profissionais devidamente autorizados e na estrita medida necessária ao exercício das respetivas funções.
- c) O acesso aos processos clínicos deve obedecer ao princípio da necessidade de conhecimento, sendo proibida a consulta de informação clínica sem fundamento funcional.
- d) Sempre que possível, os dados clínicos devem ser tratados em sistemas de informação protegidos por mecanismos de autenticação individual.
- e) Os colaboradores ficam obrigados ao dever de sigilo profissional relativamente a toda a informação clínica de que tomem conhecimento, independentemente da forma como a mesma seja obtida.
- f) O dever de confidencialidade mantém-se após a cessação da relação laboral ou contratual.

Artigo 22º. Dados Biométricos

- a) A Associação pode proceder ao tratamento de dados biométricos dos seus trabalhadores para efeitos de controlo de assiduidade e/ou controlo de acesso às suas instalações.
- b) O tratamento deve respeitar os princípios da necessidade, proporcionalidade, minimização, limitação das finalidades, segurança e limitação da conservação, sendo os dados utilizados exclusivamente para as finalidades que determinaram a sua recolha.
- c) O sistema deverá assegurar que são utilizadas apenas representações ou templates biométricos, sem possibilidade de reconstrução ou reversibilidade do dado biométrico original.
- d) A Associação não utilizará os dados biométricos para monitorizar a circulação dos trabalhadores nas suas instalações, avaliar o seu desempenho ou para qualquer outra finalidade incompatível com as previstas no presente artigo.

Artigo 23º. Dados de Natureza Social e Financeira

- a) Sempre que necessário à determinação da situação socioeconómica dos utentes, a Associação poderá proceder ao tratamento de informação relativa aos rendimentos do agregado familiar, prestações sociais, declarações fiscais e demais documentação legalmente exigível.
- b) Estes dados apenas poderão ser utilizados para as finalidades que justificaram a respetiva recolha.
- c) O acesso a esta informação será limitado aos colaboradores cujas funções o justifiquem.

Capítulo VI. Videovigilância

Artigo 24º. Finalidade

- a) A Associação dispõe de um sistema de videovigilância destinado exclusivamente à proteção de pessoas e bens, à prevenção de incidentes de segurança e à salvaguarda das instalações.
- b) O sistema não poderá ser utilizado para controlar de forma permanente o desempenho profissional dos colaboradores, sem prejuízo das situações legalmente previstas.

Artigo 25º. Funcionamento do Sistema

- a) O sistema de videovigilância, constituído por 76 câmaras, encontra-se instalado nas unidades de saúde da Associação em grupos de 18, 16 e 42, devidamente sinalizados e em conformidade com a legislação aplicável.
- b) As câmaras são posicionadas de forma a respeitar o princípio da proporcionalidade, evitando sempre que possível a captação de áreas cuja vigilância não seja necessária.
- c) Sempre que tecnicamente possível, deverão ser evitadas captações de zonas especialmente sensíveis.

Artigo 26º. Acesso às Imagens

- a) O acesso às imagens encontra-se limitado às pessoas expressamente autorizadas pela Direção.
- b) A consulta de gravações apenas poderá ocorrer quando necessária para:

- i) Investigação de incidentes;
- ii) Proteção de pessoas e bens;
- iii) Cumprimento de obrigação legal;
- iv) Colaboração com autoridades competentes.

Artigo 27º. Conservação das Gravações

- a) As gravações são conservadas em disco durante o prazo de 30 dias, sendo automaticamente eliminadas após o respetivo decurso, salvo quando devam ser preservadas para efeitos de investigação ou cumprimento de obrigação legal.
- b) A conservação por período superior apenas poderá ocorrer quando exista fundamento legal que o justifique.

Artigo 28º. Cedência de Imagens

- a) As gravações apenas poderão ser facultadas às autoridades judiciárias, órgãos de polícia criminal ou outras entidades legalmente competentes.
- b) Qualquer pedido de acesso deverá ser registado e arquivado.

Capítulo VII. Partilha e Comunicação de Dados Pessoais

Artigo 29º. Princípios Gerais

- a) A comunicação de dados pessoais a terceiros apenas poderá ocorrer quando exista fundamento jurídico para o efeito.
- b) Antes de qualquer transmissão de dados deverá ser verificada:
 - i) A identidade da entidade destinatária;
 - ii) A legitimidade do pedido;
 - iii) A proporcionalidade da informação a transmitir.
- c) Apenas deverão ser comunicados os dados estritamente necessários à finalidade pretendida.

Artigo 30º. Comunicação a Entidades Públicas

- a) A Associação poderá comunicar dados pessoais às entidades públicas competentes sempre que tal decorra de obrigação legal, decisão judicial ou exercício de poderes legalmente conferidos.

Artigo 31º. Comunicação a Familiares e Representantes Legais

- a) A prestação de informação a familiares ou representantes legais deverá respeitar os direitos dos utentes e a legislação aplicável.
- b) Sempre que existam dúvidas quanto à legitimidade do pedido, deverá ser solicitada orientação ao superior hierárquico ou ao Encarregado da Proteção de Dados.

Artigo 32º. Comunicação a Subcontratantes

- a) Sempre que entidades externas tratem dados pessoais por conta da Associação, deverá existir contrato escrito que estabeleça as respetivas responsabilidades em matéria de proteção de dados.
- b) Os subcontratantes ficam obrigados ao cumprimento integral das instruções transmitidas pela Associação e das disposições constantes da legislação aplicável.

Capítulo VIII. Direito dos Titulares dos Dados

Artigo 33º. Direito à Informação

- a) Os titulares dos dados têm o direito de ser informados, de forma clara e acessível, sobre:

- i) A identidade do responsável pelo tratamento;
 - ii) As finalidades do tratamento;
 - iii) A base jurídica aplicável;
 - iv) Os destinatários dos dados;
 - v) Os prazos de conservação;
 - vi) Os direitos que lhes assistem;
 - vii) Os contactos do Encarregado da Proteção de Dados.
- b) Sempre que os dados não sejam recolhidos diretamente junto do titular, a Associação prestará a informação legalmente exigida nos prazos previstos no RGPD.

Artigo 34º. Direito ao Acesso

- a) O titular dos dados pode solicitar confirmação de que os seus dados pessoais são objeto de tratamento.
- b) Sempre que solicitado, a Associação disponibilizará informação sobre:
- i) As categorias de dados tratados;
 - ii) As finalidades do tratamento;
 - iii) Os destinatários dos dados;
 - iv) O prazo previsto de conservação;
 - v) A origem dos dados, quando aplicável.

Artigo 35º. Direito de Retificação

- a) O titular pode solicitar a atualização ou correção dos seus dados pessoais sempre que estes se encontrem inexatos, incompletos ou desatualizados.
- b) A Associação procederá às diligências necessárias para assegurar a atualização da informação no mais curto prazo possível.

Artigo 36º. Direito ao Apagamento

- a) O titular poderá solicitar o apagamento dos seus dados pessoais quando se verificarem os pressupostos legalmente previstos.
- b) O direito ao apagamento poderá não ser exercido quando o tratamento seja necessário para:
- i) Cumprimento de obrigação legal;
 - ii) Exercício de funções de interesse público;
 - iii) Arquivo de interesse público;
 - iv) Defesa de direitos em processos judiciais ou administrativos;
 - v) Prestação continuada de cuidados ou cumprimento de obrigações decorrentes da atividade assistencial.

Artigo 37º. Direito à Limitação do Tratamento

- a) Sempre que a lei o permita, o titular poderá solicitar a limitação do tratamento dos seus dados pessoais até à verificação das circunstâncias que fundamentam o respetivo pedido.

Artigo 38º. Direito de Portabilidade

- a) Quando aplicável, o titular poderá solicitar que os seus dados pessoais lhe sejam disponibilizados em formato estruturado, de uso corrente e de leitura automática, ou transmitidos a outro responsável pelo tratamento.

Artigo 39º. Direito de Oposição

- a) O titular poderá opor-se ao tratamento dos seus dados sempre que tal seja legalmente admissível.

- b) A Associação apreciará cada pedido individualmente, ponderando os fundamentos invocados e a legislação aplicável.

Artigo 40º. Retirada de Consentimento

- a) Sempre que o tratamento tenha por base o consentimento, este poderá ser retirado a qualquer momento.
- b) A retirada do consentimento não prejudica a licitude do tratamento efetuado antes da respetiva revogação.

Artigo 41º. Exercício dos Direitos

- a) Os pedidos de exercício de direitos deverão ser apresentados por escrito, através dos canais disponibilizados pela Associação.
- b) Todos os pedidos deverão ser encaminhados para os serviços competentes, pelo que qualquer colaborador deve abster-se de responder autonomamente, salvo autorização expressa ou obrigação legal.
- c) A Associação responderá aos pedidos dentro dos prazos legalmente estabelecidos.

Artigo 42º. Reclamações

- a) Sem prejuízo de outros meios de tutela administrativa ou judicial, os titulares dos dados poderão apresentar reclamação junto da Comissão Nacional de Proteção de Dados ou recorrer aos tribunais competentes.

Capítulo IX. Conservação e Eliminação dos Dados Pessoais

Artigo 43º. Conservação

- a) Os dados pessoais apenas serão conservados durante o período necessário para as finalidades que justificaram a sua recolha ou pelo prazo imposto por disposição legal.
- b) A conservação dos dados deverá respeitar o princípio da minimização e evitar a manutenção de informação desnecessária.

Artigo 44º. Eliminação Segura

- a) Findo o período de conservação, os dados serão eliminados, anonimizados ou arquivados, quando legalmente admissível.
- b) A eliminação de dados pessoais deverá assegurar a impossibilidade da sua recuperação.

Capítulo X. Confidencialidade e Segurança da Informação

Artigo 45º. Dever da Confidencialidade

- a) Todas as pessoas que exerçam funções na Associação encontram-se obrigadas a guardar absoluto sigilo relativamente aos dados pessoais e demais informação confidencial de que tomem conhecimento no exercício das suas funções.
- b) O dever de confidencialidade mantém-se mesmo após a cessação da relação laboral, contratual ou funcional.

Artigo 46º. Segurança da Informação

- a) A Associação implementará medidas técnicas e organizativas adequadas para proteger os ativos de informação contra perda, destruição, alteração, divulgação ou acesso não autorizado.

- b) As medidas adotadas terão em consideração a natureza dos dados tratados, os riscos identificados e as boas práticas internacionalmente reconhecidas em matéria de segurança da informação.

Artigo 47º. Boas Práticas

- a) Todos os intervenientes deverão adotar comportamentos responsáveis relativamente à utilização da informação institucional, designadamente através da utilização segura dos sistemas informáticos, proteção das palavras-passe, aplicação da política de secretária limpa, bloqueio dos equipamentos, proteção da documentação em papel, utilização prudente do correio eletrónico e comunicação imediata de incidentes de segurança.

Capítulo XI. Gestão de Incidentes

Artigo 48º. Comunicação

- a) Qualquer colaborador que tenha conhecimento de um incidente deverá comunicá-lo imediatamente à respetiva chefia e ao DPO.
- b) A comunicação deverá ocorrer logo que possível, ainda que não sejam conhecidos todos os elementos do incidente.
- c) Nenhum colaborador poderá ocultar ou retardar a comunicação de uma violação de dados pessoais.
- d) Após a comunicação, a Associação procederá à análise, registo, contenção, mitigação e resolução do incidente, adotando medidas legalmente exigíveis.

Capítulo XII. Formação e Sensibilização

Artigo 49º. Formação

- a) A Associação promoverá ações regulares de formação e sensibilização destinadas a todos os colaboradores, visando reforçar a cultura organizacional de proteção de dados, segurança da informação e cibersegurança.
- b) A participação nas ações de formação constitui um dever profissional dos colaboradores.

Capítulo XIII. Auditoria e Melhoria Contínua

Artigo 50º. Monitorização

- a) A Associação promoverá a monitorização periódica da eficácia das medidas implementadas, procedendo à revisão dos procedimentos, políticas e controlos sempre que tal se revele necessário.
- b) Sempre que aplicável, poderão ser realizadas auditorias internas ou externas destinadas à avaliação da conformidade com a legislação e com os referenciais de boas práticas adotados pela instituição.

Capítulo XIV. Incumprimento

Artigo 51º. Responsabilidade

- a) O incumprimento das disposições constantes do presente Regulamento poderá determinar a aplicação das medidas disciplinares, contratuais, civis, contraordenacionais ou criminais legalmente previstas, sem prejuízo da eventual obrigação de indemnizar os danos causados.

Capítulo XV. Disposições Finais

Artigo 52º. Documentos Complementares

- a) Constituem documentos complementares ao presente Regulamento, dele fazendo parte integrante para efeitos de aplicação interna:
 - i) Política de Proteção de Dados Aplicável aos Colaboradores;
 - ii) Política de Proteção de Dados Aplicável aos Subcontratantes;
 - iii) Política de Proteção de Dados Aplicável aos Utentes, Familiares e Representantes Legais;
 - iv) Manual de Boas Práticas de Proteção de Dados e Segurança da Informação para Colaboradores;
 - v) Demais procedimentos internos aprovados pela Direção em matéria de proteção de dados e segurança da informação.

Artigo 53º. Revisão

- a) O presente Regulamento será revisto sempre que ocorram alterações legislativas, organizacionais, tecnológicas ou sempre que a avaliação dos riscos ou os resultados das auditorias o justifiquem.
- b) Na ausência de alterações relevantes, será objeto de revisão periódica, pelo menos, de três em três anos.

Artigo 54º. Entrada em Vigor

- a) O presente Regulamento entra em vigor após aprovação pela Direção da Associação, produzindo efeitos na data definida na respetiva deliberação.
- b) A Associação assegurará a divulgação do presente Regulamento e dos documentos complementares, promovendo os meios necessários para o seu efetivo cumprimento e melhoria contínua.

Artigo 55º. Casos Omissos

- a) Os casos omissos serão resolvidos de acordo com o Regulamento Geral sobre a Proteção de Dados, a Lei n.º 58/2019, demais legislação aplicável e princípios gerais de proteção de dados.

Artigo 56º. Publicitação

- a) O presente Regulamento será disponibilizado a todos os colaboradores da Associação.
- b) A Associação promoverá a divulgação do Regulamento através dos meios internos considerados adequados.

Aprovado por deliberação da Direção, exarada na Ata da Direção n.º 54, de 24 de setembro de 2026



Living
Care

Manual de Boas Práticas
Proteção de Dados e Segurança da Informação

Setembro 2026

Introdução

A proteção dos dados pessoais e da informação constitui uma responsabilidade de todos os colaboradores da Associação.

No exercício diário das suas funções, cada colaborador contacta com informação que merece elevados níveis de proteção, designadamente dados relativos aos utentes, familiares, representantes legais, colaboradores, fornecedores, parceiros e demais titulares dos dados pessoais.

A adoção de boas práticas de proteção de dados e de segurança da informação contribui não só para o cumprimento das obrigações legais decorrentes do Regulamento Geral sobre a Proteção de Dados (RGPD), mas também para a preservação da confiança depositada na Associação, para a qualidade dos serviços prestados e para a proteção da dignidade e privacidade de todas as pessoas com quem a instituição se relaciona.

O presente Manual constitui um instrumento de apoio à atividade diária dos colaboradores, reunindo um conjunto de orientações práticas destinadas a promover comportamentos seguros, prevenir incidentes e reforçar a cultura organizacional de proteção de dados, segurança da informação e cibersegurança.

Este Manual complementa o Regulamento de Proteção de Dados Pessoais, a Política de Proteção de Dados Pessoais Aplicável aos Colaboradores e os restantes documentos internos da Associação, devendo ser interpretado em articulação com esses instrumentos e aplicado por todos os colaboradores no exercício das respetivas funções.

Mais do que um conjunto de regras, este Manual pretende constituir um guia de atuação prática que apoie os colaboradores na tomada de decisões responsáveis sempre que tratem dados pessoais ou informação institucional.

Sempre que exista dúvida sobre a forma correta de atuar, deverá prevalecer o princípio da proteção da privacidade e da segurança da informação, devendo o colaborador solicitar orientação ao seu superior hierárquico ou ao Encarregado da Proteção de Dados antes de adotar qualquer decisão.

Informação a Proteger

- Todos os colaboradores devem proteger a informação a que tenham acesso no exercício das respetivas funções, independentemente do seu formato (papel, suporte digital, fotografia, áudio, vídeo ou outro) e do local onde seja tratada.
- Devem ser especialmente protegidos os dados pessoais relativos a:
 - Utes;ntes;
 - Familiares e representantes legais;
 - Colaboradores;
 - Candidatos a emprego;
 - Fornecedores e prestadores de serviços;
 - Voluntários, estagiários e parceiros;
 - Visitantes e quaisquer outros titulares dos dados com quem a Associação mantenha relações institucionais.
- Para além dos dados pessoais, os colaboradores devem igualmente proteger toda a informação institucional não destinada ao conhecimento público, designadamente documentação administrativa, financeira, contratual, técnica, estratégica ou qualquer outra cuja divulgação possa prejudicar a Associação, os seus utentes ou terceiros.
- Sempre que exista dúvida sobre a natureza da informação ou sobre o respetivo nível de proteção, o colaborador deve tratá-la como confidencial até obter orientação do superior hierárquico ou do Encarregado da Proteção de Dados.

Princípios fundamentais de atuação

- A proteção dos dados pessoais depende, em grande medida, da atuação diária de cada colaborador. No exercício das suas funções, todos devem adotar comportamentos responsáveis e diligentes, observando, designadamente, as seguintes boas práticas:
 - **Aceder apenas à informação necessária**
Consultar apenas os dados pessoais indispensáveis ao desempenho das funções que lhe estão atribuídas, respeitando o princípio da necessidade de conhecimento (*need to know*).
 - **Utilizar a informação exclusivamente para fins profissionais**
Os dados pessoais apenas podem ser utilizados para a prestação dos serviços, para o cumprimento de obrigações legais ou para outras finalidades autorizadas pela Associação, sendo proibida qualquer utilização para fins pessoais ou estranhos às funções desempenhadas.
 - **Garantir a confidencialidade da informação**
Não divulgar dados pessoais ou informação institucional a pessoas que não estejam autorizadas a conhecê-los, mesmo quando se trate de colegas da Associação.
 - **Confirmar a identidade antes de divulgar informação**
Antes de fornecer qualquer informação por telefone, correio eletrónico, presencialmente ou por outro meio, confirmar que o destinatário está devidamente identificado e possui legitimidade para receber essa informação.
 - **Proteger a informação durante todo o seu ciclo de vida**
Adotar os cuidados necessários na recolha, consulta, utilização, armazenamento, transmissão, arquivo e eliminação de documentos ou ficheiros que contenham dados pessoais.
 - **Comunicar situações de risco**
Informar de imediato o superior hierárquico ou o Encarregado da Proteção de Dados sempre que detete uma situação suscetível de comprometer a segurança da informação ou a proteção dos dados pessoais.
 - **Atuar com prudência em caso de dúvida**
Sempre que exista incerteza quanto à forma correta de tratar ou divulgar dados pessoais, o colaborador deve abster-se de praticar qualquer ato até obter orientação adequada.

Credenciais de Acesso e Autenticação

- As credenciais de acesso atribuídas pela Associação são pessoais e intransmissíveis, destinando-se exclusivamente ao colaborador a quem foram atribuídas, não podendo ser partilhadas, cedidas ou utilizadas por terceiros.
- Os colaboradores são responsáveis pela confidencialidade das respetivas credenciais de acesso, devendo adotar as medidas necessárias para impedir a sua divulgação ou utilização indevida.
- Sempre que sejam utilizadas palavras-passe, estas devem ser robustas, difíceis de adivinhar e distintas das utilizadas em contas pessoais, devendo ser alteradas sempre que exista suspeita de compromisso da sua confidencialidade ou quando tal seja determinado pela Associação.
- Sempre que disponível, deve ser utilizada a autenticação multifator (MFA) ou outro mecanismo adicional de autenticação disponibilizado pela Associação, reforçando a proteção dos sistemas de informação.
- É proibido registar palavras-passe em locais visíveis, partilhá-las através de correio eletrónico, mensagens ou outros meios inseguros, bem como permitir que terceiros utilizem as credenciais de acesso atribuídas ao colaborador.

- Sempre que o colaborador se ausente do posto de trabalho, ainda que por um curto período, deve bloquear a sessão de trabalho ou terminar a sessão, impedindo o acesso não autorizado aos sistemas de informação.
- Sempre que exista suspeita de utilização indevida das credenciais de acesso ou de comprometimento da segurança da conta, o colaborador deve alterar imediatamente a palavra-passe, quando possível, e comunicar a situação ao superior hierárquico ou ao responsável pelos sistemas de informação.

Política de Secretária Limpa e Ecrã Limpo

- A proteção da informação começa no posto de trabalho. Todos os colaboradores devem manter os respetivos espaços de trabalho organizados e livres de documentação ou informação que possa ser visualizada ou acedida por pessoas não autorizadas.
- Sempre que se ausentem do posto de trabalho, ainda que por um curto período de tempo, os colaboradores devem:
 - Bloquear o computador ou terminar a sessão de trabalho;
 - Guardar documentos contendo dados pessoais ou informação confidencial em locais seguros;
 - Recolher documentos deixados nas impressoras, fotocopiadoras ou outros equipamentos de impressão;
 - Evitar deixar processos, apontamentos, agendas ou outros suportes contendo informação confidencial sobre secretárias, balcões ou salas de atendimento.
- No final do período de trabalho, toda a documentação deve ser devidamente arquivada ou guardada nos locais destinados para o efeito, devendo as secretárias permanecer livres de documentos que contenham dados pessoais ou informação institucional confidencial.
- Os ecrãs dos computadores devem ser posicionados, sempre que possível, de forma a impedir a visualização por utentes, familiares, visitantes ou outras pessoas não autorizadas.
- Sempre que sejam realizadas reuniões presenciais, consultas técnicas ou atendimentos, deve ser assegurado que apenas permanece visível a informação estritamente necessária para a atividade em curso, devendo toda a restante documentação permanecer protegida.
- A adoção da Política de Secretária Limpa e Ecrã Limpo constitui uma medida essencial de prevenção de acessos indevidos e de proteção da privacidade dos titulares dos dados.

Utilização dos Equipamentos e dos Sistemas de Informação

- Os equipamentos informáticos, aplicações, sistemas de informação, redes e demais recursos tecnológicos disponibilizados pela Associação destinam-se prioritariamente ao exercício das funções profissionais dos colaboradores, devendo ser utilizados de forma responsável, segura e em conformidade com as normas internas em vigor.
- Os colaboradores devem utilizar exclusivamente os equipamentos, programas e aplicações autorizados pela Associação, abstendo-se de instalar software, ligar dispositivos externos ou alterar configurações dos sistemas sem autorização prévia dos serviços competentes.
- Na utilização diária dos equipamentos e sistemas de informação, os colaboradores devem observar, designadamente, as seguintes boas práticas:
 - Utilizar apenas as credenciais de acesso que lhes tenham sido atribuídas;
 - Manter os equipamentos protegidos contra acessos não autorizados;
 - Encerrar ou bloquear as sessões de trabalho sempre que se ausentem do posto de trabalho;
 - Utilizar apenas dispositivos de armazenamento autorizados pela Associação;

- Comunicar imediatamente qualquer anomalia, avaria ou comportamento inesperado dos equipamentos ou sistemas;
 - Zelar pela conservação dos equipamentos e utilizá-los de forma diligente.
- Sempre que os equipamentos sejam utilizados fora das instalações da Associação, os colaboradores devem assegurar a respetiva proteção física, evitando deixá-los em locais desprotegidos, veículos ou outros espaços suscetíveis de facilitar o furto, perda ou acesso indevido.
- É proibida a utilização dos recursos tecnológicos da Associação para atividades ilícitas, para fins incompatíveis com o exercício das funções ou suscetíveis de comprometer a segurança da informação, o funcionamento dos sistemas ou a proteção dos dados pessoais.
- Sempre que exista dúvida sobre a utilização de qualquer equipamento, aplicação ou sistema de informação, o colaborador deve solicitar orientação antes de proceder à sua utilização.

Utilização Segura do Correio Eletrónico

- O correio eletrónico institucional constitui um instrumento de trabalho e deve ser utilizado de forma responsável, segura e exclusivamente para fins profissionais, respeitando as normas internas da Associação e a legislação aplicável em matéria de proteção de dados pessoais.
- Antes de enviar mensagens de correio eletrónico, os colaboradores devem confirmar cuidadosamente os destinatários, o conteúdo da mensagem e os ficheiros anexos, assegurando que a informação é transmitida apenas às pessoas que possuem legitimidade para a receber.
- Sempre que sejam enviados dados pessoais para múltiplos destinatários externos entre si independentes, deverá ser utilizado, sempre que adequado, o campo CCO (Conhecimento Oculto), de forma a proteger a identidade e os contactos dos destinatários.
- Sempre que contenham dados pessoais ou informação confidencial, os ficheiros anexos devem ser protegidos através dos mecanismos de segurança disponibilizados pela Associação, sempre que tal seja tecnicamente possível e adequado ao risco associado.
- Os colaboradores devem manter uma atitude crítica perante mensagens inesperadas, pedidos urgentes, solicitações de informação confidencial, pedidos de pagamento, alteração de dados bancários ou quaisquer comunicações que suscitem dúvidas quanto à identidade do remetente.
- É proibido abrir anexos, clicar em hiperligações ou descarregar ficheiros provenientes de mensagens cuja autenticidade seja duvidosa ou que apresentem características suscetíveis de indiciar fraude informática, phishing ou outras formas de engenharia social.
- Sempre que exista suspeita relativamente à autenticidade de uma mensagem de correio eletrónico, o colaborador deve confirmar a identidade do remetente através de um canal alternativo antes de praticar qualquer ato solicitado.
- Sempre que seja identificada uma mensagem suspeita, o colaborador deve comunicar de imediato a situação ao superior hierárquico ou aos serviços responsáveis, abstendo-se de responder ou de reencaminhar a mensagem, clicar em hiperligações ou eliminar a evidência até receber orientações.

Utilização da Internet e das Redes Sociais

- O acesso à Internet disponibilizado pela Associação constitui um recurso de trabalho e deve ser utilizado de forma responsável, segura e compatível com o exercício das funções profissionais.
- Os colaboradores devem aceder apenas a páginas e plataformas cuja utilização seja necessária ao desempenho das respetivas funções, evitando a navegação em sítios eletrónicos suscetíveis de comprometer a segurança dos sistemas de informação ou de expor a Associação a riscos informáticos.

- É proibido descarregar ou instalar programas, aplicações, ficheiros ou outros conteúdos provenientes da Internet sem autorização prévia da Associação ou dos serviços responsáveis pelos sistemas de informação.
- Na utilização das redes sociais, os colaboradores devem respeitar os deveres de confidencialidade, sigilo profissional e proteção dos dados pessoais, abstendo-se de divulgar informação relativa à atividade da Associação, aos utentes, familiares, representantes legais, colaboradores ou quaisquer outros titulares dos dados, salvo quando tal seja expressamente autorizado.
- A publicação de fotografias, vídeos ou quaisquer imagens captadas nas instalações da Associação deve respeitar os direitos de personalidade, a legislação aplicável e as normas internas em vigor, sendo proibida a divulgação de conteúdos que permitam identificar utentes ou revelar informação confidencial sem fundamento legal ou autorização válida.
- Sempre que consultem conteúdos na Internet ou recebam informação através de plataformas digitais, os colaboradores devem adotar uma atitude crítica relativamente à autenticidade das fontes, evitando a utilização de informação proveniente de sítios não fidedignos ou potencialmente maliciosos.
- Sempre que exista dúvida quanto à segurança de um sítio eletrónico, aplicação ou plataforma digital, o colaborador deve abster-se da sua utilização até obter orientação dos serviços competentes.

Utilização de Dispositivos Móveis e Trabalho Remoto

- Sempre que sejam utilizados computadores portáteis, telemóveis, tablets ou outros dispositivos móveis para fins profissionais, os colaboradores devem assegurar a respetiva proteção física e lógica, adotando todas as medidas necessárias para impedir o acesso por pessoas não autorizadas.
- Os equipamentos disponibilizados pela Associação devem permanecer sob a guarda do colaborador, devendo ser evitado o seu abandono em veículos, locais públicos ou outros espaços suscetíveis de facilitar o furto, extravio ou acesso indevido.
- Quando o exercício de funções implique trabalho remoto ou a realização de atividades fora das instalações da Associação, os colaboradores devem assegurar que os dados pessoais e a informação institucional permanecem protegidos, adotando, designadamente, as seguintes boas práticas:
 - Trabalhar, sempre que possível, em locais que garantam a privacidade da informação;
 - Impedir que familiares, visitantes ou quaisquer terceiros visualizem documentos, ecrãs ou outra informação confidencial;
 - Evitar a utilização de redes Wi-Fi públicas ou não seguras para aceder aos sistemas da Associação;
 - Manter os equipamentos protegidos por palavra-passe, autenticação multifator ou outros mecanismos de segurança disponibilizados pela Associação;
 - Guardar os equipamentos em local seguro quando não estejam a ser utilizados;
 - Comunicar imediatamente qualquer perda, furto ou acesso indevido aos equipamentos ou à informação.
- Sempre que sejam transportados documentos em suporte físico, os colaboradores devem assegurar a sua proteção durante todo o percurso, evitando deixá-los sem vigilância ou expostos à visualização por terceiros.
- A utilização de dispositivos pessoais para tratamento de dados pessoais ou acesso aos sistemas da Associação apenas poderá ocorrer quando expressamente autorizada e de acordo com as normas internas aplicáveis.

- Os colaboradores devem assegurar que toda a informação tratada fora das instalações da Associação beneficia do mesmo nível de proteção exigido para a informação tratada nas instalações da instituição.

Armazenamento de Documentos em Servidor

- Os documentos e ficheiros digitais que contenham dados pessoais ou informação institucional devem ser armazenados, sempre que aplicável, nos servidores ou sistemas de armazenamento disponibilizados e autorizados pela Associação, de acordo com os procedimentos internos definidos para o efeito.
- Os colaboradores não devem armazenar documentos institucionais em computadores pessoais, ambientes de trabalho, dispositivos amovíveis, contas de armazenamento pessoal ou outras localizações não autorizadas pela Associação.
- O acesso às pastas e documentos armazenados no servidor deve respeitar o princípio da necessidade de conhecimento, devendo os colaboradores aceder apenas à informação necessária ao desempenho das respetivas funções.
- Os documentos devem ser organizados nas pastas e diretórios definidos pela Associação, utilizando uma estrutura que facilite a localização, gestão, atualização, conservação e eliminação da informação.
- Os colaboradores não devem criar cópias desnecessárias de documentos que contenham dados pessoais ou informação confidencial em diferentes localizações, devendo evitar a existência de versões duplicadas ou desatualizadas.
- Sempre que sejam criadas, alteradas ou eliminadas pastas ou documentos com impacto relevante na organização da informação, deverão ser observados os procedimentos internos aplicáveis e, quando necessário, solicitada orientação ao responsável pelo sistema de informação.
- A eliminação de documentos armazenados no servidor deve respeitar os prazos de conservação aplicáveis e os procedimentos definidos pela Associação, não devendo os colaboradores eliminar informação que se encontre sujeita a obrigação legal de conservação ou que seja necessária para o exercício ou defesa de direitos da Associação.

Utilização do Sistema Biométrico

- O sistema biométrico deve ser utilizado exclusivamente para as finalidades para as quais foi disponibilizado, nomeadamente o controlo de assiduidade e/ou de acesso às instalações da Associação.
- Cada trabalhador deve utilizar exclusivamente o seu próprio registo biométrico, não sendo permitido efetuar registos em nome de terceiros ou permitir que terceiros utilizem o seu registo.
- Os trabalhadores não devem tentar alterar, manipular, contornar ou interferir com o funcionamento do equipamento ou sistema biométrico.
- Qualquer erro ou anomalia no registo de entrada ou saída deve ser comunicado aos responsáveis definidos pela Associação, de forma a permitir a respetiva correção pelos meios autorizados.
- Os dados biométricos e os registos de assiduidade devem ser tratados com confidencialidade e não podem ser copiados, partilhados ou divulgados sem autorização.
- O sistema biométrico não deve ser utilizado pelos trabalhadores para qualquer finalidade diferente daquela que lhe está atribuída.
- Qualquer dúvida, incidente ou suspeita de utilização indevida do sistema deve ser comunicada à Associação ou ao responsável designado para a proteção de dados.

Impressão, Arquivo, Transporte e Eliminação Segura de Documentos

- Os documentos em suporte físico que contenham dados pessoais ou informação confidencial devem ser tratados com o mesmo nível de proteção exigido para a informação em formato

digital, assegurando a respetiva confidencialidade, integridade e disponibilidade durante todo o seu ciclo de vida.

- Os colaboradores devem imprimir apenas os documentos estritamente necessários ao desempenho das respetivas funções, evitando impressões desnecessárias ou duplicadas que possam aumentar o risco de divulgação indevida de informação.
- Após a impressão, os documentos devem ser recolhidos de imediato, não devendo permanecer nas impressoras, fotocopiadoras ou outros equipamentos de utilização comum para além do tempo estritamente necessário.
- Sempre que os documentos não estejam a ser utilizados, devem permanecer arquivados ou guardados em armários, gavetas ou outros locais adequados, de forma a impedir o acesso por pessoas não autorizadas.
- Quando seja necessário transportar documentação para fora das instalações da Associação, os colaboradores devem assegurar que os documentos permanecem protegidos durante todo o percurso, utilizando meios de transporte adequados e evitando deixá-los sem vigilância ou expostos à visualização por terceiros.
- Os documentos que contenham dados pessoais ou informação confidencial e que tenham deixado de ser necessários devem ser eliminados através dos meios definidos pela Associação, designadamente mediante destruição segura ou deposição em contentores próprios para destruição confidencial de documentos, não devendo ser descartados em recipientes destinados a resíduos comuns.
- Sempre que exista dúvida quanto ao período de conservação ou ao procedimento adequado para eliminação de documentação, o colaborador deve solicitar orientação antes de proceder à sua destruição.

Prazos de Conservação da Informação

- A Associação deve conservar os documentos e informações que contenham dados pessoais apenas durante o período necessário para o cumprimento das finalidades que justificaram a sua recolha, ou durante o período imposto por obrigação legal, regulamentar ou contratual, nos termos do artigo 9.º do Regulamento Interno de Proteção de Dados.
- Os prazos de conservação podem variar em função do tipo de documento, da finalidade do tratamento e das obrigações legais aplicáveis. Assim, a eliminação de um documento não deve ser realizada apenas com base na sua antiguidade, devendo ser considerado o respetivo contexto e finalidade.
- A título de orientação, devem ser observados os seguintes critérios:

Tipo de informação/documento	Critério de conservação
Documentação contabilística e respetivos documentos de suporte	Pelo período legalmente aplicável, designadamente o prazo de 10 anos quando previsto na legislação fiscal e contabilística
Documentação fiscal	Pelo período legalmente aplicável
Documentação de colaboradores	De acordo com os prazos aplicáveis a cada tipo de documento e com as obrigações legais em matéria laboral, fiscal e de segurança social
Processos dos utentes	De acordo com os prazos aplicáveis a cada tipo de documentação, considerando a natureza administrativa, contratual, social ou clínica da informação
Documentação clínica	Pelo período previsto na legislação aplicável à respetiva documentação

Contratos e documentação associada	Durante a vigência do contrato e pelo período adicional legalmente exigido ou necessário para o exercício ou defesa de direitos
Documentação de fornecedores e prestadores de serviços	Durante a relação contratual e pelo período adicional legalmente aplicável, nomeadamente para efeitos fiscais, contabilísticos ou de defesa de direitos
Processos de recrutamento	Pelo período necessário à finalidade do recrutamento e pelo período adicional que tenha fundamento legal ou que seja legitimamente necessário para determinada finalidade
Registos de consentimento	Enquanto forem necessários para demonstrar a obtenção e validade do consentimento e durante o período em que possam ser relevantes para a respetiva finalidade ou para o exercício/defesa de direitos
Registos de incidentes de proteção de dados e segurança da informação	Pelo período necessário à gestão e documentação do incidente e ao cumprimento das obrigações legais ou defesa de direitos
Cópias de segurança (backups)	De acordo com as regras internas de cópia de segurança e recuperação de informação, não devendo ser utilizadas como arquivo autónomo de documentos que já tenham ultrapassado o respetivo prazo de conservação

- Sempre que um documento esteja abrangido por mais do que um fundamento de conservação, deve ser mantido enquanto subsistir um fundamento válido que justifique a sua conservação.
- Sempre que exista um processo judicial, auditoria, inspeção, reclamação ou outro procedimento que possa exigir a preservação da informação, os documentos relevantes não devem ser eliminados enquanto a sua conservação for necessária para esse efeito.
- Terminando o prazo de conservação e não existindo fundamento que justifique a sua manutenção, a informação deve ser eliminada ou, quando adequado, anonimizada, através de meios que impeçam a sua recuperação ou utilização indevida.
- A eliminação deve abranger, quando aplicável, tanto os documentos em suporte físico como os ficheiros digitais e outras cópias que possam ser eliminadas de acordo com os procedimentos internos.
- Antes de eliminar um documento que contenha dados pessoais, confirme se existe um prazo legal de conservação, um processo em curso ou outra razão que justifique a sua manutenção.
- Se tiver dúvidas sobre a possibilidade de eliminar uma informação, não a elimine. Confirme primeiro com o responsável hierárquico ou com o responsável pela proteção de dados.

Conversas e Comunicação Verbal

- A comunicação verbal constitui uma forma de tratamento de dados pessoais e deve observar os mesmos princípios de confidencialidade, necessidade e reserva aplicáveis à informação em suporte físico ou digital.
- Os colaboradores devem assegurar que as conversas que envolvam dados pessoais ou informação confidencial decorrem em locais adequados, evitando a sua realização em espaços de circulação, zonas de espera, corredores, elevadores, refeitórios ou quaisquer outros locais onde possam ser ouvidas por pessoas não autorizadas.
- Sempre que prestem informações presencialmente ou por telefone, os colaboradores devem confirmar previamente a identidade e a legitimidade da pessoa que solicita a informação, garantindo que apenas são comunicados os dados estritamente necessários.

- Durante reuniões, atendimentos, consultas técnicas ou outras interações profissionais, deve ser assegurado que apenas participam as pessoas cuja presença seja necessária, preservando a privacidade dos titulares dos dados.
- Os colaboradores devem adotar um tom de voz adequado e evitar mencionar nomes, diagnósticos, situações familiares, informações clínicas ou quaisquer outros dados pessoais em locais onde possam ser escutados por terceiros.
- Sempre que exista dúvida quanto à possibilidade de divulgar determinada informação, o colaborador deve abster-se de o fazer até obter orientação do superior hierárquico ou do Encarregado da Proteção de Dados.
- O dever de confidencialidade aplica-se igualmente às conversas mantidas entre colaboradores, devendo os dados pessoais ser partilhados apenas quando tal seja necessário ao exercício das respetivas funções e de acordo com o princípio da necessidade de conhecimento.

Utilização Responsável da Inteligência Artificial e de Ferramentas Digitais

- A utilização de ferramentas de inteligência artificial, plataformas digitais e outras aplicações de apoio à atividade profissional deve respeitar a legislação aplicável, as normas internas da Associação e os princípios da proteção de dados pessoais, da confidencialidade e da segurança da informação.
- Os colaboradores apenas devem utilizar ferramentas autorizadas pela Associação ou cuja utilização seja compatível com as orientações internas em vigor, assegurando que o seu recurso não comprometa a privacidade dos titulares dos dados nem a confidencialidade da informação institucional.
- É proibida a introdução em plataformas de inteligência artificial ou noutras aplicações online de dados pessoais, informação clínica, documentos internos ou quaisquer outros conteúdos confidenciais da Associação, salvo quando exista autorização expressa e estejam reunidas as garantias técnicas e jurídicas adequadas.
- A informação produzida por ferramentas de inteligência artificial deve ser sempre analisada criticamente pelo colaborador antes da sua utilização, não dispensando a verificação da sua exatidão, atualidade, completude e conformidade com a legislação e os procedimentos internos da Associação.
- Sempre que sejam utilizadas ferramentas digitais para apoiar a redação de documentos, traduções, pesquisas ou outras tarefas profissionais, os colaboradores devem assegurar que a informação utilizada respeita os direitos de autor, a proteção dos dados pessoais e os deveres de confidencialidade a que se encontram vinculados.
- Em caso de dúvida sobre a utilização de qualquer ferramenta digital ou de inteligência artificial, o colaborador deve solicitar orientação ao superior hierárquico, ao Encarregado da Proteção de Dados ou aos serviços responsáveis pelos sistemas de informação antes da sua utilização.

Engenharia Social e Prevenção de Fraudes

- Os colaboradores devem manter uma atitude permanente de prudência perante qualquer pedido de informação, acesso a sistemas, realização de pagamentos ou divulgação de dados pessoais que apresente características invulgares ou suscite dúvidas quanto à sua legitimidade.
- A engenharia social consiste na utilização de técnicas de manipulação destinadas a induzir uma pessoa a divulgar informação confidencial, conceder acessos ou praticar atos que comprometam a segurança da informação da Associação.
- Sempre que recebam pedidos inesperados ou urgentes, os colaboradores devem confirmar a identidade do interlocutor através de um meio alternativo de contacto, abstendo-se de fornecer informação ou executar qualquer ação enquanto subsistirem dúvidas quanto à autenticidade do pedido.
- Os colaboradores devem estar particularmente atentos às seguintes situações:

- Mensagens de correio eletrónico que solicitem credenciais de acesso, dados pessoais, informações financeiras ou realização de pagamentos;
 - Chamadas telefónicas de pessoas que se apresentem como técnicos informáticos, fornecedores, entidades bancárias ou autoridades, solicitando informação confidencial;
 - Mensagens SMS ou aplicações de mensagens instantâneas contendo hiperligações ou pedidos urgentes;
 - Pedidos de alteração de contas bancárias, dados de pagamento ou instruções financeiras recebidas por correio eletrónico;
 - Pessoas desconhecidas que procurem aceder às instalações, aos sistemas informáticos ou obter informação institucional sem justificação adequada.
- Sempre que exista suspeita de fraude, tentativa de engenharia social ou qualquer outra situação suscetível de comprometer a segurança da informação, o colaborador deve interromper imediatamente a interação, preservar a evidência sempre que possível e comunicar a situação ao superior hierárquico ou aos serviços responsáveis.
- A comunicação de boa-fé de situações suspeitas constitui uma medida essencial para a prevenção de incidentes de segurança e para a proteção dos dados pessoais tratados pela Associação.

Comunicação e Gestão de Incidentes de Segurança

- Todos os colaboradores têm o dever de comunicar, de forma imediata, qualquer incidente ou suspeita de incidente suscetível de comprometer a proteção dos dados pessoais, a segurança da informação ou o normal funcionamento dos sistemas da Associação.
- Constituem, entre outras, situações que devem ser comunicadas:
 - Perda, furto ou extravio de computadores, telemóveis, tablets, dispositivos de armazenamento ou documentação em suporte físico;
 - Envio de mensagens de correio eletrónico para destinatários incorretos;
 - Divulgação accidental de dados pessoais;
 - Acesso não autorizado a informação ou sistemas informáticos;
 - Receção de mensagens de correio eletrónico ou outras comunicações suspeitas de fraude;
 - Detecção de software malicioso, comportamentos anómalos dos equipamentos ou falhas de segurança;
 - Qualquer outra situação que possa colocar em risco a confidencialidade, integridade ou disponibilidade da informação.
- Perante um incidente ou suspeita de incidente, o colaborador deve:
 - Comunicar imediatamente a ocorrência ao superior hierárquico ou ao Encarregado da Proteção de Dados;
 - Facultar toda a informação disponível sobre a situação, indicando, sempre que possível, a data, hora, natureza do incidente e os dados potencialmente envolvidos;
 - Colaborar na adoção das medidas necessárias para conter o incidente, minimizar os seus efeitos e apoiar a respetiva investigação;
 - Abster-se de eliminar documentos, mensagens de correio eletrónico, ficheiros ou outros elementos que possam constituir evidência do incidente, salvo orientação em contrário.
- A comunicação tempestiva de um incidente constitui um dever de todos os colaboradores e representa um contributo essencial para a proteção dos titulares dos dados, para a redução dos impactos da ocorrência e para o cumprimento das obrigações legais da Associação.

Formação, Sensibilização e Responsabilidade dos Colaboradores

- A proteção dos dados pessoais e da segurança da informação constitui uma responsabilidade partilhada por todos os colaboradores da Associação, independentemente das funções que desempenham ou do vínculo contratual que mantenham com a instituição.
- A Associação compromete-se a promover ações de formação, sensibilização e atualização periódica sobre proteção de dados pessoais, segurança da informação, cibersegurança e boas práticas no tratamento da informação, procurando assegurar que todos os colaboradores dispõem dos conhecimentos necessários ao desempenho das suas funções.
- Os colaboradores comprometem-se a participar nas ações de formação promovidas pela Associação e a aplicar, no exercício das suas funções, os conhecimentos adquiridos, contribuindo para a melhoria contínua das práticas de proteção de dados e segurança da informação.
- Sempre que sejam introduzidos novos procedimentos, sistemas de informação, ferramentas tecnológicas ou alterações legislativas relevantes, a Associação poderá promover ações de sensibilização complementares, de forma a garantir a sua correta implementação.
- Os colaboradores devem manter uma atitude proativa na identificação de riscos, na comunicação de incidentes e na adoção de comportamentos responsáveis, contribuindo para a criação de uma cultura organizacional assente na privacidade, na confidencialidade e na proteção da informação.
- O incumprimento das normas constantes do presente Manual, da Política de Proteção de Dados Pessoais, das demais normas internas da Associação ou da legislação aplicável poderá dar origem à adoção das medidas disciplinares, contratuais ou legais consideradas adequadas, sem prejuízo da eventual responsabilidade civil, contraordenacional ou criminal que ao caso couber.

Entrada em Vigor

- O presente Manual de Boas Práticas de Proteção de Dados Pessoais e Segurança da Informação entra em vigor na data da sua aprovação pela Direção da Associação, sendo aplicável a todos os colaboradores, independentemente da natureza do respetivo vínculo ou das funções exercidas.
- A Associação compromete-se a disponibilizar o presente Manual a todos os colaboradores, promovendo a sua divulgação, atualização periódica e integração nas ações de acolhimento, formação e sensibilização interna.
- O presente Manual deverá ser interpretado em articulação com a Política de Proteção de Dados Pessoais aplicável aos Colaboradores, a Política de Proteção de Dados Pessoais aplicável aos Utentes, Familiares e Representantes Legais, a Política de Proteção de Dados Pessoais aplicável aos Subcontratantes e demais normas internas da Associação, sem prejuízo da aplicação do Regulamento (UE) 2016/679, da Lei n.º 58/2019 e da restante legislação aplicável em matéria de proteção de dados pessoais e segurança da informação.
- Sempre que ocorram alterações legislativas, regulamentares, organizacionais ou tecnológicas que o justifiquem, o presente Manual será objeto de revisão, garantindo a sua permanente adequação às necessidades da Associação e às melhores práticas de proteção de dados e segurança da informação.

Aprovado por deliberação da Direção, exarada na Ata da Direção n.º 54, de 24 de setembro de 2026



Living
Care

Política Interna
Proteção de Dados Pessoais – Colaboradores

Setembro 2026

Introdução

A proteção dos dados pessoais constitui um compromisso permanente da Associação Living Care e um elemento essencial da relação de confiança estabelecida com os seus utentes, familiares, representantes legais, colaboradores, parceiros e demais titulares dos dados.

No exercício da sua atividade, a Associação trata diariamente informação de natureza pessoal, incluindo, em muitas situações, categorias especiais de dados, designadamente dados relativos à saúde, cuja utilização exige elevados padrões de responsabilidade, confidencialidade, segurança e respeito pelos direitos fundamentais das pessoas.

Neste contexto, a proteção de dados pessoais não constitui apenas uma obrigação legal decorrente do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – RGPD), da Lei n.º 58/2019, de 8 de agosto, e demais legislação aplicável. Representa igualmente um compromisso ético e institucional que deve orientar a atuação de todos aqueles que exercem funções na Associação.

A presente Política estabelece os princípios, deveres e regras de atuação aplicáveis aos colaboradores no tratamento de dados pessoais, promovendo uma cultura organizacional assente na responsabilidade, na integridade, na confidencialidade da informação e na adoção de boas práticas de proteção de dados.

Este documento complementa o Regulamento de Proteção de Dados Pessoais da Associação e deve ser interpretado em articulação com as restantes políticas, procedimentos internos e orientações adotadas em matéria de proteção de dados, segurança da informação e confidencialidade.

Objeto

- A presente Política estabelece os princípios, normas de atuação e deveres aplicáveis aos colaboradores da Associação relativamente ao tratamento de dados pessoais realizado no exercício das respetivas funções, assegurando o cumprimento do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – RGPD), da Lei n.º 58/2019, de 8 de agosto, e demais legislação nacional e europeia aplicável em matéria de proteção de dados pessoais.
- A presente Política tem como finalidade promover uma cultura organizacional assente na responsabilidade, na confidencialidade, na segurança da informação, na integridade dos dados pessoais e no respeito pelos direitos e liberdades dos respetivos titulares, estabelecendo regras de atuação que contribuam para a prevenção de riscos e para o cumprimento das obrigações legais e institucionais em matéria de proteção de dados.
- A presente Política complementa o Regulamento de Proteção de Dados Pessoais da Associação e deve ser aplicada em articulação com as restantes políticas, procedimentos internos e orientações adotadas pela instituição no domínio da proteção de dados pessoais e da segurança da informação.

Âmbito de Aplicação

- A presente Política aplica-se a todos os colaboradores da Associação, independentemente da natureza do respetivo vínculo jurídico ou da função desempenhada, incluindo membros dos órgãos sociais, trabalhadores, dirigentes, estagiários, voluntários, prestadores de atividade regular e quaisquer outras pessoas que, no exercício das suas funções ou colaboração com a Associação, tenham acesso a dados pessoais tratados pela instituição.
- As disposições constantes da presente Política aplicam-se a todas as operações de tratamento de dados pessoais realizadas no âmbito da atividade da Associação, independentemente do suporte

utilizado, designadamente em formato físico, digital, audiovisual ou qualquer outro meio suscetível de armazenar, consultar, transmitir ou tratar informação.

- Todos os colaboradores abrangidos pela presente Política devem conhecer, respeitar e cumprir as regras nela previstas, contribuindo para a proteção dos dados pessoais e para a salvaguarda da privacidade dos respetivos titulares.

Princípios Gerais

- Os colaboradores devem tratar os dados pessoais de forma lícita, leal, transparente e responsável, exclusivamente para o exercício das funções que lhes estejam atribuídas e apenas na medida do estritamente necessário ao respetivo desempenho, respeitando os princípios da minimização dos dados, da exatidão, da limitação das finalidades, da integridade, da confidencialidade e da responsabilidade.
- O acesso aos dados pessoais deve obedecer ao princípio da necessidade de conhecer, sendo permitido apenas aos colaboradores cuja intervenção seja necessária ao exercício das respetivas funções e estritamente limitado à informação indispensável para o desempenho das suas responsabilidades.
- No exercício das suas funções, os colaboradores devem atuar com diligência, profissionalismo, sentido de responsabilidade e respeito pela privacidade dos utentes, familiares, representantes legais, colaboradores, candidatos a emprego, fornecedores, parceiros e demais titulares dos dados pessoais, contribuindo para uma cultura organizacional assente na proteção da informação e na confiança institucional.

Dever de Confidencialidade

- Os colaboradores estão sujeitos ao dever de confidencialidade relativamente a todos os dados pessoais e demais informações de natureza pessoal ou sensível a que tenham acesso no exercício das suas funções, comprometendo-se a utilizá-los exclusivamente para o desempenho das atividades que lhes estejam confiadas.
- O dever de confidencialidade aplica-se independentemente da forma de acesso à informação, do respetivo suporte ou da natureza do vínculo existente com a Associação, abrangendo toda a informação obtida no âmbito da atividade profissional, ainda que não constitua dado pessoal nos termos da legislação aplicável.
- Os colaboradores devem adotar uma postura de permanente reserva e discrição relativamente à informação a que tenham acesso, abstenendo-se de consultar, divulgar, reproduzir, transmitir ou utilizar dados pessoais sem autorização ou para finalidades alheias ao exercício das respetivas funções.
- O dever de confidencialidade mantém-se após a cessação das funções ou da relação estabelecida com a Associação, independentemente da respetiva causa, permanecendo os colaboradores obrigados a preservar a privacidade e a confidencialidade da informação de que tenham tomado conhecimento durante o exercício da sua atividade.

Utilização Adequada dos Dados Pessoais

- Os colaboradores devem utilizar os dados pessoais exclusivamente para o exercício das funções que lhes estejam atribuídas e apenas para as finalidades legítimas relacionadas com a prestação de cuidados, o acompanhamento dos utentes, a gestão administrativa, o cumprimento de obrigações legais ou outras atividades desenvolvidas pela Associação no âmbito da sua missão.

- O acesso aos dados pessoais deve limitar-se à informação estritamente necessária ao desempenho das respetivas funções, sendo proibida a consulta, utilização, reprodução, alteração, transmissão ou divulgação de dados pessoais sem fundamento legítimo ou para fins alheios à atividade profissional.
- Os colaboradores devem assegurar que os dados pessoais tratados são exatos, atualizados e adequados às finalidades que justificam o respetivo tratamento, comunicando aos serviços competentes quaisquer inexactidões ou necessidades de atualização de que tenham conhecimento no exercício das suas funções.
- Sempre que o tratamento de dados pessoais suscite dúvidas quanto à sua licitude, finalidade ou forma de execução, os colaboradores devem solicitar orientação aos seus superiores hierárquicos ou ao Encarregado da Proteção de Dados antes de proceder ao respetivo tratamento.

Utilização dos Sistemas de Informação e Recursos da Associação

- Os sistemas de informação, equipamentos informáticos, aplicações, plataformas digitais, contas de utilizador e demais recursos tecnológicos disponibilizados pela Associação destinam-se exclusivamente ao exercício das funções profissionais dos colaboradores e devem ser utilizados de forma responsável, diligente e em conformidade com a legislação aplicável e com as normas internas em vigor.
- Os colaboradores devem adotar comportamentos que garantam a segurança da informação e a proteção dos dados pessoais, designadamente através da utilização adequada das credenciais de acesso, da proteção dos equipamentos sob a sua responsabilidade e da prevenção de acessos não autorizados aos sistemas de informação.
- Sempre que utilizem documentos físicos ou digitais contendo dados pessoais, os colaboradores devem assegurar a respetiva proteção contra perda, extravio, destruição, alteração, divulgação ou acesso indevido, adotando as medidas de segurança adequadas à natureza da informação tratada.
- É proibida a instalação de aplicações no telemóvel, computador e/ou tablet, a utilização de equipamentos ou suportes informáticos não autorizados, bem como a utilização dos sistemas da Associação para fins ilícitos ou suscetíveis de comprometer a segurança da informação ou a proteção dos dados pessoais.
- As regras específicas relativas à utilização dos sistemas de informação, equipamentos, correio eletrónico, dispositivos móveis, palavras-passe e demais recursos tecnológicos constam do Manual de Boas Práticas de Proteção de Dados e Segurança da Informação da Associação, cuja observância é obrigatória para todos os colaboradores.

Boas Práticas de Proteção de Dados Pessoais

- Os colaboradores devem adotar, no exercício das suas funções, comportamentos diligentes e responsáveis que contribuam para a proteção dos dados pessoais e para a segurança da informação, atuando sempre de forma a prevenir situações de perda, alteração, destruição, divulgação ou acesso não autorizado.
- No tratamento de dados pessoais, os colaboradores devem assegurar que a informação é utilizada exclusivamente para fins profissionais legítimos, evitando a exposição desnecessária de

documentos ou equipamentos, bem como qualquer prática suscetível de comprometer a confidencialidade, a integridade ou a disponibilidade da informação.

- Os documentos em suporte físico ou digital que contenham dados pessoais devem ser conservados de forma segura, sendo adotadas as medidas adequadas para impedir o acesso por pessoas não autorizadas durante a sua utilização, armazenamento, transporte ou eliminação.
- Os colaboradores devem cumprir as orientações, procedimentos e boas práticas definidas pela Associação em matéria de proteção de dados pessoais e segurança da informação, participando ativamente na promoção de uma cultura organizacional assente na responsabilidade, na prevenção do risco e na melhoria contínua.

Comunicação de Incidentes e Violações de Dados Pessoais

- Todos os colaboradores têm o dever de comunicar imediatamente qualquer incidente de segurança, violação de dados pessoais ou suspeita fundada da sua ocorrência de que tenham conhecimento no exercício das suas funções, independentemente da sua origem ou dimensão.
- A comunicação deve ser efetuada através dos canais internos definidos pela Associação, facultando toda a informação disponível que permita identificar a natureza do incidente, os dados pessoais envolvidos, os titulares potencialmente afetados, as consequências previsíveis e as medidas já adotadas para limitar os seus efeitos.
- Sempre que aplicável, a comunicação deverá ser dirigida ao superior hierárquico e ao Encarregado da Proteção de Dados, através do endereço eletrónico dpo@livingcare.pt, devendo os colaboradores prestar toda a colaboração necessária para a investigação, contenção, mitigação e resolução do incidente.
- Nenhum colaborador poderá ocultar, omitir ou retardar injustificadamente a comunicação de incidentes suscetíveis de comprometer a proteção dos dados pessoais, devendo atuar com diligência e sentido de responsabilidade na salvaguarda dos direitos dos titulares dos dados e dos interesses da Associação.

Direitos dos Titulares dos Dados

- Os colaboradores devem respeitar e salvaguardar os direitos dos titulares dos dados pessoais, assegurando que qualquer pedido relacionado com o exercício dos direitos previstos na legislação aplicável em matéria de proteção de dados pessoais é tratado de forma diligente, confidencial e em conformidade com os procedimentos internos da Associação.
- Sempre que recebam um pedido de exercício de direitos por parte de um titular dos dados, os colaboradores devem encaminhá-lo, com a maior brevidade, para o superior hierárquico ou para o Encarregado da Proteção de Dados, abstendo-se de responder autonomamente, salvo quando tal resulte das funções que lhes estejam atribuídas ou de instruções expressamente transmitidas pela Associação.
- Os colaboradores devem prestar toda a colaboração necessária à Associação para assegurar o cumprimento dos prazos legais e das obrigações decorrentes do exercício dos direitos dos titulares dos dados, facultando, sempre que solicitado, as informações necessárias à respetiva tramitação.
- Os pedidos relativos ao exercício dos direitos dos titulares dos dados ou quaisquer questões relacionadas com a proteção de dados pessoais podem ser encaminhados para o Encarregado da Proteção de Dados, através do endereço eletrónico dpo@livingcare.pt.

Formação e Sensibilização

- A Associação promove ações de formação, sensibilização e divulgação de boas práticas em matéria de proteção de dados pessoais e segurança da informação, com o objetivo de assegurar que os colaboradores conhecem as suas responsabilidades e adotam comportamentos conformes com a legislação aplicável e com as normas internas em vigor.
- Os colaboradores comprometem-se a participar nas ações de formação promovidas pela Associação, bem como a manter-se informados sobre as orientações, procedimentos e demais instrumentos internos relacionados com a proteção de dados pessoais e a segurança da informação.
- Sempre que sejam introduzidas alterações legislativas, organizacionais ou tecnológicas suscetíveis de afetar o tratamento de dados pessoais, a Associação promoverá, sempre que se revele adequado, ações de atualização ou reforço da sensibilização, visando assegurar a melhoria contínua das práticas de proteção de dados.
- A promoção de uma cultura de proteção de dados pessoais constitui uma responsabilidade partilhada por todos os colaboradores, devendo cada um contribuir, no exercício das suas funções, para a prevenção de riscos, para a proteção da privacidade dos titulares dos dados e para o cumprimento das obrigações legais e institucionais da Associação.

Incumprimento

- O incumprimento das disposições constantes da presente Política, do Regulamento de Proteção de Dados Pessoais da Associação e das demais normas internas aplicáveis em matéria de proteção de dados pessoais e segurança da informação poderá determinar a adoção das medidas consideradas adequadas, nos termos da legislação em vigor e dos instrumentos internos da Associação.
- Sem prejuízo da eventual responsabilidade civil, contraordenacional ou criminal prevista na lei, o incumprimento das obrigações decorrentes da presente Política poderá constituir infração disciplinar, sempre que tal resulte da atuação dolosa ou negligente do colaborador e nos termos legalmente aplicáveis.
- Sempre que seja detetado qualquer incumprimento, a Associação promoverá a respetiva análise, adotando as medidas corretivas e preventivas que se revelem adequadas, com vista à mitigação dos riscos, à proteção dos direitos dos titulares dos dados e à prevenção da repetição de situações semelhantes.
- A aplicação das medidas previstas no presente artigo observará os princípios da proporcionalidade, da legalidade e do contraditório, garantindo o respeito pelos direitos dos colaboradores e pelas normas legais aplicáveis.

Entrada em Vigor

- A presente Política entra em vigor na data da sua aprovação pela Direção da Associação, sendo disponibilizada a todos os colaboradores no momento da admissão e sempre que ocorram alterações relevantes ao seu conteúdo.

- A Associação compromete-se a assegurar a divulgação, atualização e acessibilidade da presente Política, promovendo o seu conhecimento por todos os colaboradores e incentivando o cumprimento das regras, princípios e procedimentos nela estabelecidos.
- O cumprimento da presente Política constitui parte integrante dos deveres profissionais dos colaboradores, devendo a sua atuação pautar-se pelos princípios da licitude, responsabilidade, confidencialidade, integridade, transparência e respeito pelos direitos dos titulares dos dados pessoais.
- A presente Política complementa o Regulamento de Proteção de Dados Pessoais da Associação e deve ser interpretada em articulação com as restantes políticas, procedimentos internos e demais instrumentos de gestão adotados em matéria de proteção de dados pessoais e segurança da informação.

Aprovado por deliberação da Direção, exarada na Ata da Direção n.º 54, de 24 de setembro de 2026



Living
Care

Política Interna
Proteção de Dados Pessoais – Subcontratantes

Setembro 2026

Introdução

A proteção dos dados pessoais constitui um compromisso permanente da Associação Living Care e um elemento essencial da relação de confiança estabelecida com os seus utentes, familiares, representantes legais, colaboradores, parceiros e demais titulares dos dados.

No desenvolvimento da sua atividade, a Associação recorre a entidades externas para a prestação de serviços que, pela sua natureza, podem implicar o acesso a dados pessoais ou a realização de operações de tratamento por conta da instituição. Nestes casos, é essencial assegurar que os subcontratantes atuam em conformidade com os princípios, regras e obrigações estabelecidos pelo Regulamento Geral sobre a Proteção de Dados (RGPD), pela legislação nacional aplicável e pelas normas internas da Associação.

A presente Política define os princípios e as regras que devem ser observados por todos os subcontratantes no âmbito do tratamento de dados pessoais realizado por conta da Associação, promovendo uma atuação responsável, transparente e orientada para a proteção dos direitos e liberdades dos titulares dos dados.

A Associação considera que a proteção dos dados pessoais constitui uma responsabilidade partilhada. Neste sentido, exige que todos os subcontratantes adotem elevados padrões de confidencialidade, segurança da informação e conformidade legal, contribuindo para uma cultura organizacional assente na confiança, na ética e no respeito pela privacidade.

Objeto

- A presente Política estabelece os princípios, regras e procedimentos aplicáveis ao tratamento de dados pessoais efetuado pelos subcontratantes que prestem serviços à Associação, assegurando o cumprimento do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – RGPD), da Lei n.º 58/2019, de 8 de agosto, e da demais legislação nacional e europeia aplicável em matéria de proteção de dados pessoais.
- A presente Política define as obrigações que impendem sobre os subcontratantes relativamente à confidencialidade, segurança, integridade e proteção dos dados pessoais a que tenham acesso ou que tratem por conta da Associação, no âmbito da execução dos serviços contratados.

Âmbito de Aplicação

- A presente Política aplica-se a todas as pessoas singulares ou coletivas que prestem serviços à Associação na qualidade de subcontratantes e que, no âmbito da respetiva atividade, tratem dados pessoais por conta da Associação ou tenham acesso, direto ou indireto, a dados pessoais necessários à execução dos serviços contratados.
- Encontram-se abrangidos pela presente Política, designadamente, os prestadores de serviços de informática, contabilidade, medicina, enfermagem, fisioterapia, psicologia, manutenção, limpeza, segurança, transporte, consultoria, apoio domiciliário, formação e quaisquer outros cuja atividade implique o tratamento ou o acesso a dados pessoais de utentes, familiares, representantes legais, colaboradores, candidatos a emprego, fornecedores, visitantes ou outros titulares dos dados.

Princípios do Tratamento de Dados Pessoais

- Os subcontratantes comprometem-se a tratar os dados pessoais exclusivamente de acordo com as instruções documentadas da Associação e em conformidade com os princípios da licitude,

lealdade e transparência, da limitação das finalidades, da minimização dos dados, da exatidão, da limitação do período de conservação, da integridade e confidencialidade e da responsabilização, adotando as medidas necessárias para assegurar a proteção dos direitos e liberdades dos titulares dos dados.

- Os dados pessoais não podem, em caso algum, ser utilizados para fins próprios do subcontratante ou para qualquer finalidade diferente daquela que fundamentou o respetivo tratamento por conta da Associação.

Obrigações dos Subcontratantes

- Os subcontratantes devem tratar os dados pessoais apenas na medida do estritamente necessário à execução dos serviços contratados e em conformidade com as instruções da Associação, abstendo-se de utilizar, divulgar, comunicar ou tratar esses dados para qualquer finalidade não autorizada.
- Os subcontratantes devem assegurar que apenas os colaboradores, trabalhadores, prestadores de serviços ou representantes que necessitem de aceder aos dados pessoais para o exercício das respetivas funções tenham acesso aos mesmos, adotando mecanismos de controlo de acessos adequados à natureza, sensibilidade e risco associado aos dados tratados.
- Sempre que solicitado pela Associação, os subcontratantes devem facultar as informações e evidências necessárias para demonstrar o cumprimento das obrigações decorrentes da presente Política, da legislação aplicável e das instruções que lhes tenham sido transmitidas no âmbito da execução dos serviços contratados.

Dever de Confidencialidade

- Os subcontratantes encontram-se vinculados ao dever de confidencialidade relativamente a todos os dados pessoais e demais informações a que tenham acesso no âmbito da execução dos serviços contratados, comprometendo-se a assegurar que os seus colaboradores, trabalhadores, representantes e quaisquer outras pessoas autorizadas a tratar dados pessoais se encontram igualmente sujeitos a um dever de confidencialidade de igual alcance.
- O dever de confidencialidade mantém-se mesmo após a cessação da relação contratual com a Associação, independentemente da causa que lhe tenha dado origem.

Medidas Técnicas e Organizativas de Segurança

- Os subcontratantes devem implementar medidas técnicas e organizativas adequadas para assegurar um nível de segurança apropriado ao risco associado ao tratamento dos dados pessoais, tendo em consideração a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos para os direitos e liberdades dos titulares dos dados. Sempre que estejam em causa categorias especiais de dados pessoais, designadamente dados relativos à saúde, devem ser adotadas medidas de proteção reforçadas.
- As medidas de segurança implementadas podem incluir, consoante a natureza dos serviços prestados e os riscos identificados, mecanismos de autenticação e controlo de acessos, utilização de palavras-passe robustas, proteção contra software malicioso, atualização regular dos sistemas informáticos, realização de cópias de segurança, proteção física dos equipamentos, cifragem da informação quando tecnicamente adequada e quaisquer outras medidas destinadas a prevenir a destruição, perda, alteração, divulgação ou acesso não autorizado aos dados pessoais.

Tratamento de Categorias Especiais de Dados

- Sempre que, no âmbito da prestação dos serviços, os subcontratantes procedam ao tratamento de categorias especiais de dados pessoais, designadamente dados relativos à saúde dos utentes,

devem assegurar um nível reforçado de proteção, garantindo que o acesso a essa informação é limitado aos profissionais cuja intervenção seja estritamente necessária para a execução dos serviços contratados.

- Os subcontratantes comprometem-se a observar deveres reforçados de confidencialidade, reserva e sigilo relativamente a estas categorias de dados, abstendo-se de aceder, utilizar, reproduzir, conservar, comunicar ou divulgar essa informação para além do estritamente necessário ao cumprimento das obrigações contratuais e das instruções transmitidas pela Associação.

Recursos a Outros Subcontratantes

- Os subcontratantes não podem recorrer a terceiros para tratar dados pessoais por conta da Associação sem autorização prévia, expressa e escrita desta.
- Sempre que seja autorizada a subcontratação, o subcontratante deve assegurar que o novo subcontratante assume obrigações equivalentes às previstas na presente Política, no contrato celebrado com a Associação e na legislação aplicável em matéria de proteção de dados pessoais, mantendo-se responsável perante a Associação pelo cumprimento dessas obrigações.

Captação e Divulgação de Imagens e Informação

- Com o objetivo de salvaguardar a privacidade e a dignidade de todos os utentes, não é permitida a captação, gravação ou divulgação de imagens, vídeos ou registos áudio de outros utentes, colaboradores, prestadores de serviços ou visitantes sem o consentimento dos respetivos titulares ou sem outro fundamento legal que legitime esse tratamento.
- A publicação de fotografias, vídeos ou quaisquer dados pessoais ou elementos da vida privada dos utentes nas redes sociais ou noutros meios de comunicação deve respeitar os direitos de personalidade, a legislação aplicável e os princípios da dignidade, privacidade e confidencialidade.
- A Associação poderá proceder à recolha e utilização de imagens para fins institucionais, de comunicação, divulgação das suas atividades ou memória institucional, desde que exista fundamento de licitude adequado, nomeadamente o consentimento, sempre que este seja legalmente exigido.
- A Associação reserva-se o direito de solicitar a interrupção da captação de imagens ou da gravação de áudio e vídeo sempre que tal seja necessário para proteger a privacidade, a dignidade ou os direitos dos utentes, colaboradores, visitantes ou demais pessoas presentes nas suas instalações.

Conservação dos Dados Pessoais

- Os dados pessoais serão conservados apenas durante o período necessário ao cumprimento das finalidades que justificaram a sua recolha ou durante os prazos legalmente estabelecidos para o cumprimento de obrigações legais, regulamentares ou contratuais.
- Decorrido o respetivo período de conservação, os dados pessoais serão eliminados ou anonimizados de forma segura, sem prejuízo das situações em que a sua conservação seja exigida por disposição legal ou por decisão da autoridade competente.

Violação de Dados Pessoais

- Qualquer violação de dados pessoais, ou suspeita fundada da sua ocorrência, deve ser comunicada imediatamente à Associação, facultando toda a informação disponível que permita identificar a natureza do incidente, os dados pessoais envolvidos, os titulares potencialmente

afetados, as consequências previsíveis e as medidas adotadas ou propostas para conter e mitigar os seus efeitos.

- A comunicação deve ser efetuada através dos contactos disponibilizados pela Associação, designadamente junto do Encarregado da Proteção de Dados, através do endereço eletrónico dpo@livingcare.pt.
- Os subcontratantes comprometem-se a colaborar ativamente com a Associação na investigação, contenção, mitigação e resolução de qualquer violação de dados pessoais, disponibilizando todas as informações e o apoio necessários ao cumprimento das obrigações legais aplicáveis.

Direitos dos Titulares dos Dados

- Sempre que um titular dos dados exerça qualquer direito previsto na legislação aplicável em matéria de proteção de dados pessoais junto do subcontratante, este deve remeter imediatamente o respetivo pedido à Associação, não podendo responder diretamente ao titular dos dados, salvo quando tal lhe seja expressamente autorizado pela Associação ou resulte de obrigação legal.
- Os subcontratantes comprometem-se a prestar toda a colaboração necessária à Associação para assegurar o cumprimento dos prazos legais e das obrigações decorrentes do exercício dos direitos dos titulares dos dados, facultando as informações e o apoio necessários à respetiva tramitação.

Conservação, Devolução e Eliminação dos Dados

- Terminada a prestação dos serviços ou cessada a relação contratual, os subcontratantes devem proceder, de acordo com as instruções transmitidas pela Associação, à devolução ou eliminação de todos os dados pessoais tratados por sua conta, incluindo quaisquer cópias existentes, salvo quando a respetiva conservação resulte de obrigação legal.
- Sempre que tal lhe seja solicitado pela Associação, o subcontratante deve comprovar a devolução ou a eliminação segura dos dados pessoais, através dos meios considerados adequados para esse efeito.

Auditoria e Verificação do Cumprimento

- A Associação pode, sempre que o considere necessário, solicitar aos subcontratantes informações, documentos ou outras evidências que permitam verificar o cumprimento das obrigações decorrentes da presente Política, da legislação aplicável e das instruções transmitidas no âmbito da execução dos serviços contratados.
- Os subcontratantes comprometem-se a colaborar de boa-fé nas ações de verificação promovidas pela Associação, facultando os elementos solicitados e adotando, sempre que aplicável, as medidas corretivas que se revelem necessárias para assegurar a conformidade com as obrigações em matéria de proteção de dados pessoais.

Incumprimento

- O incumprimento das disposições constantes da presente Política ou da legislação aplicável em matéria de proteção de dados pessoais pode determinar a adoção das medidas contratuais e legais que se revelem adequadas, incluindo, quando aplicável, a resolução do contrato, a exigência de indemnização pelos prejuízos causados e a comunicação da situação às autoridades competentes, sempre que tal resulte de obrigação legal.

Entrada em Vigor

- A presente Política entra em vigor na data da sua aprovação pela Direção da Associação, sendo aplicável e de cumprimento obrigatório por todos os subcontratantes que, por qualquer forma, tratem dados pessoais por conta da Associação.
- A prestação de serviços à Associação pressupõe o conhecimento e a aceitação das disposições constantes da presente Política, sem prejuízo da celebração de Acordo de Tratamento de Dados Pessoais, sempre que tal seja legalmente exigido ou contratualmente aplicável.

Aprovado por deliberação da Direção, exarada na Ata da Direção n.º 54, de 24 de setembro de 2026



Living
Care

Política Interna
**Proteção de Dados Pessoais – Utentes, Familiares e
Representantes Legais**

Setembro 2026

Introdução

A Associação Living Care tem como missão prestar cuidados e serviços de elevada qualidade, promovendo o bem-estar, a dignidade, a autonomia e a qualidade de vida dos seus utentes. No desenvolvimento desta missão, o tratamento de dados pessoais constitui uma componente indispensável à prestação de cuidados seguros, personalizados e adequados às necessidades de cada pessoa.

A proteção da privacidade e dos dados pessoais é, por isso, entendida pela Associação como um compromisso permanente e um elemento essencial da relação de confiança estabelecida com os utentes, familiares, representantes legais e demais pessoas com quem se relaciona.

A presente Política de Proteção de Dados Pessoais tem como finalidade informar, de forma clara e transparente, sobre a forma como a Associação recolhe, utiliza, conserva, protege e, quando legalmente admissível, comunica os dados pessoais tratados no âmbito da sua atividade.

Objeto

- A presente Política de Proteção de Dados Pessoais estabelece os princípios orientadores aplicáveis ao tratamento de dados pessoais dos utentes, familiares, representantes legais, pessoas de referência e demais titulares dos dados no âmbito da atividade desenvolvida pela Associação.
- A Política complementa o Regulamento Interno de Proteção de Dados Pessoais da Associação, sendo aplicada em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados- RGPD), com a Lei n.º 58/2019, de 8 de agosto, e demais legislação aplicável.

Âmbito de Aplicação

- A presente Política aplica-se ao tratamento de dados pessoais efetuado pela Associação no âmbito da prestação de cuidados e serviços, do acompanhamento social e clínico, da gestão administrativa, do cumprimento de obrigações legais e de todas as demais atividades relacionadas com a sua missão e funcionamento.
- É aplicável aos dados pessoais dos utentes, familiares, representantes legais, pessoas de referência, contactos de emergência e demais pessoas singulares cujos dados sejam tratados pela Associação no exercício da sua atividade.
- Abrange todas as operações de tratamento de dados pessoais, independentemente de serem realizadas em suporte físico ou digital, através de meios automatizados ou não automatizados.
- Articula-se com o Regulamento Interno de Proteção de Dados Pessoais e com as demais políticas e procedimentos internos da Associação em matéria de proteção de dados, segurança da informação e confidencialidade.

Princípios do Tratamento de Dados Pessoais

- A Associação trata os dados pessoais dos utentes, familiares e representantes legais com respeito pela sua privacidade, dignidade e direitos fundamentais, assegurando que todas as operações de tratamento são realizadas de forma lícita, leal, transparente e segura.
- No tratamento dos dados pessoais, a Associação compromete-se a:

- Recolher apenas os dados pessoais necessários à prestação dos cuidados e serviços, ao cumprimento das suas obrigações legais e à prossecução das finalidades para que foram recolhidos;
- Utilizar os dados pessoais exclusivamente para finalidades legítimas e previamente determinadas;
- Assegurar que os dados pessoais são exatos e, sempre que necessário, atualizados;
- Adotar medidas técnicas e organizativas adequadas para proteger os dados pessoais contra o acesso, utilização, alteração, divulgação ou destruição não autorizados;
- Conservar os dados pessoais apenas durante o período necessário ao cumprimento das finalidades que justificaram a sua recolha ou durante os prazos legalmente aplicáveis;
- Garantir o respeito pelos direitos dos titulares dos dados, promovendo uma atuação responsável, transparente e em conformidade com a legislação em vigor.

Dados Pessoais Tratados

- A Associação recolhe e trata apenas os dados pessoais estritamente necessários para prestar os cuidados e serviços solicitados, cumprir as suas obrigações legais e assegurar o adequado acompanhamento dos utentes.
- Em função da natureza dos serviços prestados, poderão ser tratados, designadamente, os seguintes dados pessoais:
 - Dados de identificação;
 - Dados de contacto;
 - Dados relativos aos familiares, representantes legais, pessoas de referência ou contactos de emergência;
 - Dados administrativos, fiscais e financeiros necessários à gestão da relação estabelecida com a Associação;
 - Dados relativos à saúde e outras informações indispensáveis à prestação de cuidados, apoio social e acompanhamento individualizado do utente;
 - Outros dados cuja recolha seja exigida por disposição legal ou necessária ao cumprimento das finalidades para as quais foram recolhidos.
- Sempre que a legislação o exija ou o tratamento dependa do consentimento do utente ou do seu representante legal, a Associação prestará previamente toda a informação necessária para que a decisão seja tomada de forma livre, específica, informada e inequívoca.

Finalidades do Tratamento

- Os dados pessoais recolhidos pela Associação são tratados exclusivamente para finalidades determinadas, explícitas e legítimas, designadamente para:
 - Assegurar a admissão, acolhimento, prestação de cuidados e acompanhamento dos utentes;
 - Elaborar, executar e acompanhar o plano individual de cuidados e demais instrumentos de intervenção técnica;
 - Garantir a gestão administrativa, financeira e contratual da relação estabelecida com os utentes e respetivos representantes legais;
 - Cumprir obrigações legais, regulamentares e contratuais a que a Associação se encontre vinculada;
 - Assegurar a comunicação com os utentes, familiares, representantes legais, pessoas de referência e contactos de emergência, sempre que necessário;

- Promover a qualidade, a segurança e a melhoria contínua dos cuidados e serviços prestados;
- Exercer direitos, cumprir deveres e defender interesses legítimos da Associação, dos utentes ou de terceiros, quando legalmente admissível;
- Prosseguir outras finalidades compatíveis com aquelas que justificaram a recolha dos dados, sempre nos termos da legislação aplicável.

Confidencialidade e Segurança da Informação

- A Associação adota medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, perda, alteração, divulgação ou acesso não autorizado, bem como contra qualquer outra forma de tratamento ilícito.
- O acesso aos dados pessoais é limitado aos colaboradores, prestadores de serviços e demais pessoas devidamente autorizadas que necessitem dessa informação para o exercício das respetivas funções, encontrando-se todos vinculados ao dever de confidencialidade, mesmo após a cessação das suas funções ou da relação estabelecida com a Associação.
- A Associação promove a formação e sensibilização dos seus colaboradores em matéria de proteção de dados pessoais, segurança da informação e dever de confidencialidade, fomentando uma cultura organizacional assente na proteção da privacidade e no respeito pelos direitos dos titulares dos dados.

Comunicação de Dados Pessoais

- Os dados pessoais apenas são comunicados a terceiros quando tal se revele necessário para a prestação dos cuidados e serviços, para o cumprimento de obrigações legais, por determinação das autoridades competentes ou mediante o consentimento do titular dos dados, quando este seja legalmente exigido.
- Sempre que a Associação recorra a entidades externas para o tratamento de dados pessoais, estas atuam na qualidade de subcontratantes, encontrando-se contratualmente obrigadas a adotar medidas técnicas e organizativas adequadas e a assegurar garantias de proteção dos dados pessoais em conformidade com a legislação aplicável.

Direitos dos Titulares dos Dados

- Os utentes, familiares, representantes legais e demais titulares dos dados podem exercer os direitos que lhes são reconhecidos pela legislação aplicável, designadamente os direitos de acesso, retificação, apagamento, limitação do tratamento, oposição, portabilidade dos dados e retirada do consentimento, quando este constitua o fundamento de licitude do tratamento, sem prejuízo do direito de apresentar reclamação junto da autoridade de controlo competente.
- O exercício destes direitos deverá ser efetuado mediante pedido dirigido à Associação, através dos meios disponibilizados para o efeito, podendo ser solicitada prova da identidade do requerente sempre que tal se revele necessário para salvaguardar a confidencialidade e a segurança dos dados pessoais.
- Os pedidos de exercício de direitos deverão ser remetidos para o endereço de correio eletrónico dpo@livingcare.pt.

Deveres dos Utentes, Familiares e Representantes Legais

- Os utentes, familiares e representantes legais devem fornecer à Associação dados pessoais verdadeiros, completos e atualizados, comunicando sempre que ocorram alterações relevantes às informações anteriormente disponibilizadas.
- Devem igualmente respeitar a privacidade dos restantes utentes, familiares, colaboradores, prestadores de serviços e visitantes, abstendo-se de divulgar ou utilizar dados pessoais de terceiros de que tenham conhecimento no âmbito da sua permanência ou relacionamento com a Associação.
- Sempre que tenham acesso a documentação ou informação clínica, administrativa ou social relativa ao utente ou à pessoa que acompanham ou representam, devem assegurar a respetiva confidencialidade e utilizá-la exclusivamente para os fins a que se destina.

Captação e Divulgação de Imagens e Informação

- Com o objetivo de salvaguardar a privacidade e a dignidade de todos os utentes, não é permitida a captação, gravação ou divulgação de imagens, vídeos ou registos áudio de outros utentes, colaboradores, prestadores de serviços ou visitantes sem o consentimento dos respetivos titulares ou sem outro fundamento legal que legitime esse tratamento.
- A publicação de fotografias, vídeos ou quaisquer dados pessoais ou elementos da vida privada dos utentes nas redes sociais ou noutros meios de comunicação deve respeitar os direitos de personalidade, a legislação aplicável e os princípios da dignidade, privacidade e confidencialidade.
- A Associação poderá proceder à recolha e utilização de imagens para fins institucionais, de comunicação, divulgação das suas atividades ou memória institucional, desde que exista fundamento de licitude adequado, nomeadamente o consentimento, sempre que este seja legalmente exigido.
- A Associação reserva-se o direito de solicitar a interrupção da captação de imagens ou da gravação de áudio e vídeo sempre que tal seja necessário para proteger a privacidade, a dignidade ou os direitos dos utentes, colaboradores, visitantes ou demais pessoas presentes nas suas instalações.

Conservação dos Dados Pessoais

- Os dados pessoais serão conservados apenas durante o período necessário ao cumprimento das finalidades que justificaram a sua recolha ou durante os prazos legalmente estabelecidos para o cumprimento de obrigações legais, regulamentares ou contratuais.
- Decorrido o respetivo período de conservação, os dados pessoais serão eliminados ou anonimizados de forma segura, sem prejuízo das situações em que a sua conservação seja exigida por disposição legal ou por decisão da autoridade competente.

Violação de Dados Pessoais

- Sempre que ocorra uma violação de dados pessoais suscetível de afetar os direitos e liberdades dos titulares dos dados, a Associação adota, com a maior brevidade possível, as medidas necessárias para conter o incidente, avaliar os respetivos riscos e cumprir as obrigações de notificação e comunicação previstas na legislação aplicável, incluindo, quando legalmente exigido, a comunicação à autoridade de controlo competente e aos titulares dos dados.
- A gestão de incidentes de segurança e de violações de dados pessoais rege-se pelos procedimentos internos da Associação e pela legislação aplicável.

Reclamações e Esclarecimentos

- Os utentes, familiares e representantes legais podem solicitar esclarecimentos sobre o tratamento dos seus dados pessoais, bem como apresentar sugestões, questões ou reclamações através dos contactos disponibilizados pela Associação, designadamente junto do Encarregado da Proteção de Dados.
- Caso considerem que o tratamento dos seus dados pessoais não respeita a legislação aplicável, podem igualmente apresentar reclamação junto da autoridade de controlo competente, sem prejuízo do recurso aos demais meios administrativos ou judiciais previstos na lei.

Entrada em Vigor

- A presente Política entra em vigor na data da sua aprovação pela Direção da Associação, sendo disponibilizada aos utentes, familiares e representantes legais no momento da admissão, sempre que solicitada e sempre que ocorram alterações relevantes ao seu conteúdo.
- A Associação assegura a divulgação e acessibilidade permanentes da presente Política, comprometendo-se a promover uma atuação transparente, responsável e orientada para a proteção dos dados pessoais, reforçando uma relação de confiança, respeito pela privacidade e cumprimento da legislação aplicável.

Aprovado por deliberação da Direção, exarada na Ata da Direção n.º 54, de 24 de setembro de 2026