Aqui sou feliz!

CASM

Berçário - Creche - Pré-escolar - CATL - Centro de Dia - Serviço Apoio Domiciliário - Lar

MANUAL DE PROCEDIMENTOS
PROTEÇÃO DE DADOS PESSOAIS

Instituição Particular de Solidariedade Social (IPSS)
Versão revista com referência ao quadro legal vigente em outubro de 2026

V2- 2026

Aqui sou feliz!

CASM

Berçário - Creche - Pré-escolar - CATL - Centro de Dia - Serviço Apoio Domiciliário - Lar

Controlo do documento

Entidade	**Centro de Apoio Social de Mozelos (confirmar denominação legal completa e NIPC)**
Responsável pelo tratamento	A própria IPSS, representada pelo órgão de direção competente
Aprovação	Direção
Data de entrada em vigor	Outubro 2026
Responsável pela revisão	Direção, com apoio do Encarregado de Proteção de Dados (quando designado)
Periodicidade de revisão	Anual e sempre que haja alterações legais, organizacionais, tecnológicas ou incidentes relevantes

1. Objetivo e âmbito

O presente Manual define princípios, responsabilidades e procedimentos internos para assegurar que os dados pessoais tratados pelo CASM são utilizados de forma lícita, leal, transparente e segura, respeitando os direitos e liberdades das pessoas singulares.

Aplica-se a todos os órgãos sociais, trabalhadores, dirigentes, estagiários, voluntários, prestadores de serviços e outras pessoas autorizadas a aceder a dados pessoais, independentemente do suporte utilizado.

Abrange, conforme aplicável, as respostas sociais de infância (creche, EEPE e CATL), respostas para pessoas idosas (Centro de Dia, Serviço de Apoio Domiciliário e ERPI), bem como os processos administrativos, sociais, clínicos, laborais, financeiros e de gestão.

2. Quadro legal e princípios

O tratamento de dados pessoais deve observar, designadamente:

- Regulamento (UE) 2016/679, de 27 de abril (Regulamento Geral sobre a Proteção de Dados — RGPD).
- Lei n.º 58/2019, de 8 de agosto, que assegura a execução do RGPD na ordem jurídica portuguesa.
- Lei n.º 12/2005, de 26 de janeiro, na parte aplicável à informação de saúde, e demais legislação setorial relevante.
- Código do Trabalho e legislação aplicável à segurança e saúde no trabalho, arquivo, fiscalidade, segurança social, cooperação com a Segurança Social e funcionamento das respostas sociais, conforme o tratamento concreto.

A lista legal deve ser revista periodicamente. Os diplomas antigos indicados no anexo do manual de 2018 não devem ser mantidos automaticamente como legislação vigente sem confirmação da sua vigência e aplicabilidade.

Em todos os tratamentos devem ser respeitados os princípios da licitude, lealdade e transparência; limitação das finalidades; minimização dos dados; exatidão; limitação da conservação; integridade e confidencialidade; e responsabilidade demonstrada (responsabilização/accountability).

3. Definições essenciais

- Dados pessoais: informação relativa a pessoa singular identificada ou identificável.
- Categorias especiais de dados: incluem, entre outros, dados de saúde, dados biométricos usados para identificação, origem racial ou étnica, opiniões políticas, convicções religiosas, filiação sindical, dados genéticos, vida sexual ou orientação sexual.
- Tratamento: qualquer operação sobre dados pessoais, como recolha, consulta, utilização, organização, conservação, transmissão, alteração ou eliminação.
- Responsável pelo tratamento: entidade que determina as finalidades e os meios do tratamento; em regra, a IPSS quanto aos seus próprios processos.
- Subcontratante: entidade que trata dados pessoais por conta da IPSS, nos termos de contrato ou outro ato jurídico.
- Encarregado de Proteção de Dados (EPD): profissional que desempenha as funções previstas no RGPD quando a sua designação seja obrigatória ou quando a instituição opte por designá-lo.
- Violação de dados pessoais: incidente de segurança que provoque, acidental ou ilicitamente, destruição, perda, alteração, divulgação ou acesso não autorizado a dados pessoais.

4. Responsabilidades

4.1. Direção

- Aprovar o Manual e assegurar os recursos humanos, técnicos e organizativos necessários.
- Determinar as finalidades e os meios dos tratamentos e garantir que existe uma base de licitude para cada finalidade.
- Apreciar riscos relevantes, decidir medidas corretivas e assegurar que os incidentes são tratados dentro dos prazos legais.
- Designar um EPD quando legalmente exigido ou quando tal seja considerado adequado, assegurando autonomia, recursos e ausência de conflito de interesses.

4.2. Encarregado de Proteção de Dados

Quando designado, o EPD informa e aconselha a instituição e os trabalhadores, acompanha a conformidade, coopera com a CNPD e atua como ponto de contacto para titulares e autoridade de controlo. Deve poder exercer as suas funções com independência e não deve receber instruções sobre o conteúdo das suas recomendações. A Direção mantém a responsabilidade pelo cumprimento da lei.

A obrigatoriedade de designação deve ser avaliada com base nos critérios do artigo 37.º do RGPD, incluindo a natureza, o âmbito e a escala dos tratamentos. O tratamento de dados de saúde não determina, por si só e em todos os casos, a obrigatoriedade automática de designação; deve avaliar-se se ocorre em larga escala e se se verificam os restantes critérios.

4.3. Responsáveis de resposta social e serviços

- Garantir que apenas são recolhidos os dados necessários ao serviço e que os processos são mantidos atualizados.
- Definir acessos de acordo com as funções e comunicar imediatamente incidentes, pedidos de titulares ou dúvidas.
- Assegurar que documentos em papel e ecrãs não ficam acessíveis a pessoas não autorizadas.

4.4. Trabalhadores, voluntários, estagiários e prestadores

- Aceder apenas aos dados necessários às funções atribuídas e utilizar exclusivamente os canais e sistemas autorizados.
- Manter sigilo e confidencialidade durante e após o vínculo com a instituição, nos termos legais e contratuais.
- Não copiar, fotografar, exportar, divulgar ou utilizar dados para fins pessoais, nem os enviar para contas ou dispositivos não autorizados.
- Participar nas ações de formação e comunicar de imediato erros de envio, perda de documentos, acessos indevidos ou outros incidentes.

5. Recolha e licitude do tratamento

Antes de iniciar ou alterar um tratamento, o serviço responsável deve identificar e documentar a finalidade, as categorias de titulares e dados, os destinatários, os prazos de conservação, os sistemas utilizados, a base de licitude e as medidas de segurança.

O consentimento não é a base legal universal. Conforme o caso, o tratamento pode assentar na execução de contrato ou diligências pré-contratuais, cumprimento de obrigação legal, proteção de interesses vitais, exercício de funções de interesse público quando aplicável, interesses legítimos devidamente ponderados, ou consentimento válido. Para dados de saúde e outras categorias especiais é ainda necessária uma condição específica prevista no artigo 9.º do RGPD e na legislação aplicável.

Quando se recorra ao consentimento, este deve ser livre, específico, informado, inequívoco e demonstrável, podendo ser retirado com a mesma facilidade com que foi dado. A prestação de cuidados ou serviços não deve ser indevidamente condicionada a consentimentos que não sejam necessários.

Devem ser fornecidas informações de privacidade claras, acessíveis e adequadas ao público, incluindo, conforme aplicável, identidade e contactos da instituição, finalidades, bases legais, destinatários, conservação, direitos, possibilidade de reclamação à CNPD e existência de transferências internacionais ou decisões automatizadas.

6. Tratamentos por resposta social e processo

6.1. Infância — creche, EEPE e CATL

Os processos podem incluir dados da criança e dos representantes legais necessários à inscrição, prestação do serviço, segurança, faturação e cumprimento de obrigações legais. Dados de saúde, alergias, medicação, necessidades específicas e contactos para emergências devem ser limitados ao necessário e disponibilizados apenas aos profissionais que deles necessitem.

- Confirmar a identidade e legitimidade dos representantes legais, sem presumir que qualquer familiar tem direito a receber informação.
- Separar, sempre que adequado, autorizações para imagem, comunicação externa, saídas e outros fins opcionais.
- Não divulgar listas de crianças, horários, contactos, informação clínica ou fotografias em canais públicos sem base legal adequada e salvaguardas específicas.
- Assegurar que a informação é transmitida a escolas, profissionais de saúde ou outras entidades apenas quando exista fundamento legal e seja necessário.

6.2. Pessoas idosas — Centro de Dia, SAD e ERPI

Os processos administrativos, sociais e clínicos devem ter acessos diferenciados. Informação sobre diagnósticos, medicação, avaliações, dependência, alimentação, ocorrências e cuidados é especialmente confidencial.

- Partilhar informação clínica apenas com profissionais envolvidos nos cuidados ou com entidades legitimadas, na medida necessária.
- Verificar a legitimidade de representantes, procuradores ou pessoas com poderes legalmente reconhecidos; o parentesco, por si só, não confere automaticamente acesso a toda a informação.
- Nas deslocações a hospitais ou consultas, enviar apenas os documentos necessários, em envelope fechado ou por canal eletrónico seguro, entregando-os a profissional ou entidade legitimada.
- Nas passagens de turno, registar apenas a informação relevante para a continuidade e segurança dos cuidados, em local e sistema com acesso restrito.

6.3. Recursos humanos e saúde ocupacional

Os dados dos trabalhadores são tratados para finalidades laborais, administrativas, remuneratórias, fiscais, de segurança social e outras obrigações legais ou contratuais aplicáveis. O acesso a informação de saúde ocupacional deve respeitar o regime próprio: o CASM não deve aceder indiscriminadamente a diagnósticos ou processos clínicos, limitando-se à informação legalmente comunicável, como aptidão e restrições funcionais quando aplicável.

6.4. Doadores, associados, fornecedores e parceiros

A informação deve ser limitada às finalidades de gestão da relação, obrigações legais e execução de contratos. A divulgação de contactos ou utilização para comunicação promocional exige avaliação da base legal e das regras aplicáveis às comunicações eletrónicas.

7. Direitos dos titulares dos dados

O CASM deve disponibilizar um canal para receção e registo de pedidos de acesso, retificação, apagamento, limitação, portabilidade, oposição e retirada de consentimento, quando aplicáveis. Deve também permitir reclamações e esclarecer como contactar a CNPD.

Os pedidos devem ser encaminhados sem demora para o responsável designado e, quando exista, para o EPD. A identidade do requerente deve ser confirmada de forma proporcional, evitando recolher cópias adicionais de documentos de identificação sem necessidade.

A resposta deve ser dada, em regra, no prazo de um mês após a receção. Esse prazo pode ser prorrogado por mais dois meses em casos complexos ou devido ao número de pedidos, devendo o titular ser informado da prorrogação e dos respetivos motivos dentro do primeiro mês. Podem aplicar-se exceções ou limitações previstas na lei.

O apagamento não é automático quando existam obrigações legais de conservação, necessidade de defesa de direitos ou outras bases legítimas. Qualquer recusa, limitação ou impossibilidade de satisfazer o pedido deve ser fundamentada e comunicada nos termos legais.

8. Partilha de dados e prestadores externos

Os dados só podem ser comunicados a terceiros quando exista fundamento jurídico, finalidade compatível e necessidade. A instituição deve verificar a identidade e legitimidade do destinatário e transmitir apenas os dados estritamente necessários.

- Pedidos telefónicos: não confirmar nem divulgar dados sensíveis sem autenticação adequada e verificação da legitimidade.
- Familiares: aplicar os mesmos critérios de legitimidade e minimização; não presumir acesso automático com base no parentesco.
- Autoridades, auditores e financiadores: confirmar competência, finalidade e âmbito do pedido e conservar registo da comunicação quando adequado.
- Prestadores que tratem dados por conta da IPSS: celebrar contrato ou outro ato jurídico conforme ao artigo 28.º do RGPD, com instruções documentadas, confidencialidade, segurança, regras para subcontratantes ulteriores, assistência, incidentes, auditoria e devolução/apagamento dos dados.
- Transferências para países fora do Espaço Económico Europeu: não realizar sem verificar as condições e garantias previstas no capítulo V do RGPD.

9. Conservação, arquivo e eliminação

A instituição deve manter um calendário de conservação por categoria documental, tendo em conta obrigações legais, regulatórias, contratuais, fiscais, laborais, sociais e clínicas, bem como a necessidade de defesa de direitos. Não deve aplicar-se uma regra única de eliminação a todos os processos.

- Conservar apenas durante o período necessário ou legalmente exigido.

- Quando termina a finalidade, eliminar ou anonimizar de forma segura, salvo obrigação de conservação ou fundamento legítimo para manter os dados.
- Quando os dados tenham de ser conservados, mas já não sejam necessários à atividade corrente, restringir o acesso e documentar a razão e o prazo de conservação.
- Destruir papel por trituração segura ou serviço controlado; eliminar ficheiros e suportes digitais através de métodos adequados ao risco.
- Suspender a eliminação quando exista litígio, investigação ou obrigação de preservação documental.

A Direção deve aprovar uma tabela de conservação específica, com categoria documental, fundamento, prazo, evento inicial do prazo, responsável e método de eliminação. Os prazos devem ser confirmados com assessoria jurídica/contabilística e legislação setorial.

10. Segurança física, digital e organizativa

- Manter processos em papel em armários fechados e limitar chaves e acessos a pessoas autorizadas.
- Adotar contas individuais, palavras-passe robustas, autenticação multifator quando disponível e bloqueio automático dos equipamentos.
- Atribuir acessos por função e revê-los quando haja mudança de posto ou cessação de funções; remover prontamente contas e permissões desnecessárias.
- Manter atualizações, proteção antimalware, cópias de segurança e testes de recuperação adequados ao risco.
- Não usar contas pessoais de email, aplicações de mensagens, armazenamento na nuvem ou dispositivos pessoais para dados institucionais sem autorização e salvaguardas aprovadas.
- Verificar destinatários e anexos antes de enviar emails; usar envio protegido ou canais seguros para dados de saúde e outros dados sensíveis.
- Evitar impressões desnecessárias; recolher imediatamente documentos da impressora e não deixar ecrãs ou documentos visíveis a utentes, visitantes ou outros trabalhadores.
- Transportar documentos em invólucro fechado, mantendo-os sob controlo e entregando-os apenas ao destinatário autorizado.
- Avaliar periodicamente riscos, permissões, fornecedores, cópias de segurança e formação.

11. Imagem, som, redes sociais e videovigilância

A captação e divulgação de imagem ou som são tratamentos de dados pessoais. Devem ter finalidade definida, base legal adequada, informação transparente e medidas de minimização. A autorização para captar ou divulgar imagens deve ser tratada de forma específica por finalidade e canal, quando o consentimento seja a base utilizada; a autorização de imagem não equivale a autorização geral para qualquer utilização.

Não publicar imagens, nomes, histórias pessoais, informação de saúde ou outros elementos que permitam identificar utentes, crianças ou trabalhadores em redes sociais ou no website sem validação prévia do fundamento jurídico, da informação prestada e das salvaguardas. Deve ser considerada a vulnerabilidade dos utentes e, no caso de crianças, o superior interesse da criança e a legitimidade de quem exerce responsabilidades parentais.

A videovigilância, se existir, exige análise autónoma da finalidade, necessidade, proporcionalidade, sinalização, acessos, conservação e legislação aplicável. Não deve ser instalada nem utilizada para finalidades incompatíveis ou para controlo laboral fora dos limites legais. Antes de iniciar ou alterar o sistema, consultar o EPD/assessoria jurídica e avaliar se é necessária uma avaliação de impacto.

12. Incidentes e violações de dados pessoais

Qualquer pessoa que detete perda de documentos, envio ao destinatário errado, divulgação indevida, acesso não autorizado, roubo de equipamento, ataque informático ou outro incidente deve comunicá-lo imediatamente à Direção e ao EPD, se designado. Não deve tentar ocultar o incidente nem aguardar por confirmação de todos os factos.

1. Conter o incidente quando possível e seguro: recuperar a mensagem, bloquear acessos, preservar evidências e contactar o suporte informático.
2. Registar a data/hora, natureza do incidente, sistemas e dados envolvidos, titulares potencialmente afetados, destinatários, medidas tomadas e contactos relevantes.
3. A Direção, com apoio do EPD e dos responsáveis técnicos, avalia o risco para os direitos e liberdades das pessoas e documenta a decisão.
4. Quando exigível, notificar a CNPD sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter conhecimento da violação.
5. Quando a violação for suscetível de implicar elevado risco para os titulares, comunicá-la aos titulares sem demora injustificada, salvo se se verificar uma exceção legal.
6. Registar todos os incidentes e decisões, incluindo os casos em que se conclua não ser necessária notificação.

A avaliação e a notificação são responsabilidade da instituição enquanto responsável pelo tratamento; a existência de EPD não transfere essa responsabilidade.

13. Avaliação de riscos e avaliação de impacto

Antes de novos tratamentos ou alterações relevantes, deve ser feita uma análise proporcional dos riscos. Uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) é obrigatória quando o tratamento seja suscetível de resultar num elevado risco para os direitos e liberdades das pessoas, designadamente em situações previstas no artigo 35.º do RGPD. A instituição deve documentar a decisão de realizar ou não realizar a AIPD e consultar previamente a CNPD quando tal seja exigido pelo artigo 36.º.

Tratamentos de dados de saúde em larga escala, monitorização sistemática, combinação de grandes conjuntos de dados, utilização de novas tecnologias ou tratamentos que afetem pessoas vulneráveis devem ser analisados com especial atenção.

14. Formação, confidencialidade e incumprimento

Todos os colaboradores devem receber formação inicial e periódica, adequada às funções, incluindo confidencialidade, uso de email, partilha de informação, direitos dos titulares e comunicação de incidentes. A participação deve ser registada.

O incumprimento das regras pode determinar medidas corretivas e, quando aplicável, consequências disciplinares ou contratuais, com respeito pela lei e pelos procedimentos internos. A confidencialidade mantém-se após o fim das funções, sem prejuízo de obrigações legais de comunicação.

15. Monitorização, auditoria e revisão

A instituição deve manter evidências adequadas do cumprimento: registo das atividades de tratamento, avisos de privacidade, contratos com subcontratantes, registos de pedidos dos titulares, incidentes, formação, acessos e decisões sobre AIPD, conforme aplicável.

A Direção deve rever o Manual pelo menos anualmente e após alterações relevantes. O EPD, quando exista, pode recomendar auditorias periódicas e não programadas. As conclusões devem originar plano de ação com responsável e prazo.

16. Procedimentos operacionais mínimos

- Novo formulário ou novo tratamento: o serviço descreve finalidade, dados, titulares, destinatários, base legal, conservação e segurança; submete à Direção/EPD antes de entrar em funcionamento.
- Pedido de acesso ou retificação: registar a data, verificar identidade e legitimidade, encaminhar para o responsável, controlar o prazo de resposta e guardar a decisão.
- Envio de informação para hospital ou profissional de saúde: confirmar necessidade e destinatário; enviar apenas o necessário, em envelope fechado ou canal seguro; registar a transmissão quando adequado.
- Publicação de imagem: confirmar finalidade, base legal, informação prestada, autorização específica quando aplicável, canal e prazo; obter validação antes da publicação.
- Entrada ou saída de trabalhador: atribuir ou revogar acessos, recolher equipamentos e chaves, informar sobre confidencialidade e atualizar permissões.
- Incidente: comunicar imediatamente à Direção/EPD; não apagar evidências; seguir o procedimento da secção 12.
- Pedido de entidade externa: confirmar identidade, competência, base legal e âmbito; transmitir apenas o estritamente necessário e registar a decisão.

17. Registos e anexos a manter

A instituição deve criar e manter, conforme aplicável, os seguintes instrumentos, que complementam este Manual:

- Registo das atividades de tratamento (artigo 30.º do RGPD), com finalidades, categorias de dados e titulares, destinatários, conservação, medidas de segurança e transferências.
- Avisos de privacidade para utentes e representantes legais, trabalhadores, candidatos, fornecedores e outros titulares.
- Tabela de conservação e eliminação documental.
- Lista de acessos por função e registo de revisão de permissões.
- Registo de pedidos de exercício de direitos.
- Registo de incidentes e violações de dados pessoais.
- Contratos/atos jurídicos com subcontratantes e avaliação dos seus mecanismos de segurança.
- Registo de formação e declarações de confidencialidade.
- Avaliações de risco e, quando aplicável, avaliações de impacto.
- Registo de autorizações de imagem e de outras opções facultativas, quando aplicável.

18. Referências oficiais

Regulamento (UE) 2016/679 (RGPD): https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt

Lei n.º 58/2019, de 8 de agosto: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982

CNPD — Encarregado de Proteção de Dados: https://www.cnpd.pt/organizacoes/outras-obrigacoes/encarregado-de-protecao-de-dados/

CNPD — Violação de dados pessoais: https://www.cnpd.pt/organizacoes/outras-obrigacoes/violacao-de-dados-ou-data-breach/

CNPD — Avaliação de Impacto sobre a Proteção de Dados: https://www.cnpd.pt/organizacoes/outras-obrigacoes/avaliacao-de-impacto/