

Avaliação de Impacto sobre a Proteção de Dados
(AIPD)

Guia de Preenchimento AIPD

Documento de apoio à minuta AIPD PT



Índice

Finalidade do guia.....	5
Como utilizar este guia.....	5
Antes de começar	5
O que é uma AIPD?	5
Quando considerar a AIPD concluída?.....	6
A. Informação genérica	7
Autor	7
Versão do documento e data.....	7
B. Entidade que realiza a avaliação	8
Empresa, NIPC e sede.....	8
DPO e CSO.....	8
C. Descrição geral do processo	9
Âmbito do processo.....	9
D. Consulta	10
Consulta do DPO e do CSO	10
E. Natureza da avaliação	11
1. Descrição sistemática das operações de tratamento	12
1.1 Intervenientes.....	12
Qualidade da entidade	12
Responsabilidade conjunta	12
Acordos de tratamento	12
1.2 Finalidades do tratamento	13
Descrição das finalidades.....	13
1.3 Dados pessoais.....	13
Titulares dos dados	13
Pessoas em situação de vulnerabilidade.....	13
Categorias e elementos de dados	14
Categorias especiais	14
Dados penais e outros dados altamente pessoais.....	14
Dados por tipo de titular	15
1.4 Conservação	15
Prazo e fundamento	15

1.5 Exatidão	15
Garantia de exatidão	15
1.6 Operações de tratamento	16
1.7 Operações de elevado risco	16
Decisões automatizadas e perfis	17
2. Necessidade e proporcionalidade	18
2.1 Necessidade dos dados	18
Justificação por dado	18
2.2 Licitude.....	18
Base do artigo 6.º.....	18
Condição do artigo 9.º	19
Dados penais	19
2.3 Consentimento e interesse legítimo	19
Consentimento	19
Interesse legítimo	20
2.4 Lealdade e transparência	20
Informação aos titulares	20
2.5 Direitos dos titulares.....	20
Medidas para exercício de direitos	20
3. Destinatários	22
3.1 Fluxos e relações de dados.....	22
Fluxograma	22
Ativos	22
3.2 Subcontratantes	22
Ficha por subcontratante.....	22
3.3 Terceiros	23
Destinatários independentes	23
4. Transferências internacionais.....	24
Identificação das transferências	24
Garantias	24
5. Avaliação dos riscos para direitos e liberdades	25
5.1 Medidas técnicas e organizativas.....	25
Medidas existentes.....	25
Impactos possíveis.....	25
5.2 Identificação e avaliação dos riscos	26

Exemplos de riscos bem formulados	27
6. Partes interessadas, códigos e certificações.....	28
Opinião dos titulares ou representantes	28
Códigos de conduta e certificações	28
7. Registo das atividades de tratamento	29
Preenchimento do registo.....	29
8. Lista de anexos	30
Referência dos anexos.....	30
9. Pareceres e recomendações	31
Parecer do DPO	31
Parecer do CSO	31
Revisão da AIPD	31
10. Consulta prévia	32
Recomendação	32
Resposta da autoridade	32
11. Controlo e gestão do documento.....	33
Histórico de alterações	33
Anexo I. Como aplicar as escalas de risco.....	34
Probabilidade	34
Impacto	34
Fatores moduladores	35
Anexo II. Glossário simples.....	35

Guia de Preenchimento AIPD

Finalidade do guia

Este guia tem como finalidade apoiar o preenchimento, a revisão e a documentação de uma avaliação de impacto sobre a proteção de dados, de forma completa, coerente e verificável, por pessoas sem conhecimentos prévios sobre o Regulamento Geral sobre a Proteção de Dados (RGPD) ou a AIPD.

Como utilizar este guia

Este guia acompanha a minuta de AIPD campo a campo. Não substitui o parecer do Encarregado de Proteção de Dados (DPO – *Data protection officer*), a análise jurídica nem a validação das áreas de segurança e tecnologia. O responsável pelo tratamento continua responsável pelas decisões documentadas na AIPD.

Regra de ouro: Não responda apenas “Sim”, “Não” ou “Não aplicável”. Sempre que o campo permita texto, explique o motivo, identifique evidência e refira anexos.

Antes de começar

- Leia a minuta completa para compreender a sequência das secções.
- Defina claramente qual é o tratamento avaliado e o que fica fora do âmbito.
- Reúna contratos, diagramas, avisos de privacidade, políticas de conservação, especificações técnicas e avaliações anteriores.
- Identifique o responsável operacional, o responsável pelo tratamento, os subcontratantes, o DPO e o *Chief Security Officer* (CSO) ou função de segurança equivalente.
- Use a mesma terminologia em todo o documento. Se chamar “Plataforma X” ao sistema numa secção, não lhe chame “Aplicação Y” noutra.
- Diferencie factos existentes, medidas planeadas e recomendações ainda por implementar.

O que é uma AIPD?

Uma AIPD é um processo documentado para compreender um tratamento de dados pessoais, verificar a sua necessidade e proporcionalidade, identificar riscos para as pessoas e decidir que medidas são necessárias antes e durante o tratamento. O

objeto da avaliação não é apenas o sistema informático: é o tratamento completo, incluindo pessoas, procedimentos, fornecedores, fluxos, arquivos e eliminação.

Quando considerar a AIPD concluída?

- O âmbito encontra-se delimitado.
- Os dados, titulares, finalidades, intervenientes, fluxos e prazos estão descritos.
- A licitude e, quando aplicável, a condição do artigo 9.º estão justificadas.
- Os riscos estão formulados na perspetiva dos titulares e avaliados segundo a metodologia definida.
- As medidas existentes e adicionais têm responsável e estado de execução.
- Se aplicável, o DPO emitiu parecer e a decisão final foi formalmente assumida.
- Foi definido quando e por que motivo a AIPD será revista.

A. Informação genérica

Autor

O que preencher: Indique quem coordenou ou redigiu a AIPD. Pode ser uma pessoa da área de negócio, projeto, privacidade, jurídico, tecnologia ou segurança.

Inclua:

- Nome completo e função.
- Unidade organizacional.
- Email profissional.
- Quando existam vários autores, indique o coordenador e liste a restante equipa numa nota ou anexo.

Exemplo: Bruno Silva, Gestor do Projeto, Direção de Operações,
bruno.silva@empresa.pt.

Evite: Indicar apenas “Equipa do Projeto”. A rastreabilidade exige identificar pessoas e responsabilidades.

Versão do documento e data

O que preencher. Registe a versão atual e a data de emissão. Utilize numeração coerente, por exemplo 0.1 para rascunhos e 1.0 para a versão aprovada.

Exemplo: Versão 0.3, 12 de agosto de 2026, em revisão pelo DPO.

B. Entidade que realiza a avaliação

Empresa, NIPC e sede

O que preencher: Identifique a entidade que promove e documenta a AIPD. Esta identificação não resolve, por si só, a qualificação jurídica da entidade como responsável ou subcontratante, que é analisada na secção 1.1.

Inclua:

- Denominação social completa.
- Número de identificação de pessoa coletiva ou VAT.
- Morada da sede.

DPO e CSO

O que preencher: Indique os pontos de contacto para proteção de dados e segurança da informação. Se não existir CSO, identifique a função equivalente. Se não existir DPO designado, indique “Não designado” e o contacto interno responsável por privacidade.

Evite: Inventar uma função ou pessoa apenas para preencher o campo.

C. Descrição geral do processo

Âmbito do processo

O que preencher: Descreva o tratamento de forma breve, mas suficientemente concreta para um leitor externo compreender o que acontece.

Inclua:

- Objetivo operacional do projeto.
- Principais titulares e dados.
- Origem dos dados.
- Sistemas e fornecedores principais.
- Início e fim do ciclo de vida.
- Limites da AIPD: componentes, países, entidades ou utilizações excluídas e respetivo motivo.

Exemplo: Implementação de plataforma para recolher questionários de acompanhamento farmacoterapêutico, associar respostas a um identificador de utente, permitir consulta por farmacêuticos autorizados e produzir relatórios estatísticos agregados. A AIPD abrange a recolha, alojamento, consulta, exportação e eliminação; não abrange o sistema autónomo de faturação.

Evite: Descrições vagas como “tratamento de dados para apoiar o negócio”.

D. Consulta

Consulta do DPO e do CSO

O que preencher: Assinale se cada função foi consultada e resuma o contributo. A consulta não é a aprovação final. Registe a data, os temas analisados, recomendações e o modo como foram consideradas.

Exemplo: DPO consultado em 02/08/2026 sobre base de licitude, informação aos titulares e conservação. CSO consultado em 04/08/2026 sobre autenticação, registos de acesso e cifragem. Recomendações incorporadas nas secções 2.2 e 5.1.

E. Natureza da avaliação

Tipo	Quando selecionar	O que identificar
Inicial	Primeira AIPD deste tratamento ou projeto antes da entrada em produção.	Data prevista de início e versão do desenho avaliado.
Revisão regular	Revisão periódica prevista na AIPD anterior.	Referência da AIPD anterior, alterações e conclusão da revisão.
Revisão extraordinária	Alteração relevante do tratamento, risco, tecnologia, fornecedor, finalidade, dados ou incidente.	Evento que desencadeou a revisão e secções afetadas.

1. Descrição sistemática das operações de tratamento

Objetivo da secção: Documentar quem trata, para quê, que dados, sobre quem, durante quanto tempo e através de que operações.

1.1 Intervenientes

Qualidade da entidade

O que preencher: Assinale se a entidade atua como responsável, subcontratante ou subcontratante ulterior no tratamento avaliado. A resposta depende de quem decide as finalidades e os meios essenciais, e não do nome dado no contrato.

Inclua:

- Responsável: decide porquê e os elementos essenciais de como os dados são tratados.
- Subcontratante: trata dados por conta e segundo instruções do responsável.
- Subcontratante ulterior: é contratado por um subcontratante para executar parte do tratamento.

Evite: Selecionar “subcontratante” apenas porque existe um contrato de prestação de serviços.

Responsabilidade conjunta

O que preencher: Assinale “Sim” quando duas ou mais entidades determinam conjuntamente finalidades e meios essenciais. Identifique cada corresponsável, descreva as decisões partilhadas e anexe o acordo aplicável.

Exemplo: Entidade A define com Entidade B os critérios do estudo, os dados recolhidos, a plataforma e os destinatários dos resultados. Ambas aprovam o protocolo e decidem conjuntamente sobre pedidos de direitos.

O que preencher: Quando a entidade for subcontratante ou subcontratante ulterior, identifique o responsável ou subcontratante inicial e confirme a existência do acordo escrito. Anexe-o ou indique a referência no repositório contratual.

Evite: Responder “Sim” sem verificar se o contrato cobre objeto, duração, natureza, finalidade, dados, titulares, instruções, confidencialidade, segurança, subcontratação, apoio, eliminação e auditoria.

1.2 Finalidades do tratamento

Descrição das finalidades

O que preencher: Indique cada finalidade de forma separada, concreta e orientada para o resultado. Uma finalidade explica por que motivo os dados são necessários.

Inclua:

- Utilize verbos e resultados: “gerir inscrições”, “prestar acompanhamento”, “prevenir fraude”.
- Diferencie finalidades principais de utilizações secundárias.
- Associe posteriormente cada finalidade à base de licitude, aos dados e aos destinatários.

Exemplo: Finalidade 1 - Gerir a inscrição e participação no estudo; Finalidade 2 - Analisar resultados e produzir estatísticas pseudonimizadas; Finalidade 3 - Cumprir pedidos de autoridades competentes.

Evite: “Melhorar serviços”, “fins administrativos” ou “tratamento no âmbito do projeto”, sem detalhe.

1.3 Dados pessoais

Titulares dos dados

O que preencher: Liste grupos de pessoas, não nomes individuais. Quando um grupo tenha relação ou risco diferente, crie categoria própria.

Inclua:

- Participantes, utentes, clientes, trabalhadores, candidatos, profissionais de saúde, representantes legais, pessoas de contacto de fornecedores.

Exemplo: Participantes adultos no estudo; farmacêuticos utilizadores da plataforma; pessoas de contacto do promotor.

Pessoas em situação de vulnerabilidade

O que preencher: Assinale se os titulares dos dados serão considerados categorias vulneráveis. Poderão existir titulares dos dados que se enquadrem em diferentes categorias vulneráveis.

Exemplo: Crianças; idosos; doentes.

Categorias e elementos de dados

O que preencher: Na coluna “Categoria”, use grupos compreensíveis. Na coluna “Dados”, liste cada elemento efetivamente tratado.

Exemplo: Categoria: Contactos. Dados: email profissional e telefone. Categoria: Saúde. Dados: medicação, alergias, diagnóstico e resultados laboratoriais.

Evite: Escrever apenas “dados pessoais”, “dados do cliente” ou copiar toda a definição legal sem indicar elementos concretos.

Categorias especiais

O que preencher: Assinale apenas as categorias efetivamente tratadas. Para biometria, a imagem, voz ou impressão só constitui categoria especial quando resulta de tratamento técnico específico para identificação única. Para dados inferidos, considere se o tratamento pretende revelar uma categoria especial.

Inclua:

- Saúde.
- Genéticos.
- Biométricos para identificação única.
- Origem racial ou étnica.
- Opiniões políticas.
- Convicções religiosas ou filosóficas.
- Filiação sindical.
- Vida sexual ou orientação sexual.

Dados penais e outros dados altamente pessoais

O que preencher: Identifique separadamente condenações, infrações e medidas de segurança. Nos “outros dados altamente pessoais”, assinale só os que existam.

Exemplo: Dados financeiros: IBAN e histórico de pagamentos. Comunicações: conteúdo de emails de suporte. Localização: coordenadas recolhidas a cada cinco minutos

Dados por tipo de titular

O que preencher: Relacione cada categoria de titular com as categorias de dados correspondentes. Esta tabela serve de teste de coerência e minimização.

Exemplo: Participantes: identificação, contacto, saúde. Investigadores: identificação profissional, contacto, CV. Utilizadores do sistema: identificação, credenciais e registos de acesso.

1.4 Conservação

Prazo e fundamento

O que preencher: Indique o prazo para cada conjunto de dados e o momento a partir do qual se conta. Explique a razão e identifique norma legal, contrato, prescrição, necessidade operacional ou critério de arquivo.

Inclua:

- Use prazos objetivos: “10 anos após o encerramento do processo”.
- Se não for possível fixar número, indique critério verificável e data de revisão.
- Diferencie produção, arquivo restrito, anonimização e eliminação.
- Explique quem executa e como é evitada a conservação em cópias, exportações e fornecedores.

Exemplo: Respostas identificáveis: duração do estudo + 2 anos para validação e auditoria. Após esse prazo, anonimização irreversível. Ficheiros temporários de importação: 30 dias após validação.

Evite: “Enquanto necessário” sem critério; “indefinidamente”; utilizar o mesmo prazo para todos os dados sem justificação.

1.5 Exatidão

Garantia de exatidão

O que preencher: Descreva controlos proporcionais ao impacto de dados incorretos.

Inclua:

- Validação de formato e campos obrigatórios.
- Confirmação pelo titular.

- Sincronização com fonte autorizada.
- Revisões periódicas e alertas de desatualização.
- Registo de correções e propagação aos destinatários.

Exemplo: O email é validado por confirmação; dados clínicos são inseridos por profissional autorizado; correções ficam registadas em registo de auditoria.

1.6 Operações de tratamento

Assinale todas as operações que realmente ocorrem ao longo do ciclo de vida.

Operação	Pergunta prática
Recolha	Os dados entram diretamente do titular ou de outra fonte?
Registo / conservação	São gravados ou mantidos em qualquer suporte?
Organização / estruturação	São classificados, indexados, formatados ou agregados?
Consulta / utilização	Alguém vê, pesquisa, calcula ou toma ações com base nos dados?
Alteração / adaptação	Os dados são corrigidos, transformados ou normalizados?
Transmissão / disponibilização	Há acesso ou envio para outra entidade, equipa ou utilizador?
Comparação / interconexão	São cruzados com outro conjunto de dados?
Limitação	Existe bloqueio para impedir usos enquanto os dados são conservados?
Apagamento / destruição	Como e quando deixam de estar disponíveis e recuperáveis?

Pode consultar a definição de cada operação de tratamento, ao passar o apontador por cima das operações de tratamento na minuta de Avaliação de Impacto sobre a Proteção de Dados.

1.7 Operações de elevado risco

Para cada critério, selecione Sim ou Não e justifique. A presença de critérios ajuda a explicar a necessidade da AIPD, mas a conclusão depende do contexto e da combinação dos fatores.

Critério	Questões para responder na justificação
Avaliação ou classificação	Que aspetos pessoais são avaliados? Existe pontuação, perfil ou previsão? Para que decisão?
Decisão automatizada significativa	A decisão é exclusivamente automatizada? Produz efeito jurídico ou impacto semelhante? Existe intervenção humana efetiva?
Controlo sistemático	Quem é observado, onde, com que frequência e por quanto tempo?

Critério	Questões para responder na justificação
Dados sensíveis ou altamente pessoais	Que dados, em que volume e com que possíveis consequências?
Grande escala	Quantos titulares e elementos? Qual a área geográfica, frequência e duração?
Combinação de dados	Que fontes são cruzadas? A combinação excede expectativas razoáveis?
Titulares vulneráveis	Que relação de dependência ou menor capacidade de escolha existe?
Tecnologia inovadora	O que é novo no contexto e que incertezas acresce?
Impedimento de direito, serviço ou contrato	O tratamento condiciona acesso, preço, benefício ou exercício de direito?
Recolha indireta sem informação	Qual a fonte e por que não é exequível informar? Que salvaguardas alternativas existem?

Decisões automatizadas e perfis

O que preencher: Se existirem, descreva a lógica em linguagem compreensível, a importância e as consequências. Indique dados de entrada, regras ou modelo, validação, limiares, intervenção humana, contestação e monitorização de erros ou enviesamentos.

Exemplo: O sistema calcula uma prioridade de contacto a partir de três respostas. A pontuação não decide a prestação do serviço; um profissional revê todos os casos e pode alterar a prioridade, registando a razão.

2. Necessidade e proporcionalidade

Diferença essencial: Necessidade pergunta se o tratamento e cada dado são realmente indispensáveis para atingir a finalidade. Proporcionalidade pergunta se os benefícios justificam a interferência nos direitos, considerando alternativas e salvaguardas.

2.1 Necessidade dos dados

Justificação por dado

O que preencher: Para cada elemento ou grupo homogêneo, explique a ligação direta à finalidade. Teste se a finalidade continua alcançável sem esse dado, com menor detalhe, menor frequência ou anonimização.

Inclua:

- Finalidade suportada.
- Decisão ou operação que depende do dado.
- Alternativas consideradas.
- Consequência de não recolher.
- Medidas de minimização.

Exemplo: Data de nascimento: necessária para aplicar critérios etários do protocolo. Alternativa “ano de nascimento” rejeitada porque o critério depende da idade na data de inclusão. A data completa é convertida em idade e removida do conjunto analítico.

Evite: Afirmar apenas “necessário ao projeto”.

2.2 Licitude

Base do artigo 6.º

O que preencher: Escolha a base aplicável a cada finalidade e justifique os requisitos. Pode existir mais de uma base no mesmo projeto, mas não deve selecionar várias em alternativa para a mesma finalidade sem explicar.

Inclua:

- Consentimento: livre, específico, informado, inequívoco e demonstrável.
- Contrato: tratamento objetivamente necessário para executar contrato com o próprio titular ou diligências pedidas pelo titular.
- Obrigação jurídica: identifique norma e obrigação concreta.

- Interesses vitais: situações excecionais para proteção da vida ou integridade.
- Interesse público / autoridade pública: identifique fundamento jurídico e função.
- Interesse legítimo: identifique interesse, necessidade e ponderação.

Exemplo: Gestão da conta: artigo 6.º, n.º 1, alínea b), porque login e contacto são necessários para prestar o serviço pedido. Segurança e prevenção de abuso: artigo 6.º, n.º 1, alínea f), sustentado em avaliação de interesses legítimos anexa.

Condição do artigo 9.º

O que preencher: Se tratar categorias especiais, identifique uma condição do artigo 9.º, n.º 2, adicionalmente à base do artigo 6.º. Explique os requisitos e a norma nacional ou europeia quando a condição a exigir.

Evite: Usar “investigação científica” como justificação automática sem demonstrar necessidade, garantias e base jurídica aplicável.

Dados penais

O que preencher: Quando existam dados do artigo 10.º, identifique a base do artigo 6.º e a autorização legal ou controlo de autoridade pública aplicável. Solicite validação jurídica específica.

2.3 Consentimento e interesse legítimo

Consentimento

O que preencher: Descreva quem pede, quando, como, para que finalidades, como é registado e como é retirado sem prejuízo. Explique como lida com menores, representantes ou desequilíbrio de poder.

Inclua:

- Texto separado e claro.
- Ação positiva inequívoca.
- Prova da versão apresentada.
- Retirada tão fácil como a prestação.
- Consequências reais da recusa.

Interesse legítimo

O que preencher: Anexe ou resuma uma avaliação em três passos: finalidade legítima, necessidade e ponderação. Considere expectativas razoáveis, relação com titulares, natureza dos dados, impacto e salvaguardas.

Exemplo: Interesse: prevenir utilizações abusivas. Necessidade: registos limitados de IP e tentativas falhadas; alternativa sem IP não permite detetar padrões. Ponderação: retenção de 90 dias, acesso restrito e informação no aviso reduzem impacto.

2.4 Lealdade e transparência

Informação aos titulares

O que preencher: Identifique o aviso aplicável, artigos 13.º ou 14.º, canal e momento em que é disponibilizado. Confirme que cobre responsável, contactos, finalidades, bases, destinatários, transferências, conservação, direitos, reclamação, obrigatoriedade e decisões automatizadas quando aplicável.

Inclua:

- Anexe a versão do aviso.
- Se os dados forem indiretos, identifique a fonte e a exceção invocada, se alguma.
- Explique como alterações relevantes são comunicadas.

Evite: Indicar apenas “política de privacidade disponível no site” sem referência, versão ou momento de apresentação.

2.5 Direitos dos titulares

Medidas para exercício de direitos

O que preencher: Explique o procedimento real, não apenas enumere os direitos. Indique canal de entrada, autenticação, triagem, pesquisa nos sistemas, resposta, prazos, exceções, registo e comunicação a destinatários.

Exemplo: Pedidos recebidos em privacidade@empresa.pt são registados no sistema de gestão. A equipa identifica os sistemas através do inventário, valida a identidade de modo proporcional e envia resposta aprovada pelo DPO. Correções são propagadas a dois subcontratantes através de pedido registado.

Atenção: A existência e extensão de cada direito dependem da base de licitude e do contexto. Não trate a tabela do Anexo A como decisão automática; valide exceções e limitações caso a caso.

3. Destinatários

3.1 Fluxos e relações de dados

Fluxograma

O que preencher: Mostre o percurso desde a origem até à eliminação. Inclua titulares, recolha, aplicações, integrações, armazenamento, equipas, fornecedores, destinatários, exportações, arquivo, backups e eliminação.

Inclua:

- Numere cada fluxo.
- Indique direção, dados e canal.
- Assinale países ou regiões.
- Diferencie ambiente de produção, teste e suporte.
- Inclua acessos humanos relevantes.

Exemplo: F1 Participante → formulário web: identificação e respostas, HTTPS. F2 Formulário → base cloud UE: dados pseudonimizados. F3 Base → equipa analítica: exportação mensal cifrada. F4 Tabela de correspondência → servidor separado, acesso restrito ao coordenador.

Ativos

O que preencher: Liste ativos essenciais para compreender o risco: aplicações, bases de dados, APIs, equipamentos, redes, pessoas, instalações, documentos, arquivos e medidas contratuais. Agrupe por função, evitando inventário técnico excessivo.

Exemplo: Portal de recolha; base de dados SQL; serviço de identidade; portáteis dos investigadores; arquivo físico; equipa de suporte; contrato com alojamento cloud.

3.2 Subcontratantes

Ficha por subcontratante

O que preencher: Preencha uma ficha por entidade que trate dados por conta do responsável.

Inclua:

- Denominação, sede, país e identificador fiscal.
- Serviço e instruções.

- Dados e titulares.
- Finalidade e duração.
- Localização efetiva do tratamento e suporte.
- Subcontratantes ulteriores.
- Contrato e medidas de controlo.

Evite: Listar apenas a marca comercial sem identificar a entidade contratual e as localizações relevantes.

3.3 Terceiros

Destinatários independentes

O que preencher: Identifique entidades que recebem dados para finalidades próprias ou ao abrigo de obrigação legal, contratual ou regulamentar. Explique o fundamento da comunicação e quais dados são estritamente necessários.

Exemplo: Autoridade reguladora: comunicação de dados de segurança quando legalmente exigida. Seguradora: apenas quando exista fundamento contratual ou legal aplicável e informação ao titular.

4. Transferências internacionais

Identificação das transferências

O que preencher: Mapeie acessos, alojamento, suporte, administração remota e comunicações para fora do Espaço Económico Europeu ou para organizações internacionais. Uma transferência pode ocorrer sem deslocação física se uma entidade de país terceiro tiver acesso.

Inclua:

- País e destinatário.
- Dados e titulares.
- Finalidade e frequência.
- Mecanismo do Capítulo V.
- Medidas suplementares.
- Avaliação das leis e práticas do país quando necessária.

Evite: Assumir “sem transferências” apenas porque o servidor principal está na UE; confirme suporte e subcontratantes ulteriores.

Garantias

O que preencher: Assinale o mecanismo correto e anexe a evidência: decisão de adequação, regras vinculativas, cláusulas-tipo, instrumento autorizado, código ou certificação. Se depender de derrogação, documento carácter excecional e requisitos específicos.

Exemplo: Fornecedor X, Estados Unidos: transferência abrangida por decisão de adequação aplicável à entidade certificada, verificação realizada em 05/08/2026 e evidência anexa.

5. Avaliação dos riscos para direitos e liberdades

Perspetiva correta: Avalie o risco para as pessoas. Custos, sanções ou danos reputacionais da organização podem ser consequências empresariais, mas não substituem a descrição do dano para o titular.

5.1 Medidas técnicas e organizativas

Medidas existentes

O que preencher: Descreva medidas concretas, estado de implementação e evidência. Relacione cada medida com o risco que reduz.

Inclua:

- Controlo de acessos e revisão de permissões.
- Autenticação multifator.
- Cifragem em trânsito e repouso.
- Pseudonimização e separação de chaves.
- Registos e monitorização.
- Backups e testes de restauro.
- Gestão de vulnerabilidades.
- Segregação de ambientes.
- Formação e confidencialidade.
- Gestão de fornecedores e incidentes.
- Eliminação segura.

Exemplo: Acesso à tabela de correspondência limitado a dois coordenadores por grupo dedicado; MFA obrigatório; revisão trimestral; logs protegidos durante 12 meses; evidência no relatório de acessos anexo.

Evite: Expressões genéricas como “medidas adequadas”, “sistema seguro” ou “cumprimento do RGPD”.

Impactos possíveis

O que preencher: Selecione os tipos de dano relevantes e descreva cenários concretos. Um mesmo incidente pode causar vários impactos.

Exemplo: Divulgação de medicação para empregador pode causar discriminação e perda de emprego. Alteração de alergia pode conduzir a recomendação inadequada e dano físico. Indisponibilidade pode atrasar acesso à informação necessária ao cuidado.

5.2 Identificação e avaliação dos riscos

Redija cada risco como um cenário: fonte ou causa + evento + consequência para o titular. Evite listar apenas vulnerabilidades.

Modelo recomendado: Devido a [fonte/causa], pode ocorrer [evento sobre os dados], levando a [consequência concreta para os titulares].

Elemento	Como preencher	Exemplo
Descrição do risco	Cenário completo e específico.	Permissões excessivas podem permitir consulta não autorizada de diagnósticos, causando quebra de confidencialidade e discriminação.
Natureza	Confidencialidade, integridade, disponibilidade ou risco estrutural do desenho.	Confidencialidade.
Probabilidade	Escolha 1–5 segundo a escala, com evidência e fatores moduladores.	3 Possível: acessos frequentes e equipa alargada; MFA e logs reduzem probabilidade.
Impacto	Escolha 1–5 segundo consequência plausível para pessoas.	4 Elevado: informação de saúde pode causar discriminação e consequências difíceis de ultrapassar.
Risco inerente	Multiplique probabilidade por impacto, usando as medidas de base já previstas conforme a metodologia da minuta.	$3 \times 4 = 12$.
Decisão	Aceitar, mitigar, evitar ou, com cautela, transferir.	Mitigar.
Ações	Medida adicional, responsável, prazo e evidência.	Rever perfis; responsável IAM; antes da produção; relatório de teste.
Risco residual	Reavaliar após as medidas adicionais; não copiar automaticamente o risco inerente.	$2 \times 4 = 8$, após redução de probabilidade.

Sobre “transferir”: A contratação de seguro ou fornecedor pode repartir consequências organizacionais, mas não elimina a responsabilidade do responsável nem o impacto para o titular. Use esta decisão apenas com explicação.

Exemplos de riscos bem formulados

- Acesso indevido por utilizador interno a dados de saúde devido a perfis demasiado amplos, podendo causar exposição, discriminação e perda de confiança.
- Associação incorreta entre identificador e participante devido a erro de importação, podendo gerar decisão clínica ou contacto dirigido à pessoa errada.
- Reidentificação de conjunto pseudonimizado através da combinação de idade, localidade e diagnóstico raro, podendo revelar identidade e estado de saúde.
- Indisponibilidade prolongada causada por ransomware, impedindo o acesso oportuno a informação necessária e atrasando a prestação do serviço.
- Conservação para além do prazo por falha na eliminação de exportações locais, prolongando exposição e impedindo o controlo dos dados pelo titular.

6. Partes interessadas, códigos e certificações

Opinião dos titulares ou representantes

O que preencher: Indique se foram consultados, como foram selecionados, informação apresentada, principais observações e impacto no desenho. Se não foram consultados, justifique por que não era adequado ou possível.

Exemplo: Foi testado o aviso e o fluxo de consentimento com representantes de participantes. A expressão “dados codificados” foi substituída por “dados pseudonimizados” e foi acrescentado exemplo de retirada.

Códigos de conduta e certificações

O que preenche: Identifique apenas códigos aprovados e certificações efetivamente aplicáveis ao tratamento. Explique o âmbito e anexe comprovativo. Políticas internas ou certificações gerais de segurança podem ser evidência útil, mas não devem ser apresentadas como certificação RGPD se não o forem.

7. Registo das atividades de tratamento

Preenchimento do registo

O que preencher: Transponha os elementos consolidados da AIPD para o formato de registo aplicável ao responsável ou subcontratante. Verifique coerência com o registo corporativo já existente.

Inclua:

- Finalidades.
- Licitude quando aplicável.
- Titulares e dados.
- Destinatários.
- Transferências e garantias.
- Prazos de apagamento.
- Medidas de segurança gerais.

Evite: Criar informação nova nesta secção que contradiga as anteriores. Corrija primeiro a fonte da inconsistência.

8. Lista de anexos

Referência dos anexos

O que preencher: Atribua referência estável, nome e descrição. Cite a referência nas secções relevantes.

Exemplo: A01 – Diagrama de fluxos v1.2 – Fluxos F1 a F8, sistemas e países. A02 – Aviso de privacidade v3 – Informação a participantes. A03 – Contrato de subcontratação – Fornecedor cloud.

Anexos frequentemente úteis	Quando incluir
Diagrama de fluxos e arquitetura	Sempre que existam vários sistemas, integrações ou entidades.
Avisos de privacidade e consentimentos	Para demonstrar transparência e, quando aplicável, consentimento.
Contratos e acordos	Subcontratação, corresponsabilidade, partilha ou transferências.
Avaliação de interesse legítimo	Quando o artigo 6.º, n.º 1, alínea f), é utilizado.
Especificações de segurança e testes	Para evidenciar medidas e estado de implementação.
Política ou tabela de conservação	Quando suporta prazos e eliminação.
Protocolo do estudo ou requisitos funcionais	Para demonstrar finalidades, dados e necessidade.

9. Pareceres e recomendações

Parecer do DPO

O que preencher: O DPO deve analisar conformidade, necessidade, proporcionalidade, riscos, medidas e eventual consulta prévia. O parecer deve ser datado, claro e indicar recomendações ou condições. O responsável decide e deve documentar desvios ao parecer.

Parecer do CSO

O que preencher: A função de segurança deve validar arquitetura, ameaças, medidas, dependências, testes e riscos técnicos. Indique limitações, pressupostos e ações pendentes.

Revisão da AIPD

O que preencher: Defina eventos e periodicidade. Uma revisão não deve consistir apenas em mudar a data; deve verificar alterações de finalidade, dados, escala, tecnologia, fornecedores, ameaças, incidentes, legislação e eficácia das medidas.

Inclua:

- Alterações nos riscos ou no desenho.
- Novas vulnerabilidades ou incidentes.
- Maior impacto de decisões automatizadas.
- Mudança organizacional, tecnológica ou contratual.
- Revisão periódica definida pelo risco.

10. Consulta prévia

Recomendação

O que preencher: O DPO indica se, após todas as medidas previstas, permanece risco elevado que não possa ser reduzido. Nessa situação, documente a análise e prepare consulta à autoridade antes do tratamento.

Evite: Confundir a existência de risco elevado inerente com a obrigação automática de consulta. O foco é o risco residual depois das medidas.

Resposta da autoridade

O que preencher: Registe autoridade, datas, responsável, orientações e forma de implementação. Anexe correspondência e atualize a decisão final.

11. Controlo e gestão do documento

Histórico de alterações

O que preencher: Registe cada versão relevante, data, autor e resumo. Alterações que afetem conclusões devem ser facilmente localizáveis.

Exemplo: 1.1 | 20/08/2026 | Ana Costa | Alterado fornecedor cloud; revistos fluxos F3–F5, transferências e riscos R04/R07.

Anexo I. Como aplicar as escalas de risco

Probabilidade

Avalie a plausibilidade do cenário no contexto real. Utilize histórico, exposição, número de utilizadores, acessibilidade, complexidade, maturidade de controlos, motivação de atacantes e frequência do tratamento. As percentagens da minuta são indicativas; documente a evidência usada.

Nível	Leitura prática	Perguntas de apoio
1 Raro	Só em circunstâncias muito particulares; sem histórico relevante.	O cenário exige várias falhas independentes? Os controlos são testados?
2 Remoto	Pode ocorrer em condições excecionais.	Há exposição limitada e poucos intervenientes?
3 Possível	Pode ocorrer em condições normais.	Já ocorreu no setor ou existem falhas plausíveis?
4 Provável	É expectável em várias situações normais.	Há exposição frequente, fragilidades conhecidas ou controlos incompletos?
5 Quase certo	É repetido ou fortemente expectável.	O evento já ocorre ou a causa está presente continuamente?

Impacto

Avalie a gravidade para os titulares, não apenas a sensibilidade abstrata do dado. Considere reversibilidade, duração, número e vulnerabilidade dos afetados, contexto, sigilo e possibilidade de agregação de danos.

Nível	Leitura prática	Exemplos de consequência
1 Insignificante	Sem impacto relevante plausível.	Perturbação praticamente nula.
2 Menor	Pequeno incómodo facilmente ultrapassável.	Tempo gasto, contacto indesejado pontual.
3 Moderado	Inconveniente significativo com alguma dificuldade.	Stress, custos, recusa temporária de serviço.
4 Elevado	Consequência significativa, ultrapassável apenas com séria dificuldade.	Perda de emprego, perda financeira relevante, discriminação.
5 Crítico	Consequência grave ou irreversível.	Dano físico prolongado, perseguição, impacto duradouro na vida.

Fatores moduladores

- **Aumentam o risco:** grande escala, alta sensibilidade, crianças ou dependência, exposição pública, decisões com efeitos significativos, dados combináveis, longa conservação.
- **Reduzem o risco:** minimização real, pseudonimização robusta, separação de chaves, MFA, acessos estritos, monitorização, curta conservação, intervenção humana efetiva.
- Uma medida só deve reduzir a classificação se estiver implementada ou incluída no conjunto de medidas de base definido pela metodologia. Medidas adicionais pendentes reduzem o risco apenas na avaliação residual condicionada à implementação.

Anexo II. Glossário simples

Termo	Definição prática
AIPD	Avaliação documentada dos impactos e riscos de um tratamento para os direitos e liberdades das pessoas.
Dado pessoal	Informação relativa a pessoa identificada ou identificável.
Tratamento	Qualquer operação sobre dados, como recolher, consultar, alterar, partilhar, conservar ou eliminar.
Titular	Pessoa a quem os dados dizem respeito.
Responsável	Entidade que decide finalidades e meios essenciais.
Subcontratante	Entidade que trata dados por conta do responsável.
Terceiro	Entidade ou pessoa diferente do titular, responsável, subcontratante e pessoas autorizadas sob autoridade destes.
Destinatário	Entidade ou pessoa a quem os dados são divulgados.
Pseudonimização	Tratamento que impede atribuição a pessoa específica sem informação adicional mantida separadamente e protegida.
Anonimização	Transformação irreversível que impede identificação por meios razoavelmente suscetíveis de ser utilizados.
Risco inerente	Risco avaliado considerando o desenho e conjunto inicial de medidas definido na metodologia, antes das medidas adicionais.
Risco residual	Risco que permanece após as medidas adicionais.
Probabilidade	Possibilidade de o cenário ocorrer.
Impacto	Gravidade das consequências para os titulares.
Transferência internacional	Disponibilização de dados a destinatário em país terceiro ou organização internacional, incluindo certos acessos remotos.

