

Acordo de tratamento de dados (DPA)

Última atualização: 1 de maio de 2026 · Contrato nos termos do art. 28.º do RGPD.

Esta tradução é fornecida apenas a título informativo. Em caso de divergência entre esta tradução e a versão em inglês, prevalece a versão em inglês.

Como funciona

Este DPA faz parte dos termos de utilização. Aplica-se automaticamente quando é criado um espaço de trabalho e nele são guardados dados pessoais. A organização cliente proprietária do espaço de trabalho é o responsável pelo tratamento; a Dazr é o subcontratante. Não é necessária assinatura; se o seu processo de compras exigir um exemplar assinado por ambas as partes, escreva para legal@dazr.eu.

1. Definições

Os termos deste DPA têm o significado que lhes é dado pelo Regulamento (UE) 2016/679 (o RGPD). «Dados pessoais do cliente» são os dados pessoais que o responsável pelo tratamento (ou os membros e auditores que atuam sob a sua autoridade) coloca no espaço de trabalho, incluindo dados pessoais em tarefas de controlo, evidências, comentários, ficheiros, riscos, incidentes, registos de fornecedores, membros e convites, comunicações recebidas pelo portal público e o registo de atividade.

2. Objeto, duração, natureza e finalidade

- Objeto: o tratamento dos dados pessoais do cliente para que o responsável pelo tratamento possa gerir o seu programa de conformidade em segurança da informação e proteção de dados através da plataforma Dazr Compliance.
- Duração: a vigência da subscrição do responsável pelo tratamento, acrescida do período de tolerância após a cessação previsto nos termos de utilização.
- Natureza e finalidade: alojamento, armazenamento, transmissão, consulta, apagamento e as operações descritas nos termos de utilização e na política de privacidade.
- Tipo de dados pessoais: dados de identificação dos membros dos espaços de trabalho e dos auditores convidados (e-mail, nome, função); quando aplicável, dados de identificação de quem comunica pelo portal público e de quem comunica incidentes; dados de contacto de entidades empregadoras e metadados operacionais carregados pelo responsável pelo tratamento. O responsável pelo tratamento assegura que não carrega categorias especiais de dados, salvo se a sua própria base jurídica o permitir.
- Categorias de titulares dos dados: trabalhadores, prestadores de serviços e auditores externos convidados do responsável pelo tratamento, e qualquer pessoa identificada nos conteúdos de conformidade que o responsável pelo tratamento decida carregar.

3. Obrigações do subcontratante

1. Tratamos os dados pessoais do cliente apenas mediante instruções documentadas do responsável pelo tratamento. As instruções consistem na utilização das funções previstas da plataforma; se considerarmos que uma instrução viola o RGPD ou outra disposição de proteção de dados da União ou de um Estado-Membro, informamos o responsável pelo tratamento.
2. Garantimos que as pessoas autorizadas a tratar os dados pessoais do cliente assumiram um compromisso de confidencialidade.
3. Adotamos todas as medidas exigidas pelo art. 32.º do RGPD (segurança do tratamento). As medidas atuais estão descritas na secção 7.
4. Respeitamos as condições do art. 28.º, n.ºs 2 e 4, para a contratação de subcontratantes ulteriores (ver secção 6).

5. Tendo em conta a natureza do tratamento e a informação de que dispomos, prestamos assistência ao responsável pelo tratamento na resposta aos pedidos dos titulares dos dados, na notificação de violações, nas avaliações de impacto e na consulta prévia às autoridades de controlo (art. 28.º, n.º 3, alíneas e) e f)).
6. Consoante a escolha do responsável pelo tratamento, no fim da prestação dos serviços apagamos ou devolvemos todos os dados pessoais do cliente e apagamos as cópias existentes, salvo se o direito da União ou de um Estado-Membro exigir a sua conservação.
7. Disponibilizamos ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento do art. 28.º e permitimos e contribuímos para auditorias, incluindo inspeções (ver secção 9).

4. Obrigações do responsável pelo tratamento

- O responsável pelo tratamento garante que tem um fundamento jurídico nos termos do art. 6.º (e, se for o caso, do art. 9.º) para os dados pessoais que coloca no espaço de trabalho.
- O responsável pelo tratamento é responsável pela exatidão dos dados pessoais do cliente e pela resposta aos pedidos dos titulares dos dados relativos ao seu espaço de trabalho (encaminhamos-lhe os pedidos que recebermos e prestamos assistência nos termos do art. 28.º, n.º 3, alínea e)).
- O responsável pelo tratamento controla o acesso (funções dos membros, convites a auditores, o portal público de comunicação) através das definições da plataforma.

5. Transferências internacionais

Por predefinição, os dados pessoais do cliente são armazenados na União Europeia. Quando um subcontratante ulterior tem sede fora da UE, as transferências regem-se pelas cláusulas contratuais-tipo da Comissão Europeia (Decisão 2021/914), módulo 3 (de subcontratante para subcontratante), com as medidas complementares descritas na secção 7. Os subcontratantes ulteriores atuais e as respetivas localizações constam de [/legal/subprocessors](#).

6. Subcontratantes ulteriores

1. O responsável pelo tratamento autoriza-nos a recorrer a subcontratantes ulteriores para prestar o serviço. A lista atual consta de [/legal/subprocessors](#).
2. Informamos o responsável pelo tratamento de qualquer adição ou substituição prevista com, pelo menos, 30 dias de antecedência, através da subscrição por e-mail dessa página ou por e-mail à pessoa proprietária do espaço de trabalho.
3. O responsável pelo tratamento pode opor-se por motivos razoáveis de proteção de dados. Se não pudermos atender à objeção, pode rescindir o serviço em causa e receber o reembolso proporcional da parte não utilizada do período de faturação em curso.
4. Impomos a cada subcontratante ulterior, por contrato escrito, obrigações de proteção de dados não menos protetoras do que as deste DPA, e continuamos responsáveis perante o responsável pelo tratamento pelo cumprimento das obrigações do subcontratante ulterior.

7. Medidas de segurança (art. 32.º)

- Cifragem. Os dados pessoais do cliente são cifrados em repouso com AES-256-GCM na camada de aplicação, além da cifragem do fornecedor de armazenamento. Todo o transporte é feito por HTTPS com HSTS pré-carregado, sem alternativa não cifrada. As chaves são derivadas por HKDF de um segredo principal guardado apenas nas variáveis de ambiente da infraestrutura de produção.
- Controlo de acesso. Controlo de acesso baseado em funções na plataforma (proprietário, administrador, membro, auditor); sessões de auditor limitadas no tempo e revogáveis. O acesso operacional está limitado a uma pequena equipa de suporte através do portal de suporte, que por conceção só mostra metadados.
- Autenticação. Início de sessão sem palavra-passe com código de utilização única. Tokens de sessão assinados

com HMAC e de duração limitada. Limitação de pedidos em cada ponto de acesso público, incluindo o início de sessão de administração.

- Resiliência e integridade. Registo de atividade só de acréscimo de cada ação que altera um estado. Cópias de segurança na UE. A integridade dos dados guardados é verificada por etiquetas de autenticação AEAD; um texto cifrado adulterado gera um erro e não é servido.
- Rede e cabeçalhos. Content-Security-Policy rigorosa com uma lista de scripts embutidos permitidos por hash, X-Frame-Options rigoroso, X-Content-Type-Options nosniff e HSTS pré-carregado.
- Gestão de vulnerabilidades. As dependências têm versões fixas; acompanhamos os avisos de segurança e aplicamos correções num prazo adequado à gravidade.

8. Violação de dados pessoais

Se tomarmos conhecimento de uma violação de dados pessoais que afete os dados pessoais do cliente, notificamos a pessoa proprietária do espaço de trabalho sem demora injustificada e, o mais tardar, 72 horas após termos tido conhecimento (art. 33.º, n.º 2). A notificação descreve, na medida do conhecido: a natureza da violação, as consequências prováveis, as medidas adotadas ou propostas e o ponto de contacto para mais informações. Prestamos assistência ao responsável pelo tratamento no cumprimento das suas próprias obrigações de notificação nos termos dos arts. 33.º e 34.º.

9. Auditorias

O responsável pelo tratamento (ou um auditor externo por ele mandatado) pode auditar o cumprimento deste DPA uma vez em cada doze meses, com um pré-aviso escrito de, pelo menos, 30 dias e durante o horário de expediente, de forma que não perturbe indevidamente as nossas operações e respeite a confidencialidade dos dados de outros clientes. Podemos cobrar uma taxa razoável por auditorias além deste limite. Quando uma obrigação de auditoria do art. 28.º, n.º 3, alínea h), puder ser cumprida com uma certificação de terceiros que detenhamos, fornecemos-la em vez de uma auditoria presencial.

10. Responsabilidade

A responsabilidade de cada parte ao abrigo deste DPA está sujeita aos limites dos termos de utilização. Esses limites não restringem a responsabilidade pelos danos sofridos pelos titulares dos dados nos termos do art. 82.º do RGPD.

11. Vigência e cessação

Este DPA aplica-se enquanto tratarmos dados pessoais do cliente e mantém-se após a cessação dos termos de utilização na medida e pelo tempo em que ainda detivermos esses dados. As secções 8 (violações), 9 (auditorias) e 12 (devolução e apagamento) mantêm-se após a cessação.

12. Devolução e apagamento

No fim do serviço, o responsável pelo tratamento pode exportar os dados do espaço de trabalho com as ferramentas de exportação da plataforma durante o período de tolerância de 30 dias dos termos de utilização. Após esse período, apagamos os dados pessoais do cliente; as cópias de segurança expiram de acordo com o nosso calendário de conservação. Os dados que somos obrigados a conservar (por exemplo, a faturação ao abrigo do direito comercial italiano) só são conservados durante o prazo dessa obrigação.

13. Ordem de prevalência

Em caso de conflito entre este DPA e os termos de utilização ou a política de privacidade, este DPA prevalece em matéria de tratamento de dados. As cláusulas contratuais-tipo incorporadas para uma transferência fora da UE

prevalecem sobre este DPA e os termos de utilização nas matérias que regulam.

14. Comunicações

- À Dazr: privacy@dazr.eu (proteção de dados) ou security@dazr.eu (incidentes).
- Ao responsável pelo tratamento: o e-mail da pessoa proprietária do espaço de trabalho registado no momento da comunicação.