

ISO/IEC 27018:2025, Segurança da informação, cibersegurança e proteção da privacidade: Diretrizes para a proteção de informação de identificação pessoal (PII) em nuvens públicas que atuam como subcontratantes de PII (3.ª edição, 2025-08)

Proteção de PII na nuvem pública

36 requisitos. Para esta norma não existe um certificado acreditado. Versão de 07/2026.

A ISO/IEC 27018 não é uma norma de sistema de gestão, mas sim um conjunto de diretrizes com controles adicionais sobre a base da ISO/IEC 27002:2022. Não existe um certificado acreditado autônomo para a ISO/IEC 27018. Os controles são incorporados na Declaração de Aplicabilidade de um sistema ISO/IEC 27001, e o certificado é então emitido em conformidade com a ISO/IEC 27001, com referência à ISO/IEC 27018. A norma dirige-se ao fornecedor de um serviço de computação em nuvem pública que trata informação de identificação pessoal por conta dos seus clientes do serviço na nuvem. Uma organização que apenas consome serviços na nuvem não assume esse papel e deve avaliar de forma sensata os requisitos perante os seus fornecedores, não perante si própria. Para a Leanshift, esta lista de verificação é, portanto, sobretudo uma grelha de avaliação de fornecedores. Cada ponto pode ser colocado ao fornecedor como uma pergunta e assegurado através do contrato de subcontratação nos termos do artigo 28.º do RGPD. O resultado dessa avaliação é um registo interno de conformidade ou um perfil de avaliação do fornecedor, não um certificado. Quanto à numeração: as cláusulas A.2 a A.12 seguem os princípios de privacidade do anexo A da norma, os pontos numerados como A.11.6 são os controles adicionais aí enumerados. Os pontos numerados como 8.10 ou 5.34 remetem para controles da ISO/IEC 27002:2022 que a norma torna específicos para a nuvem. Os pontos com o sufixo "(Grundsatz)", que significa princípio, derivam do princípio da própria cláusula, nos casos em que o anexo A não prevê um controlo adicional dedicado.

Empresa	Data	Elaborado por
---------	------	---------------

A.2 Consentimento e escolha2

A.2.1

O fornecedor do serviço de computação em nuvem apoia o cliente do serviço na nuvem a satisfazer os direitos dos titulares dos dados, como o acesso, a retificação, o apagamento e a oposição. As responsabilidades e os prazos são definidos contratualmente.

Documento

Como se comprova: Como evidência serve o contrato de subcontratação nos termos do artigo 28.º do RGPD, com uma cláusula de assistência ao exercício dos direitos dos titulares dos dados, juntamente com os meios técnicos do próprio serviço: funcionalidades de exportação, correção e eliminação, ou um procedimento de suporte documentado com um prazo de resposta. Pergunta ao fornecedor: que funcionalidade ou processo disponibiliza para que possamos atender um pedido de acesso ou de apagamento no prazo de um mês?

AbertoEm cursoCumpridoNão aplicável

Evidência / justificação

A.2 (Grundsatz)Informação de identificação pessoal pertencente aos clientes do serviço na nuvem só é tratada de acordo com as instruções documentadas do cliente. A obtenção do consentimento dos titulares dos dados continua a ser tarefa do cliente enquanto responsável pelo tratamento, e o fornecedor não se antecipa a essa tarefa.

Como se comprova: Como evidência serve a cláusula de instruções do contrato de subcontratação, juntamente com a prova de que o fornecedor não faz uso secundário dos dados, por exemplo a política de privacidade do serviço e a documentação do produto. Pergunta ao fornecedor: trata os dados dos nossos clientes de alguma forma fora das nossas instruções, por exemplo para melhoria do produto ou treino de modelos?

AbertoEm cursoCumpridoNão aplicável

Evidência / justificação

A.3 Legitimidade e especificação da finalidade2

A.3.1

A finalidade para a qual o fornecedor trata informação de identificação pessoal limita-se à prestação do serviço acordado e está identificada no contrato. Não ocorre qualquer tratamento para fins próprios do fornecedor.

Documento

Como se comprova: Como evidência serve o contrato de subcontratação que indica o objeto, a natureza, a finalidade e a duração do tratamento, bem como as categorias de titulares dos dados nos termos do artigo 28.º, n.º 3, do RGPD. Pergunta ao fornecedor: forneça o anexo contratual que descreve de forma exaustiva a finalidade do tratamento. Para organizações pequenas, basta o aditamento padrão de tratamento de dados do fornecedor, desde que contenha esta informação.

AbertoEm cursoCumpridoNão aplicável

Evidência / justificação

A.3.2	A informação de identificação pessoal confiada ao fornecedor não é utilizada para publicidade, marketing ou outros fins comerciais próprios do fornecedor sem consentimento expresso prévio. A prestação do serviço não é condicionada a esse consentimento.
	Como se comprova: Como evidência serve uma cláusula contratual explícita que exclua o uso comercial secundário, juntamente com os termos de serviço. Pergunta ao fornecedor: confirme por escrito que os dados dos clientes não são utilizados para publicidade, definição de perfis ou treino de modelos de IA. Caso esse compromisso não exista, o serviço não é adequado para informação de identificação pessoal.
	Aberto Em curso Cumprido Não aplicável
	Evidência / justificação

A.4 Limitação da recolha					1
A.4 (Grundsatz)	Para além dos dados que o cliente introduz no serviço, o fornecedor não recolhe informação de identificação pessoal adicional para fins próprios, como telemetria, perfis de utilização ou análise de conteúdo. Os dados operacionais e os metadados recolhidos estão identificados e justificados.				
	Como se comprova: Como evidência serve uma lista dos dados que o serviço regista além dos dados de conteúdo (registos de acesso, telemetria, dados de diagnóstico), com a respetiva finalidade e prazo de conservação, juntamente com uma captura de ecrã da definição que desativa a telemetria opcional. Pergunta ao fornecedor: que dados de utilização, telemetria e diagnóstico recolhe adicionalmente, para que os utiliza, e podemos desativar essa recolha?				
	Aberto	Em curso	Cumprido	Não aplicável	
	Evidência / justificação				

A.5 Minimização de dados2

A.5.1

Os ficheiros temporários criados durante o tratamento de informação de identificação pessoal, como armazenamento provisório, caches ou registos de reversão, são eliminados de forma segura dentro de um prazo definido.

Como se comprova: Como evidência serve um procedimento operacional ou de eliminação com um prazo de conservação definido para os dados temporários, suportado pela configuração do sistema, por exemplo um TTL de cache ou uma tarefa de limpeza agendada com o respetivo registo de execução. Pergunta ao fornecedor: ao fim de que prazo são eliminados as caches, os ficheiros temporários e os estados intermédios, e como é isso monitorizado?

Aberto

Em curso

Cumprido

Não aplicável

Evidência / justificação

8.11

Sempre que as operações, os testes ou o suporte não exijam dados reais, a informação de identificação pessoal é mascarada, pseudonimizada ou anonimizada. O volume de dados tratados mantém-se limitado ao que o serviço realmente necessita.

Como se comprova: Como evidência serve uma norma que determine quais os ambientes que podem aceder a dados reais, juntamente com capturas de ecrã ou scripts do mascaramento aplicado nos sistemas de teste e de desenvolvimento. Pergunta ao fornecedor: as suas equipas de suporte e desenvolvimento trabalham com dados de produção e, em caso afirmativo, sob que garantias? Para organizações pequenas, basta uma regra que estabeleça que os sistemas de teste funcionam exclusivamente com dados de amostra gerados.

Aberto

Em curso

Cumprido

Não aplicável

Evidência / justificação

A.6 Limitação da utilização, conservação e divulgação		3
A.6.1	Sempre que o fornecedor recebe um pedido juridicamente vinculativo de divulgação de informação de identificação pessoal, por exemplo de uma autoridade pública, informa previamente o cliente do serviço na nuvem, na medida em que a lei o permita.	
	Como se comprova: Como evidência serve uma cláusula contratual de notificação e um processo interno para pedidos de autoridades com um responsável designado. Pergunta ao fornecedor: notifica-nos antes de entregar dados, e publica um relatório de transparência sobre os pedidos das autoridades? Um relatório de transparência atualizado constitui uma evidência sólida.	
	Aberto Em curso Cumprido Não aplicável	
	Evidência / justificação	

A.6.2 Sempre que o fornecedor divulga informação de identificação pessoal a terceiros, regista o facto de forma rastreável: quem recebeu os dados, quando ocorreu, que dados estavam envolvidos e em que base assenta a divulgação. Documento

Como se comprova: Como evidência serve um registo de divulgações ou um histórico de pedidos de suporte com esses campos, mesmo que não contenha entradas. Um registo vazio mas mantido é aceitável e é a via prática para organizações pequenas. Pergunta ao fornecedor: mantém um registo das divulgações de dados, e podemos obter extratos dele?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

8.10 A informação de identificação pessoal é eliminada assim que expira o prazo de conservação acordado ou termina o contrato, incluindo as cópias mantidas em cópias de segurança após o respetivo ciclo de rotação.

Como se comprova: Como evidência serve um conceito de eliminação com prazos de conservação por categoria de dados, o prazo de conservação das cópias de segurança e um registo ou confirmação de eliminação. Pergunta ao fornecedor: durante quanto tempo os nossos dados permanecem nas suas cópias de segurança após a cessação do contrato, e recebemos confirmação por escrito da sua eliminação?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.7 Exatidão e qualidade

2

A.7 (Grund) O fornecedor não altera por iniciativa própria a informação de identificação pessoal que lhe é confiada. As correções e atualizações são efetuadas exclusivamente por instrução do cliente do serviço na nuvem ou através de funcionalidades operadas pelo próprio cliente.

Como se comprova: Como evidência servem as funcionalidades de edição do serviço juntamente com o respetivo histórico de alterações, além da cláusula de instruções do contrato de subcontratação. Pergunta ao fornecedor: podemos corrigir os registos nós próprios, e fica cada alteração registada de forma rastreável?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

8.13 A integridade da informação de identificação pessoal está protegida no armazenamento, na transmissão e na restauração. Existem cópias de segurança e a respetiva capacidade de restauro foi testada.

Como se comprova: Como evidência serve a configuração das cópias de segurança, os mecanismos de soma de verificação ou de integridade, e pelo menos um teste de restauro documentado por ano, com data e resultado. Pergunta ao fornecedor: com que frequência testa os restauros, e que tempo de recuperação assume no nível de serviço?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.8 Abertura, transparência e aviso

2

A.8.1 A utilização de subcontratantes que tratam informação de identificação pessoal é divulgada antes da celebração do contrato. As alterações à lista são notificadas ao cliente com a devida antecedência, de forma a que este possa opor-se ou resolver o contrato. Documento

Como se comprova: Como evidência serve uma lista atualizada de subcontratantes, publicada ou disponibilizada contratualmente, com nome, país e finalidade do tratamento, juntamente com uma regra de notificação nos termos do artigo 28.º, n.º 2, do RGPD. Pergunta ao fornecedor: onde encontramos a sua lista de subcontratantes, com que antecedência notifica as alterações, e como podemos opor-nos?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.8 (Grund) Antes da celebração do contrato, o fornecedor disponibiliza informação compreensível sobre a forma como a informação de identificação pessoal é tratada, quais as garantias existentes e em que jurisdições ocorre o tratamento.

Como se comprova: Como evidência servem a política de privacidade, um documento técnico de segurança, uma página de centro de confiança e o contrato de subcontratação com as medidas técnicas e organizativas em anexo. Pergunta ao fornecedor: forneça a lista atualizada das medidas técnicas e organizativas como anexo contratual, não apenas como material de marketing.

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.9 Participação individual e acesso

2

A.9 (Grundsatz) O serviço disponibiliza ao cliente do serviço na nuvem os meios técnicos para atender por si próprio os pedidos de acesso, retificação e apagamento dos titulares dos dados, por exemplo através de funcionalidades de exportação, pesquisa e eliminação.

Como se comprova: Como evidência serve a documentação do produto sobre as funcionalidades de exportação e eliminação, apoiada por um ensaio interno: tramitar um pedido de acesso do início ao fim e registar quanto tempo demora. Pergunta ao fornecedor: conseguimos localizar, exportar e eliminar todos os dados relativos a uma única pessoa sem o seu suporte?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

5.34 Quando o cliente não consegue tratar por si próprio um pedido de um titular dos dados, o fornecedor presta assistência dentro de um prazo acordado. Os pedidos que os titulares dos dados enviam diretamente ao fornecedor são reencaminhados para o cliente, em vez de serem respondidos pelo fornecedor.

Como se comprova: Como evidência serve a respetiva cláusula do contrato de subcontratação com um prazo de resposta concreto, juntamente com um histórico de pedidos de suporte como exemplo real. Pergunta ao fornecedor: que prazo assume para a assistência ao exercício dos direitos dos titulares dos dados, e qual é o custo?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.10 Responsabilização

4

A.10.1 As violações de segurança que envolvam informação de identificação pessoal são comunicadas ao cliente do serviço na nuvem sem demora injustificada, indicando o âmbito, os dados afetados, a causa e as medidas adotadas. É definido um processo de notificação com responsabilidades e prazos.

[Documento](#)

Como se comprova: Como evidência serve o plano de resposta a incidentes com a respetiva cadeia de escalonamento, o prazo contratual de notificação (entre 24 e 48 horas funciona na prática, de modo a que o cliente ainda consiga cumprir o prazo de 72 horas do artigo 33.º do RGPD) e os registos de incidentes anteriores ou de um exercício de simulação. Pergunta ao fornecedor: em que prazo comunica um incidente, por que canal, e que informação fornece juntamente com a notificação?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.10.2 As políticas de segurança, os procedimentos operacionais e os registos correspondentes são conservados durante um prazo definido, de modo a que o tratamento possa ser reconstituído a posteriori.

[Documento](#)

Como se comprova: Como evidência serve uma regra de conservação com o histórico de versões das políticas, por exemplo através de um registo documental ou de um sistema de controlo de versões com a data de aprovação. Pergunta ao fornecedor: durante quanto tempo conserva as versões das políticas e os registos correspondentes, e temos acesso a eles em caso de auditoria?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.10.3 Existe um procedimento definido para a devolução, transferência e destruição da informação de identificação pessoal no final do contrato, especificando formatos, prazos e o tratamento das cópias.

[Documento](#)

Como se comprova: Como evidência serve a cláusula de saída do contrato de subcontratação, juntamente com uma confirmação de eliminação após o termo do contrato. Pergunta ao fornecedor: em que formato e em que prazo recuperamos os nossos dados, quando são destruídas todas as cópias, e recebemos confirmação por escrito?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

5.35 A eficácia das garantias é revista de forma independente a intervalos regulares, por exemplo através de auditorias internas, testes de intrusão ou relatórios de garantia de terceiros. Os resultados são disponibilizados ao cliente do serviço na nuvem de forma adequada.

Como se comprova: Como evidência serve um certificado ISO/IEC 27001 com uma Declaração de Aplicabilidade que inclua os controlos da ISO/IEC 27018, ou um relatório SOC 2, juntamente com resumos atualizados de testes de intrusão. Pergunta ao fornecedor: forneça o certificado, o respetivo âmbito e a confirmação de que a ISO/IEC 27018 se reflete na Declaração de Aplicabilidade. Verifique se o âmbito cobre realmente o serviço que utiliza.

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.11 Segurança da informação

13

A.11.1 Todas as pessoas com acesso a informação de identificação pessoal estão vinculadas a um dever de confidencialidade, quer sejam colaboradores diretos, quer prestadores externos.

[Documento](#)

Como se comprova: Como evidência servem os acordos ou compromissos de confidencialidade assinados que permanecem em vigor após o termo da relação. Pergunta ao fornecedor: todos os colaboradores e prestadores de serviços com acesso aos dados estão vinculados por escrito a um compromisso de confidencialidade?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.11.2 As impressões e outras cópias em papel que contenham informação de identificação pessoal só são criadas quando estritamente necessário. O âmbito permitido é regulado por uma norma.

Como se comprova: Como evidência serve uma norma sobre o tratamento de impressões, que nos centros de dados corresponde tipicamente a uma proibição geral de imprimir nas áreas onde se encontram dados de clientes. Pergunta ao fornecedor: chegam a ser impressos dados de clientes nas suas operações e, em caso afirmativo, em que condições?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.11.3 As restaurações a partir de cópias de segurança são autorizadas previamente e registadas, incluindo a pessoa que iniciou a restauração e os dados afetados.

[Documento](#)

Como se comprova: Como evidência serve o registo de restaurações com data e hora, origem e âmbito, normalmente gerado de forma automática pela ferramenta de cópia de segurança. Pergunta ao fornecedor: regista todas as restaurações, e podemos consultar esses registos em caso de auditoria?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.11.4 Os suportes de armazenamento com informação de identificação pessoal que saem das instalações são protegidos contra o acesso não autorizado e a perda, regra geral através de cifragem e de um registo de transporte.

Como se comprova: Como evidência serve a prova da cifragem (cifragem completa do suporte), os registos de transporte e entrega, e um inventário de suportes. Pergunta ao fornecedor: saem alguma vez das suas instalações suportes com dados de clientes, por exemplo para cópias de segurança, e como são protegidos durante o transporte?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.11.5 A utilização de suportes e dispositivos portáteis não cifrados para informação de identificação pessoal é proibida ou limitada a exceções justificadas com aprovação documentada.

Como se comprova: Como evidência serve uma política de suportes amovíveis, juntamente com a respetiva aplicação técnica, por exemplo cifragem obrigatória de dispositivos ou bloqueio de portas USB através de gestão de dispositivos. Pergunta ao fornecedor: os colaboradores podem copiar dados de clientes para dispositivos não cifrados, e o que impede isso tecnicamente?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.11.6 A informação de identificação pessoal transmitida através de redes públicas é cifrada. Os mecanismos utilizados refletem o estado da técnica atual.

Como se comprova: Como evidência serve a configuração TLS (versão de protocolo atual, sem cifras obsoletas) e um teste externo de configuração documentado num relatório. Prático para organizações pequenas: realizar uma verificação TLS gratuita uma vez por ano e arquivar o resultado. Pergunta ao fornecedor: que cifragem de transporte aplica de forma obrigatória, e a cifragem em repouso está ativa?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.11.7 Os registos em papel que contenham informação de identificação pessoal são destruídos de forma a excluir qualquer reconstituição.

Como se comprova: Como evidência servem trituradoras de papel com um nível de segurança adequado ou certificados de destruição de um prestador de serviços que trabalhe segundo a norma DIN 66399 ou uma norma equivalente. Pergunta ao fornecedor: como destrói os registos em papel relativos a clientes, e existem certificados de destruição arquivados?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.11.8 Os identificadores de utilizador são atribuídos de forma exclusiva a uma pessoa e não são reatribuídos nem partilhados. As contas partilhadas só existem em exceções justificadas e com rastreabilidade adicional.

Como se comprova: Como evidência serve uma lista de utilizadores do sistema de identidade sem contas de grupo, juntamente com a regra de que os trabalhos administrativos são realizados a partir de uma conta pessoal. Pergunta ao fornecedor: o seu pessoal de operações trabalha com contas pessoais, e a autenticação multifator é obrigatória?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.11.9 O fornecedor consegue indicar a qualquer momento quais as pessoas ou funções autorizadas a aceder à informação de identificação pessoal, e mantém essa visão geral atualizada.

[Documento](#)

Como se comprova: Como evidência serve uma visão geral dos direitos de acesso por função, apoiada por uma revisão periódica de acessos com data e resultado. Para organizações pequenas, basta uma exportação semestral da lista de utilizadores, com aprovação registada. Pergunta ao fornecedor: quantos dos seus colaboradores podem aceder aos nossos dados, e com que frequência revê isso?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.11.10 As contas de utilizador são geridas ao longo de todo o seu ciclo de vida: criação, alteração e desativação imediata quando alguém sai da organização ou muda de função.

Como se comprova: Como evidência serve um procedimento de admissão e saída com uma lista de verificação, juntamente com registos de contas desativadas com data e hora. Pergunta ao fornecedor: em que prazo retira o acesso aos colaboradores que saem, e como o comprova?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.11.11 As obrigações de segurança e privacidade do fornecedor são fixadas contratualmente, incluindo as medidas técnicas e organizativas, o carácter vinculativo das instruções do cliente e o direito de auditoria do cliente.

[Documento](#)

Como se comprova: Como evidência serve o contrato de subcontratação assinado nos termos do artigo 28.º do RGPD, com o anexo de medidas e um direito de auditoria ou de informação. Pergunta ao fornecedor: forneça o contrato de subcontratação assinado, incluindo os respetivos anexos, e não apenas uma remissão para as condições gerais de serviço.

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.11.12 Os subcontratantes que tratam informação de identificação pessoal estão sujeitos, no mínimo, às mesmas obrigações que o próprio fornecedor. A sua seleção e a monitorização contínua são regidas por um processo definido.

Como se comprova: Como evidência serve a transposição das obrigações nos contratos com os subcontratantes (artigo 28.º, n.º 4, do RGPD) e uma avaliação de fornecedores com data. Pergunta ao fornecedor: como avalia os seus subcontratantes, e que evidências lhes exige?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.11.13 Antes de o espaço de armazenamento ser reutilizado, é assegurado que não permanecem acessíveis dados de utilizadores anteriores, nem em suportes físicos nem em ambientes virtualizados.

Como se comprova: Como evidência serve o procedimento de saneamento ou substituição aplicado quando o armazenamento é libertado, os registos de destruição de suportes e a separação entre clientes descrita no documento de arquitetura. Pergunta ao fornecedor: como assegura que o armazenamento reutilizado não contém dados residuais de outros clientes?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.12 Conformidade em matéria de privacidade

3

A.12.1 Os países em que a informação de identificação pessoal é armazenada e tratada estão identificados e são do conhecimento do cliente do serviço na nuvem. As alterações às localizações de armazenamento são notificadas.

[Documento](#)

Como se comprova: Como evidência serve a visão geral de locais e regiões do fornecedor, no contrato ou na documentação, juntamente com uma captura de ecrã da definição de região do serviço utilizado. Pergunta ao fornecedor: em que países ficam armazenados os nossos dados em repouso, a partir de que países é feito o acesso, por exemplo no suporte, e podemos fixar a região?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

A.12.2 As transferências de informação de identificação pessoal para países terceiros são conhecidas, justificadas e cobertas por garantias adequadas.

[Documento](#)

Como se comprova: Como evidência servem as cláusulas contratuais tipo ou uma decisão de adequação, apoiadas por uma avaliação de impacto da transferência, que em organizações pequenas pode ser breve: categorias de dados afetadas, país de destino, risco, medidas adicionais adotadas. Pergunta ao fornecedor: em que base legal assenta a transferência de dados para países terceiros, e que medidas suplementares aplica?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação

5.31 Os requisitos legais e contratuais aplicáveis ao tratamento da informação de identificação pessoal estão identificados e são mantidos atualizados à medida que a situação legal muda. São avaliados os conflitos entre jurisdições.

Como se comprova: Como evidência serve uma visão geral dos requisitos aplicáveis (RGPD, normas nacionais, obrigações setoriais) com um responsável e uma data de revisão. Numa organização pequena, basta uma lista de uma página revista anualmente. Pergunta ao fornecedor: está sujeito, ou os seus subcontratantes estão sujeitos, a jurisdições que permitam às autoridades aceder aos nossos dados, e como lida com isso?

Aberto Em curso Cumprido Não aplicável

Evidência / justificação