

Wentz Vieira Hentges & Schettert
ADVOCACIA EMPRESARIAL

VERSÃO 1.0 · OUTUBRO DE 2026

GUIA ORIENTATIVO · PROTEÇÃO DE DADOS

CHECKLIST DE PROTEÇÃO DE DADOS EM CONTRATOS COM FORNECEDORES DE TI

Ferramenta prática para verificar se os contratos com terceiros que acessam dados pessoais da empresa estão protegidos. São 38 itens, com o fundamento legal de cada um.

APRESENTAÇÃO

Por que olhar para os contratos com fornecedores de TI

Sistemas de folha de pagamento, plataformas de CRM, serviços de nuvem, ERP, e-mail corporativo e suporte técnico terceirizado fazem parte da rotina de qualquer empresa. Em todos esses casos, um terceiro passa a tratar dados pessoais de clientes e colaboradores em nome dela.

A LGPD não transfere ao fornecedor a responsabilidade da empresa contratante. Ela continua sendo a controladora dos dados e precisa demonstrar que deu instruções claras, exigiu medidas de segurança e acompanhou a execução do serviço. O contrato é o principal instrumento para isso.

Este guia reúne, em formato de checklist, os pontos que um contrato com fornecedor de tecnologia deve cobrir sob a ótica da proteção de dados e da segurança da informação, com o fundamento legal de cada item.

PARA QUEM É

Jurídico, compras e suprimentos, tecnologia da informação, segurança da informação e encarregado pelo tratamento de dados pessoais.

QUANDO USAR

Na contratação de novo fornecedor, na renovação de contrato e na revisão periódica dos fornecedores que já tratam dados da empresa.

COMO USAR EM QUATRO ETAPAS

01 Classifique o fornecedor
Responda à etapa 1 para definir o nível de criticidade da contratação e o alcance da análise.

02 Aplique o checklist
Com o contrato, os anexos e os termos do fornecedor em mãos, marque uma resposta para cada item da etapa 2.

03 Apure o resultado
Some os pontos de cada bloco na etapa 3 e identifique o que precisa de ajuste.

04 Registre o plano de ação
Na etapa 4, defina ajustes, responsáveis e prazos, e documente os riscos aceitos.

COMO RESPONDER

Sim 2 PONTOS	O contrato trata do ponto de forma clara e suficiente.
Parcial 1 PONTO	O ponto aparece, mas de forma genérica, incompleta ou sem prazo.
Não 0 PONTO	O contrato não trata do ponto.
N.A. FORA DO CÁLCULO	O item não se aplica a essa contratação.

ESSENCIAL Item indispensável. Resposta **Não** indica prioridade alta, qualquer que seja a pontuação do bloco.

Baixe o arquivo antes de preencher. Ele funciona em leitores de PDF como o Adobe Acrobat Reader e no navegador, e também pode ser impresso. Use uma cópia por fornecedor.



O que a LGPD espera dessa relação

O contrato é o lugar em que a empresa registra as instruções ao fornecedor (art. 39), define as medidas de segurança exigidas (art. 46) e reúne a prova de que agiu com diligência (art. 6º, X).

CONTROLADORA

A empresa contratante

A quem competem as decisões sobre o tratamento dos dados pessoais (art. 5º, VI). Define finalidades, instruções e critérios de segurança, e comunica os incidentes relevantes (art. 48).

OPERADOR

O fornecedor

Realiza o tratamento em nome do controlador (art. 5º, VII) e deve seguir as instruções recebidas (art. 39). Responde solidariamente se descumprir a lei ou essas instruções (art. 42, § 1º, I).

O serviço pode ser terceirizado. A responsabilidade pelo tratamento, não.

Nem todo fornecedor é apenas operador. Quando usa os dados para finalidades próprias, por exemplo para aprimorar produtos ou treinar modelos de inteligência artificial, ele também decide sobre o tratamento e passa a atuar como controlador nessa parte. O contrato precisa delimitar o que é permitido.

Nem todo terceiro trata dados pessoais. Fornecedores sem acesso a dados de clientes ou colaboradores ficam fora deste checklist, embora continuem sujeitos às regras gerais de segurança da informação da empresa.

CONTEXTO NORMATIVO

Deveres que o contrato ajuda a cumprir e a provar

Instruções	O operador trata os dados segundo as instruções do controlador, que verifica a sua observância.	ART. 39
Registro	Controlador e operador mantêm registro das operações de tratamento que realizam.	ART. 37
Segurança	Os agentes adotam medidas aptas a proteger os dados. O dever alcança quem intervém no tratamento, mesmo após o seu término.	ARTS. 46 E 47
Incidentes	O controlador comunica à ANPD e aos titulares o incidente que possa acarretar risco ou dano relevante.	ART. 48
Exterior	A transferência internacional só ocorre nas hipóteses legais, como país com adequação reconhecida ou cláusulas-padrão.	ART. 33
Término	Encerrado o tratamento, os dados são eliminados, ressalvadas as hipóteses legais de conservação.	ARTS. 15 E 16
Prova	O agente deve demonstrar a adoção de medidas eficazes e capazes de comprovar o cumprimento da lei.	ART. 6º, X

RESPONSABILIDADE CIVIL

O controlador ou o operador que causar dano em violação à legislação é obrigado a repará-lo (art. 42). O operador responde solidariamente quando descumprir a lei ou não seguir as instruções lícitas do controlador (art. 42, § 1º, I), e quem reparar o dano tem direito de regresso contra os demais responsáveis, na medida da sua participação (art. 42, § 4º). **Sem instruções e deveres documentados, essa participação fica difícil de demonstrar.**

ESFERA ADMINISTRATIVA

A multa simples pode chegar a 2% do faturamento no Brasil, limitada a R$ 50 milhões por infração (art. 52, II). Na dosimetria, a ANPD considera a adoção reiterada e demonstrada de mecanismos internos capazes de minimizar o dano e a adoção de política de boas práticas e governança (art. 52, § 1º, VIII e IX). **Contratos bem estruturados fazem parte dessa demonstração.**



PRAZOS E REGRAS

Números que mudam a negociação

São obrigações da empresa, mas o cumprimento depende de informações e condutas do fornecedor. Por isso, o contrato precisa tratar delas de forma expressa.

3 dias úteis

Prazo da empresa para comunicar à ANPD e aos titulares o incidente que possa acarretar risco ou dano relevante, contado do conhecimento de que o incidente afetou dados pessoais. Em dobro para agentes de tratamento de pequeno porte.

RESOLUÇÕES CD/ANPD Nº 15/2024 E Nº 2/2022

Nenhum

Prazo legal para o fornecedor avisar a empresa sobre o incidente. A LGPD não o fixa. Se não estiver no contrato, a empresa depende da iniciativa do fornecedor.

ITEM D1 DESTE GUIA

5 anos

Prazo mínimo de guarda, pelo controlador, do registro de incidentes, inclusive dos que não foram comunicados à ANPD.

RESOLUÇÃO CD/ANPD Nº 15/2024

23/08/2025

Fim do prazo para incorporar as cláusulas-padrão da ANPD aos contratos que amparam transferências internacionais por meio de cláusulas. Elas devem ser adotadas na íntegra, sem alteração.

RESOLUÇÃO CD/ANPD Nº 19/2024

Jan. 2026

Brasil e União Europeia formalizaram o reconhecimento mútuo de adequação. Transferências do Brasil para países da União Europeia deixam de depender das cláusulas-padrão.

DECISÃO DE ADEQUAÇÃO DA ANPD

2%

Limite da multa simples por infração: até 2% do faturamento no Brasil, limitada a R$ 50 milhões. Boas práticas e mecanismos internos demonstrados são considerados na dosimetria.

LGPD, ART. 52, II, E § 1º, VIII E IX

Quando o fornecedor não negocia o contrato

Grandes provedores de nuvem e de software costumam oferecer termos padronizados, sem negociação. Nesses casos, aplique o checklist aos termos de serviço, ao acordo de tratamento de dados publicado pelo fornecedor (DPA) e à sua documentação de segurança. O que não estiver coberto deve ser tratado por configuração do serviço, por controle interno ou por aceite formal de risco, registrado na etapa 4.

ETAPA 1

Identificação e criticidade do fornecedor

A criticidade define o alcance da análise. Um serviço de suporte eventual não exige o mesmo rigor que uma plataforma que armazena toda a base de clientes.

FORNECEDOR

SERVIÇO CONTRATADO

CONTRATO E VERSÃO ANALISADOS

ÁREA RESPONSÁVEL PELA CONTRATAÇÃO

RESPONSÁVEL PELA AVALIAÇÃO

DATA DA AVALIAÇÃO

MARQUE UMA OPÇÃO POR CRITÉRIO

Dados tratados	☐ **1** · Cadastrais e de contato	☐ **2** · De clientes ou colaboradores além do cadastro	☐ **3** · Sensíveis, de crianças e adolescentes ou financeiros
Forma de acesso	☐ **1** · Eventual e supervisionado	☐ **2** · Recorrente, nos sistemas da empresa	☐ **3** · Armazena ou processa em ambiente próprio
Abrangência	☐ **1** · Grupo restrito de titulares	☐ **2** · Parte relevante da base	☐ **3** · Toda ou quase toda a base
Localização	☐ **1** · Somente no Brasil	☐ **2** · Exterior, com local identificado	☐ **3** · Local não informado
Dependência	☐ **1** · Substituível sem impacto relevante	☐ **2** · Falha afeta processos internos	☐ **3** · Falha interrompe a operação ou o atendimento

SOMA DOS PONTOS

☐ **Nível 1** · 5 A 7 PONTOS
Responda, no mínimo, aos itens essenciais.

☐ **Nível 2** · 8 A 11 PONTOS
Responda a todos os itens.

☐ **Nível 3** · 12 A 15 PONTOS
Responda a todos os itens, exija evidências documentais e reavalie ao menos uma vez por ano.

Classifique como **nível 3**, qualquer que seja a soma, o fornecedor que armazena ou processa em ambiente próprio dados sensíveis ou de crianças e adolescentes.

ETAPA 2

Checklist do contrato

Marque uma resposta por item. **Sim** vale 2 pontos, **Parcial** vale 1 e **Não** vale 0. Itens marcados como **N.A.** ficam fora do cálculo. Um **Não** em item ESSENCIAL indica prioridade alta, qualquer que seja a pontuação.

A Bloco A. Enquadramento da relação

Antes de avaliar cláusulas, confirme quem decide sobre o tratamento e o que, de fato, o fornecedor faz com os dados.

ITEM	REQUISITO	VERIFIQUE	BASE	SIM	PARCIAL	NÃO	N.A.
A1 ESSENCIAL	**O contrato identifica o papel de cada parte no tratamento: controladora, operador ou controladores conjuntos.**	A qualificação corresponde ao que o fornecedor faz na prática, e não apenas ao rótulo usado no contrato.	LGPD, ART. 5º, VI E VII · GUIA ANPD DE AGENTES DE TRATAMENTO	☐	☐	☐	☐
A2	**O contrato ou um anexo descreve os dados pessoais tratados, as categorias de titulares e as finalidades do tratamento.**	A descrição é específica. Expressões como "quaisquer dados necessários" não delimitam o tratamento.	LGPD, ART. 6º, I A III, E ART. 37	☐	☐	☐	☐
A3	**Há indicação expressa quando o serviço envolve dados sensíveis ou dados de crianças e adolescentes, com salvaguardas próprias.**	Exemplos: dados de saúde em sistemas de RH, biometria em controle de acesso, dados de dependentes.	LGPD, ARTS. 11 E 14	☐	☐	☐	☐
A4	**O fornecedor indica um ponto de contato para privacidade e segurança da informação, como encarregado ou equipe responsável.**	O contato está atualizado e é capaz de responder a solicitações e incidentes.	RESOLUÇÃO CD/ANPD Nº 18/2024, ART. 6º	☐	☐	☐	☐

OBSERVAÇÕES DO BLOCO A

B Bloco B. Instruções e limites de uso

O operador só pode tratar os dados conforme as instruções da empresa. O contrato é onde essas instruções ficam registradas.

ITEM	REQUISITO	VERIFIQUE	BASE	SIM	PARCIAL	NÃO	N.A.
B1 ESSENCIAL	**O fornecedor trata os dados apenas conforme instruções documentadas da empresa.**	As instruções estão no contrato, em anexo ou em canal formal definido, e não apenas em conversas informais.	LGPD, ART. 39	☐	☐	☐	☐
B2 ESSENCIAL	**É vedado o uso dos dados para finalidades próprias do fornecedor, inclusive comercialização, criação de perfis e treinamento de modelos de inteligência artificial, salvo autorização expressa.**	Leia os termos de uso e a política de privacidade do serviço, onde essas permissões costumam aparecer.	LGPD, ART. 6º, I E III, E ART. 39	☐	☐	☐	☐

B Bloco B. Instruções e limites de uso (continuação)

ITEM	REQUISITO	VERIFIQUE	BASE	SIM	PARCIAL	NÃO	N.A.
B3	**O fornecedor deve avisar a empresa se considerar uma instrução contrária à lei ou se não puder cumpri-la.**	Há canal e prazo para esse aviso.	LGPD, ART. 39, E ART. 42, § 1º, I	☐	☐	☐	☐
B4	**O fornecedor apoia o atendimento aos direitos dos titulares e repassa à empresa, em prazo definido, as solicitações que receber.**	O prazo de repasse é compatível com o prazo de resposta ao titular, que pode ser de 15 dias.	LGPD, ARTS. 18 E 19	☐	☐	☐	☐
B5	**O fornecedor mantém registro das operações de tratamento que realiza em nome da empresa.**	O registro pode ser solicitado pela empresa quando necessário.	LGPD, ART. 37	☐	☐	☐	☐

OBSERVAÇÕES DO BLOCO B

C Bloco C. Segurança da informação

A segurança que o titular pode esperar é dever de todos os agentes. O contrato deve dizer quais medidas o fornecedor mantém e como a empresa pode verificá-las.

ITEM	REQUISITO	VERIFIQUE	BASE	SIM	PARCIAL	NÃO	N.A.
C1 ESSENCIAL	**As medidas técnicas e administrativas de segurança estão descritas no contrato, em anexo ou em documento verificável.**	Controle de acesso, autenticação multifator, criptografia, cópias de segurança, registro de acessos e gestão de vulnerabilidades.	LGPD, ARTS. 46 E 47 · ISO/IEC 27001:2022, 5.20	☐	☐	☐	☐
C2	**O acesso aos dados é restrito a pessoas autorizadas, e o dever de confidencialidade alcança empregados e prestadores do fornecedor.**	O fornecedor se compromete a orientar e treinar quem tem acesso.	LGPD, ART. 47	☐	☐	☐	☐
C3	**O fornecedor informa certificações ou relatórios independentes de segurança, e a empresa acompanha a validade desses documentos.**	Exemplos: certificado ISO/IEC 27001 e relatório SOC 2, com escopo que inclua o serviço contratado.	BOA PRÁTICA · ISO/IEC 27001:2022, 5.19	☐	☐	☐	☐
C4	**A empresa pode solicitar evidências ou realizar auditoria, com forma, periodicidade e aviso prévio definidos.**	Na impossibilidade de auditoria presencial, há alternativa documental, como questionário e relatórios.	LGPD, ART. 39	☐	☐	☐	☐

C Bloco C. Segurança da informação (continuação)

ITEM	REQUISITO	VERIFIQUE	BASE	SIM	PARCIAL	NÃO	N.A.
C5	**Há níveis de serviço, cópias de segurança e plano de recuperação compatíveis com a criticidade do serviço.**	Tempo de restabelecimento e periodicidade de cópias estão definidos e são testados.	LGPD, ART. 46 · ISO/IEC 27001:2022, 5.30 E 8.13	☐	☐	☐	☐
C6	**O fornecedor comunica com antecedência mudanças relevantes que afetem a segurança, como troca de infraestrutura ou do local de tratamento.**	A empresa pode se opor ou rever a contratação diante da mudança.	ISO/IEC 27001:2022, 5.22	☐	☐	☐	☐

OBSERVAÇÕES DO BLOCO C

D Bloco D. Incidentes de segurança

Quem comunica o incidente à ANPD e aos titulares é a empresa, em três dias úteis. Ela depende do fornecedor para saber do fato e reunir as informações.

ITEM	REQUISITO	VERIFIQUE	BASE	SIM	PARCIAL	NÃO	N.A.
D1 ESSENCIAL	**O prazo para o fornecedor avisar a empresa sobre incidente está definido em horas, contadas da ciência do fato.**	Expressões como "em tempo razoável" não fixam prazo. Como referência de mercado, adotam-se 24 a 48 horas.	LGPD, ART. 48 · RESOLUÇÃO CD/ANPD Nº 15/2024	☐	☐	☐	☐
D2	**O aviso tem conteúdo mínimo definido: natureza do incidente, dados e titulares afetados, riscos, medidas adotadas e contato.**	O conteúdo permite à empresa avaliar o risco e preencher a comunicação à ANPD.	LGPD, ART. 48, § 1º	☐	☐	☐	☐
D3	**O fornecedor deve cooperar na investigação e na contenção, preservar evidências e fornecer as informações necessárias.**	Há responsável técnico designado e canal disponível também fora do horário comercial, quando o serviço for crítico.	LGPD, ARTS. 39 E 48 · BOA PRÁTICA	☐	☐	☐	☐
D4	**A comunicação à ANPD e aos titulares é coordenada pela empresa, e o fornecedor não se manifesta publicamente sobre o incidente sem alinhamento prévio.**	O contrato distingue o aviso à empresa da comunicação oficial.	LGPD, ART. 48	☐	☐	☐	☐

OBSERVAÇÕES DO BLOCO D

E Bloco E. Subcontratação

Quando o fornecedor repassa parte do serviço a terceiros, os dados passam por outras empresas. A cadeia precisa ser conhecida e autorizada.

ITEM	REQUISITO	VERIFIQUE	BASE	SIM	PARCIAL	NÃO	N.A.
E1 ESSENCIAL	**A subcontratação de terceiros que tratem os dados depende de autorização prévia da empresa, específica ou geral com aviso e direito de oposição.**	Inclui serviços de hospedagem, suporte e processamento usados pelo fornecedor.	LGPD, ART. 39 · GUIA ANPD DE AGENTES DE TRATAMENTO	☐	☐	☐	☐
E2	**O fornecedor mantém lista atualizada dos suboperadores, com o serviço prestado e o local de tratamento.**	A lista está disponível para consulta, inclusive em página pública do fornecedor.	BOA PRÁTICA · ISO/IEC 27001:2022, 5.21	☐	☐	☐	☐
E3	**Os suboperadores ficam sujeitos a obrigações equivalentes, e o fornecedor responde por eles perante a empresa.**	As obrigações de segurança, sigilo e incidentes são repassadas por escrito.	LGPD, ART. 42, § 1º, I	☐	☐	☐	☐

OBSERVAÇÕES DO BLOCO E

F Bloco F. Transferência internacional

Serviços de nuvem e suporte remoto costumam levar dados ao exterior. Cada transferência precisa de um mecanismo previsto em lei.

ITEM	REQUISITO	VERIFIQUE	BASE	SIM	PARCIAL	NÃO	N.A.
F1	**O contrato informa os países em que os dados são armazenados ou acessados, inclusive por suporte remoto e suboperadores.**	Verifique as opções de residência de dados oferecidas pelo serviço.	LGPD, ART. 33	☐	☐	☐	☐
F2 ESSENCIAL	**Cada transferência internacional tem mecanismo válido: país com adequação reconhecida pela ANPD, cláusulas-padrão contratuais ou outra hipótese do art. 33.**	Para destinos sem adequação reconhecida, como os Estados Unidos, o mecanismo usual são as cláusulas-padrão da ANPD.	LGPD, ART. 33 · RESOLUÇÃO CD/ANPD Nº 19/2024	☐	☐	☐	☐
F3	**Quando o mecanismo são as cláusulas-padrão da ANPD, elas foram incorporadas na íntegra, sem alteração do texto aprovado.**	Modelos estrangeiros, como as cláusulas da União Europeia, não substituem as da ANPD sem reconhecimento de equivalência.	RESOLUÇÃO CD/ANPD Nº 19/2024	☐	☐	☐	☐

OBSERVAÇÕES DO BLOCO F

G Bloco G. Responsabilidade e garantias

O contrato não afasta a responsabilidade da empresa perante o titular, mas define como o prejuízo causado pelo fornecedor será suportado entre as partes.

ITEM	REQUISITO	VERIFIQUE	BASE	SIM	PARCIAL	NÃO	N.A.
G1 ESSENCIAL	**O fornecedor responde pelos danos decorrentes do descumprimento da LGPD ou das instruções da empresa, com previsão de ressarcimento.**	A cláusula se aplica também a danos causados por suboperadores.	LGPD, ART. 42, § 1º, I, E § 4º	☐	☐	☐	☐
G2	**A limitação de responsabilidade do contrato não exclui nem reduz a valor irrisório os danos ligados a dados pessoais e segurança da informação.**	Confira o teto de responsabilidade, as exclusões e se há exceção para violação de dados.	BOA PRÁTICA	☐	☐	☐	☐
G3	**Está definido quem arca com os custos de resposta a incidente causado pelo fornecedor, como investigação, comunicação a titulares e apoio técnico.**	Os custos internos da empresa também estão contemplados.	LGPD, ART. 42, § 4º · BOA PRÁTICA	☐	☐	☐	☐
G4	**Para fornecedores de nível 3, há exigência de seguro de responsabilidade cibernética compatível com o risco.**	A apólice cobre o serviço contratado e está vigente.	BOA PRÁTICA	☐	☐	☐	☐

OBSERVAÇÕES DO BLOCO G

H Bloco H. Encerramento do contrato

O fim do contrato é um dos momentos de maior exposição: dados podem permanecer em ambientes que a empresa não controla mais.

ITEM	REQUISITO	VERIFIQUE	BASE	SIM	PARCIAL	NÃO	N.A.
H1 ESSENCIAL	**Ao fim do contrato, o fornecedor devolve os dados em formato utilizável e, em seguida, os elimina, inclusive cópias e backups, em prazo definido.**	Formato, prazo e responsável pela devolução estão claros.	LGPD, ARTS. 15 E 16	☐	☐	☐	☐
H2	**A eliminação é comprovada por declaração ou certificado, ressalvadas as hipóteses legais de conservação.**	A empresa guarda o comprovante junto ao registro do fornecedor.	LGPD, ART. 16, E ART. 6º, X	☐	☐	☐	☐

H Bloco H. Encerramento do contrato (continuação)

ITEM	REQUISITO	VERIFIQUE	BASE	SIM	PARCIAL	NÃO	N.A.
H3	**Os deveres de confidencialidade e de segurança permanecem após o término do contrato.**	A cláusula de sobrevivência inclui as obrigações de proteção de dados.	LGPD, ART. 47	☐	☐	☐	☐
H4	**Há rotina para revogar acessos, credenciais e integrações do fornecedor no encerramento.**	A rotina inclui contas de serviço e chaves de integração.	ISO/IEC 27001:2022, 5.18	☐	☐	☐	☐

OBSERVAÇÕES DO BLOCO H

I Bloco I. Gestão contínua do fornecedor

O contrato é o ponto de partida. A proteção depende de acompanhar o fornecedor durante toda a relação.

ITEM	REQUISITO	VERIFIQUE	BASE	SIM	PARCIAL	NÃO	N.A.
I1	**O fornecedor e os dados que ele trata constam do mapeamento de dados e do registro de operações da empresa.**	O registro indica o serviço, os dados, a localização e o contrato vigente.	LGPD, ART. 37	☐	☐	☐	☐
I2 ESSENCIAL	**Houve avaliação de risco do fornecedor antes da contratação, com resultado documentado.**	Questionário de segurança, evidências apresentadas e histórico de incidentes conhecidos.	LGPD, ART. 6º, X, E ART. 50 · ISO/IEC 27001:2022, 5.19	☐	☐	☐	☐
I3	**A reavaliação periódica está prevista conforme a criticidade, ao menos anual para fornecedores de nível 3.**	Há responsável e data definidos para a próxima reavaliação.	ISO/IEC 27001:2022, 5.22	☐	☐	☐	☐
I4	**Os acessos do fornecedor aos sistemas da empresa são nominais, protegidos por autenticação multifator e revisados periodicamente.**	Não há contas compartilhadas nem acessos sem data de expiração.	LGPD, ART. 46 · ISO/IEC 27001:2022, 5.15 A 5.18	☐	☐	☐	☐
I5	**Os riscos não tratados no contrato estão registrados e foram aceitos formalmente por quem tem alçada, com data de revisão.**	Use o quadro de aceite de risco da etapa 4.	LGPD, ART. 6º, X · ISO/IEC 27001:2022, 6.1.3	☐	☐	☐	☐

OBSERVAÇÕES DO BLOCO I

ETAPA 3

Resultado da avaliação

Para cada bloco, conte os itens aplicáveis e some os pontos. Pontos possíveis são o dobro dos itens aplicáveis. O percentual é a divisão dos pontos obtidos pelos pontos possíveis.

BLOCO	ITENS APLICÁVEIS	PONTOS OBTIDOS	PONTOS POSSÍVEIS	PERCENTUAL
A · Enquadramento da relação				
B · Instruções e limites de uso				
C · Segurança da informação				
D · Incidentes de segurança				
E · Subcontratação				
F · Transferência internacional				
G · Responsabilidade e garantias				
H · Encerramento do contrato				
I · Gestão contínua do fornecedor				
Total				

ITENS ESSENCIAIS COM RESPOSTA NÃO

Se houver ao menos um item essencial com resposta **Não**, trate a situação geral como **Crítico**.

SITUAÇÃO GERAL

☐ **Adequado** · 80% A 100%

O contrato cobre bem o tema. Mantenha a reavaliação periódica e acompanhe mudanças no serviço.

☐ **Atenção** · 50% A 79%

Há lacunas relevantes. Ajuste por aditivo ou na próxima renovação, conforme a criticidade do fornecedor.

☐ **Crítico** · ABAIXO DE 50%

A proteção contratual é insuficiente. Priorize aditivo ou renegociação e avalie medidas compensatórias até o ajuste.

Olhe os blocos, não só o total

Um total adequado pode esconder um bloco crítico, como incidentes ou transferência internacional.

Comece pelos essenciais

Eles concentram os pontos que mais pesam em um incidente, em uma reclamação de titular ou em uma fiscalização.

Date a avaliação

O resultado vale para o contrato e a versão analisados. Mudança relevante no serviço pede nova avaliação.

ETAPA 4

Plano de ação e aceite de risco

Registre os ajustes a partir dos itens com resposta Não ou Parcial, começando pelos essenciais. Instrumentos possíveis:

Aditivo contratual | **Renegociação na renovação** | **Configuração do serviço** | **Controle interno** | **Aceite de risco** | **Substituição do fornecedor**

ITEM	AJUSTE NECESSÁRIO	INSTRUMENTO	RESPONSÁVEL	PRAZO

Aceite formal de risco

ITEM I5

Use quando a empresa decidir manter a contratação sem resolver uma lacuna. O aceite deve ser dado por quem tem alçada para assumir o risco e revisto na data indicada.

ITEM OU ITENS RELACIONADOS

RISCO ACEITO E JUSTIFICATIVA

MEDIDAS COMPENSATÓRIAS ADOTADAS

APROVADO POR (NOME E CARGO)

DATA

REVISÃO PREVISTA EM

REFERÊNCIAS

Normas consultadas

Lei nº 13.709/2018 (LGPD)	Arts. 5º, 6º, 11, 14, 15, 16, 18, 19, 33, 37, 39, 42, 46, 47, 48, 50 e 52.
Resolução CD/ANPD nº 2/2022	Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte.
Resolução CD/ANPD nº 4/2023	Regulamento de dosimetria e aplicação de sanções administrativas.
Resolução CD/ANPD nº 15/2024	Regulamento de comunicação de incidente de segurança.
Resolução CD/ANPD nº 18/2024	Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.
Resolução CD/ANPD nº 19/2024	Regulamento de transferência internacional de dados e cláusulas-padrão contratuais.
Decisão de adequação Brasil e União Europeia	Reconhecimento mútuo de adequação formalizado em janeiro de 2026.
Guia Orientativo da ANPD	Definições dos agentes de tratamento de dados pessoais e do encarregado.
ABNT NBR ISO/IEC 27001:2022	Controles 5.15 a 5.23 (acessos e relacionamento com fornecedores), 5.30 e 8.13 (continuidade e cópias de segurança) e cláusula 6.1.3 (tratamento de riscos).

GLOSSÁRIO

Termos usados

Controlador
Quem decide sobre o tratamento de dados pessoais. Nesta relação, a empresa contratante.

Operador
Quem trata os dados em nome do controlador. Em regra, o fornecedor.

Suboperador
Terceiro contratado pelo operador para auxiliar no tratamento.

Incidente de segurança
Evento que compromete a confidencialidade, a integridade, a disponibilidade ou a autenticidade de dados pessoais.

Cláusulas-padrão contratuais
Modelo aprovado pela ANPD para amparar transferências internacionais. Deve ser adotado na íntegra.

DPA
Acordo de tratamento de dados (data processing agreement), em geral anexo ao contrato principal.

Aceite de risco
Decisão formal e documentada de manter um risco conhecido, tomada por quem tem alçada.



O risco do fornecedor também é risco da empresa. O contrato é onde ele se controla.

COORDENAÇÃO TÉCNICA

Lucas F. A. Schettert

Sócio responsável pela área de Direito Digital, Privacidade e Proteção de Dados da WVHS Advocacia Empresarial

linkedin.com/in/lucasschettert

EXIN Privacy & Data Protection — FOUNDATION — Certified by EXIN

EXIN Privacy & Data Protection LGPD — ESSENTIALS — Certified by EXIN

EXIN Information Security Management ISO/IEC 27001 — FOUNDATION — Certified by EXIN

Conteúdo informativo, de caráter preventivo, atualizado em outubro de 2026. Não substitui a análise jurídica do caso concreto.

Wentz Vieira Hentges & Schettert
ADVOCACIA EMPRESARIAL

wvhs.com.br · @wvhsadv
Ágora Tech Park, Joinville, SC
OAB/SC 34.715