



(Preferencialmente preencher digitalmente)

Ao responder este Questionário, a empresa garante à CTG Brasil que:

- (i) O signatário deste Questionário detém todos os poderes e informações necessários para respondê-lo, bem como todos os poderes para representar a empresa no âmbito deste Questionário;
- (ii) Todas as informações fornecidas pela empresa são verdadeiras, responsabilizando-se por qualquer omissão, informação incorreta ou incompleta contida neste Questionário;
- (iii) Caso ocorram alterações as respostas fornecidas neste Questionário, a empresa se compromete a informar a CTG Brasil tão logo seja possível.

As informações fornecidas neste Questionário são reputadas confidenciais. As partes comprometem-se a manter completa confidencialidade e sigilo sobre quaisquer dados ou informações trocadas no bojo deste Questionário, não as divulgando ou transferindo a terceiros sem a devida e expressa autorização da outra parte. As partes exercerão medidas de segurança e grau de cuidado com as informações confidenciais recebidas não inferior àqueles que seriam aplicados às suas próprias informações confidenciais, garantindo proteção adequada contra qualquer divulgação, cópia ou utilização não autorizada.

Não serão reputadas informações confidenciais as informações que:

- (i) Estejam ou venham a tornar-se de domínio público de outra forma que não em função da revelação deste Questionário;
- (ii) Comprovadamente já estivessem na posse da parte receptora por conta de ter sido registrada em seus arquivos ou que já estivesse em uso antes do seu recebimento pela parte divulgadora e que não estivessem cobertas por obrigação de confidencialidade; ou
- (iii) Tenham sido recebidas de um terceiro de boa-fé, não tendo recebido a informação diretamente ou indiretamente da parte divulgadora.

Não serão consideradas quebra à obrigação de confidencialidade a divulgação de informações exigidas por lei ou por autoridade policial, judicial ou administrativa, ordem judicial ou regulamento aplicável a parte receptora. Caso a Parte Receptora seja demandada a divulgar dados pessoais ou informações confidenciais vinculadas à outra Parte recebido por meio deste Questionário, a Parte Receptora deverá informar imediatamente a Parte Divulgadora para que possa tomar as medidas cabíveis.

A CTG Brasil se reserva ao direito de realizar inspeções e avaliações sobre os níveis de proteção de dados pessoais adotados por seus parceiros sempre que julgar necessário. Estas avaliações poderão compreender análise de documentos solicitados, solicitação de informações e auditorias. As partes se comprometem a envidar seus melhores esforços para colaborar uma com a outra em procedimentos de verificação de nível de proteção de dados pessoais e adequação às legislações sobre proteção de dados.

As garantias e obrigações estabelecidas neste Questionário passarão a vigorar a partir da data de sua assinatura e permanecerão em vigor pelo prazo de 10 (dez) anos a contar do fornecimento da informação confidencial. Caso as informações deste Questionário sejam atualizadas, conforme estabelecido na cláusula 1. (iii) acima, as condições estabelecidas nas Disposições Gerais deste Questionário se aplicarão também às novas informações confidenciais complementares.

1. Descreva os dados pessoais que você recebe e/ou transmite e em quais circunstâncias. (Anexar o RoPA).



2. Descreva os dados pessoais sensíveis que você recebe e/ou transmite e em quais circunstâncias. (Anexar RoPA).

3. Os dados pessoais recebidos da Organização são acessados por terceiros (por exemplo, seus próprios prestadores de serviços/subcontratados/fornecedores terceirizados)?

Sim Não

Em caso positivo, por favor detalhe em que circunstâncias:

4. Se respondeu 'sim' para a pergunta acima, especifique os terceiros e confirme quais medidas foram implementadas para cumprir as leis de proteção de dados, incluindo análise/due diligence que você realizou ou pretende realizar com esses terceiros.



5. Você realiza tratamento de dados pessoais com fundamento nas bases legais e para cada atividade de tratamento, em conformidade com a LGPD?

Sim Não

6. Você limita o processamento de dados pessoais ao tratamento necessário para os fins específicos que justificam a sua coleta?

Sim Não

7. Você possui Record of Processing Activities (Registro das Operações de Tratamento de Dados Pessoais)?

Sim Não

8. Você possui políticas de proteção de dados interna e externa? Se sim, por favor encaminhe uma cópia.

Sim Não

9. Caso seja um requisito legal que a empresa tenha Data Protection Officer (Encarregado), confirme o cumprimento a esse requerimento.

10. O acesso a dados pessoais está restrito somente a funcionários autorizados? Quais as medidas implementadas para garantir o respeito por seus funcionários de suas políticas de proteção de dados?

Sim Não

Em caso positivo, por favor detalhar as informações:

11. Quais são as medidas protetivas adotadas para garantir a segurança de dados pessoais (por exemplo, controles de acesso, criptografia, modificação de dados, mascaramento de dados)?



12. Os dados pessoais são armazenados em um local e ambiente seguros?

Sim Não

Em caso positivo, por favor descreva como é feito o armazenamento:

13. Você possui mecanismos de segregação entre os dados fornecidos pela Organização e aqueles que constam de sua base de dados?

Sim Não

Se sim, por favor descreva-o:

14. Você possui as tecnologias e os processos necessários para responder às solicitações de acesso do titular de dados pessoais em conformidade com a LGPD?

Sim Não

15. Você possui as tecnologias e os processos necessários para responder às solicitações do titular para exclusão de seus dados pessoais em conformidade com a LGPD?

Sim Não

16. Você possui as tecnologias e os processos necessários para atender ao direito de portabilidade do titular de dados pessoais em conformidade com a LGPD?

Sim Não



17. Você possui diferentes níveis de segurança da informação para dados sensíveis? Por favor, descreva-os.

Sim Não

Se sim, por favor descreva-o:

18. Caso os serviços solicitados exijam atividades de tratamento que resultem em um alto risco para os titulares de dados, você realiza um Relatório de Impacto à Proteção de Dados Pessoais (Data Protection Impact Assessment - DPIA) nos serviços solicitados?

Sim Não

19. Você possui salvaguardas/mecanismos adequados, em conformidade com a LGPD, para o armazenamento e/ou transferência internacional de dados pessoais?

Sim Não

20. Você anonimiza dados pessoais e sensíveis mediante encriptação ou remoção de informações que tornam uma pessoa natural identificada ou identificável?

Sim Não

21. Seu processamento inclui automatização de qualquer tomada de decisão, criação perfis com base nos dados pessoais transferidos (profiling) ou utilização analítica (analytics)?

Sim Não

22. Caso você colete dados pessoais, você fornece informações sobre o tratamento de dados aos titulares (incluindo clientes, pessoal, etc.), em conformidade com o artigo 9º da LGPD?

Sim Não

23. Caso você obtenha dados pessoais de titulares através de consentimento, o consentimento é obtido de acordo com as estipulações da LGPD?

Sim Não



24. Você possui contratos compatíveis com as leis de proteção de dados, em vigor, com seus fornecedores e parceiros?

Sim Não

25. Você oferece orientação aos funcionários de terceiros a respeito das práticas a serem tomadas em relação à proteção de dados pessoais?

Sim Não

Se sim, forneça uma cópia das instruções enviadas a terceiros envolvidos no processamento de dados destinados/enviados pela Organização:

26. Você exige que seus funcionários e prestadores de serviços assinem acordos de confidencialidade e segurança de dados?

Sim Não

Em caso afirmativo, forneça uma cópia para revisão:

27. Você instrui seus funcionários e contratados a limitar o armazenamento de dados pessoais do cliente em dispositivos de armazenamento móvel ao mínimo exigido para fins comerciais?

Sim Não

28. Você possui uma política de revisão regular das permissões de acesso aos dados pessoais que garanta o acesso somente aos funcionários e contratados que precisam ter acesso, bem como um procedimento para prevenir prontamente funcionários e contratados desligados de acesso a dados pessoais?

Sim Não



Se sim, forneça uma cópia:

29. Você conduz avaliações de vulnerabilidade e testes de penetração em seus sistemas de tratamento de dados pessoais?

Sim Não

30. Você será capaz de atender solicitações da Organização para remover dados pessoais de seus sistemas, se necessário?

Sim Não

Se sim, dentro de qual prazo?:

31. Se respondeu “sim” para a pergunta acima, especifique o procedimento para descarte de dados.

32. Você - em relação aos serviços solicitados - é capaz de detectar incidentes de segurança (incluindo acesso não autorizado, destruição, perda, alteração e violações de dados)?

Sim Não

33. Você possui um procedimento para agir, prontamente, em caso de incidentes de segurança, incluindo notificação aos titulares de dados afetados e para a Organização?

Sim Não

Se sim, descreva-o:



34. Se respondeu 'sim' para a pergunta acima, especifique os terceiros e confirme quais medidas foram implementadas para cumprir as leis de proteção de dados, incluindo análise/ due diligence que você realizou ou pretende realizar com esses terceiros.

35. Você transfere dados do cliente para outro país?

Sim Não

Se sim, é a transferência interna/externa? Por favor, forneça uma cópia das medidas de segurança tomadas e contrato:

36. Você possui uma política/procedimento de back-up em relação aos dados pessoais? Se sim, por favor, forneça uma cópia para revisão.

Sim Não

37. Você contratou algum serviço de assessoria para implementação da LGPD?

Sim Não

Se sim, quais as medidas que estão sendo adotadas para regularização:



38. Sua empresa já passou por algum incidente de violações de segurança da informação nos últimos dois (2) anos?

Sim Não

Se sim, quais foram as circunstâncias em que a violação ocorreu e quais medidas foram adotadas para evitar novos incidentes:

39. Sua empresa está atualmente sujeita a quaisquer ações de execução, investigações ou litígios relacionados à privacidade ou à segurança da informação?

Sim Não

Em caso afirmativo, por favor indique sobre quais circunstâncias e forneça cópias de documentos mais relevantes:

40. A empresa é certificada em algum padrão ou framework de segurança?

Sim Não

Se sim, quais são eles?



CTG Brasil

Risk & Compliance

Código

03_RC_Anexo 3

Anexo 3

Validade

30/09/2022

Questionário para Avaliação de Privacidade e Conformidade com a LGPD

Versão

001

Página

10 / 10

Agradecemos as informações prestadas à CTG Brasil, o que nos auxiliará nos nossos procedimentos de prevenção à corrupção nos negócios.

Eu, _____, declaro que as informações fornecidas nesta declaração são verdadeiras e completas. Comprometo-me ainda a notificar imediatamente à CTG Brasil caso tenha conhecimento de quaisquer informações adicionais ou alterações nas informações aqui fornecidas.

NOME COMPLETO

CARGO/ÁREA

LOCAL E DATA

ASSINATURA
