SERPRO lgpd

Guia da Avaliação de Conformidade

Um conteúdo para você analisar, com informações extras, suas respostas e confirmar como está a situação de sua empresa perante a **LGPD**

SERPRO

Guia da Avaliação de Conformidade

Se você chegou até aqui certamente é porque busca mais informações para adequar sua empresa à LGPD, certo?

Por isso preparamos este guia que, de forma explicativa e descomplicada, aborda os principais pontos da lei, a partir de complementos às respostas **SIM e/ou NÃO** dadas por você na avaliação on-line e gratuita no portal serpro.gov.br/lgpd. A proposta é que, com as informações extras, você possa checar se realmente respondeu à avaliação de forma adequada. Ou seja, para saber se o resultado representa o estágio em que sua empresa está à luz da Lei Geral de Proteção de Dados Pessoais. Vamos confirmar?

Ah! E, em caso de outras dúvidas, escreva para nós pelo **lgpd@serpro.gov.br.**

Guia da Avaliação de Conformidade

A empresa faz algum tipo de tratamento de dados pessoais, coletados no território brasileiro, para fins econômicos, com o objetivo de ofertar produtos e serviços?

Em geral, respondem “sim” as empresas que tratam dados: relacionados ao titular (brasileiro ou não) que esteja no Brasil, no momento da coleta; dentro do território nacional, independentemente do meio aplicado (físico ou digital), do país-sede do operador ou do país onde se localizam os dados; para fornecimento de bens ou serviços. É o que preconiza o artigo 3º da LGPD.

“Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento” (inciso V, artigo 5º)

Respondem “não” normalmente as empresas que usam dados pessoais apenas para fins acadêmicos e/ou artísticos e/ou jornalísticos.

Sabemos que empresas que se encaixam nisso são a minoria. Portanto, para responder “não”, é preciso verificar se de fato não há nenhum tipo de tratamento de dados que se encaixe nas condições citadas no “sim”. Caso identifique que algum tratamento se enquadre no SIM – e mesmo que se refira a poucos dados –, esse tratamento deverá seguir os preceitos da LGPD e sua empresa, então, estará sujeita à adequação.

Se você respondeu “não” à primeira pergunta, a avaliação termina aqui. Se respondeu “sim”, a avaliação continua para você.

A empresa possui dados pessoais, de seus colaboradores e clientes, de forma organizada?

Em regra, marcam “sim” as empresas que conhecem o que são dados pessoais e que sabem que há alguns deles sujeitos a cuidados ainda mais específicos (como os sensíveis e os sobre crianças e adolescentes).

““Dado pessoal: informação relacionada à pessoa natural identificada ou identificável” (inciso I, artigo 5º)
“Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (inciso II, artigo 5º)

O “não” costuma ser assinalado pelas empresas que não sabem bem o que é considerado dado pessoal, e quais são as especificidades desse dado.

Guia da Avaliação de Conformidade

A empresa sabe que, segundo a LGPD, há tratamentos de dados pessoais que poderão ser considerados discriminatórios, ilegais e/ou abusivos?

O “sim” é escolhido por empresas que já sabem, por exemplo, que é possível tratar dados pessoais para definir o perfil de consumo de uma pessoa, mas se ela autorizar isso - se for sem consentimento, só se for para algum fim legitimado por lei.

Essas empresas provavelmente também sabem que, segundo o artigo 20 da LGPD, o titular terá direito de pedir que revisem decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

A resposta “não” é dada, via de regra, pelo dono de negócio que não sabe que, dependendo do tratamento do dado que sua empresa fizer, do objetivo do tratamento e do consentimento ou não do titular, isso poderá ser considerado irregular ou discriminatório.

Um exemplo de discriminação é contratar ou desligar um profissional baseando-se em dados sobre origem racial, religião, política, filiação sindical, vida sexual ou dado genético.
Outra irregularidade é não pedir o consentimento explícito para enviar, via e-mail, alguma promoção comercial aos clientes.

Os tratamentos de dados feitos pela empresa estão devidamente justificados?

O mais comum é o “sim” ser selecionado por empresas que sabem que, segundo a LGPD, os dados devem ser tratados com o consentimento do titular, ou para: cumprir uma obrigação legal; realizar estudos via órgão de pesquisa; executar contratos; defender um direito em processo; preservar a vida e a integridade física de uma pessoa; tutelar procedimentos feitos por profissionais das áreas da saúde ou sanitária; prevenir fraudes contra o titular; propiciar a proteção do crédito; para atender um interesse legítimo da empresa, mas que não fira os direitos fundamentais do titular.

“Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (inciso XII, artigo 5º)

O “não” é marcado quando há tratamentos que a empresa não sabe justificar, se levar em conta os critérios acima.

A empresa informa ao titular o que vai fazer, de fato, com os dados pessoais coletados?

Essa resposta é eleita por empresas que já solicitam o consentimento do cidadão de forma explícita, e para as finalidades específicas.

"O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas." (parágrafo 4º, artigo 8º)

A resposta negativa é a opção escolhida por empresas que não solicitam o consentimento do cidadão, ou que o solicitam de forma genérica, sem detalhar as finalidades.

Se o cidadão quisesse saber como seus dados pessoais são tratados, a empresa já estaria preparada para atendê-lo?

A resposta positiva é a eleita pelas empresas que estão pensando sobre (ou mesmo as que já têm) alguns procedimentos e/ou tecnologias para atender às solicitações dos titulares. Mesmo que ainda não estejam "prontas", são as empresas que já têm consciência que é preciso evoluir para garantir ao cidadão, assim que a LGPD entrar em vigor, todos os direitos dele.

Os direitos do titular, como o de acesso, correção, portabilidade, oposição e eliminação dos dados, são tratados no capítulo III da lei.

Empresas que respondem "não" usualmente são as que têm pouco ou nenhum preparo e/ou ferramentas para lidar com as demandas dos titulares.

SERPRO lgpd

Guia da Avaliação de Conformidade

Os profissionais – sejam eles da empresa ou terceirizados, e trabalhando no Brasil ou no exterior – responsáveis por tratar os dados pessoais estão claramente identificados?

Costuma marcar "sim" o proprietário do negócio que já sabe as funções dos agentes de tratamento (operador e controlador); e que está atento à necessidade de realizar, para atender à lei, uma monitoração sobre as atividades de tratamento que os profissionais executam em nome da empresa.

A resposta negativa é dada em geral pelo proprietário que até então não sabe os papéis dos agentes de tratamento; e que não despertou que, segundo a lei, é preciso adotar um controle sobre as atividades de tratamento que os profissionais realizam em nome da empresa.

"Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (inciso VI, artigo 5º)
"Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (inciso VII, artigo 5º)

A empresa possui documentações e práticas relacionadas à gestão da privacidade da informação?

O "sim" é a opção de empresas que já possuem alguma documentação – mesmo que precisem atualizar essa documentação e as práticas para adequá-las à nova lei.

O "não" é marcado em geral pelas empresas para as quais até o momento esse assunto não era, na teoria e/ou na prática, uma grande preocupação.

"Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais." (artigo 50)

SERPRO

Caso transmita dados pessoais para outras empresas, de dentro ou de fora do Brasil, faz isso apenas para a(s) habilitada(s) por tratar os dados em seu nome?

A resposta positiva é indicada quando a transmissão de dados é feita apenas para o operador responsável pelo tratamento de dados que atua em nome da empresa.

Sobre a transferência de dados além-fronteira, ela é permitida pela LGPD desde que seja: com o consentimento específico do titular dos dados; a pedido do titular para que esse possa executar pré-contrato ou contrato; para proteger a vida e a integridade física do titular ou de terceiro; para ajudar na execução de política pública; para país ou organismo internacional que projeta dados pessoais de forma compatível com o Brasil; para cooperar juridicamente com órgãos públicos de inteligência, investigação, ou por conta de compromisso assumido via acordo internacional; para cumprir obrigação legal; com a autorização da ANPD; comprovado que o controlador segue a LGPD na forma de normas globais, selos, certificados e códigos de conduta. Mais sobre assunto estão no capítulo V da lei.

A resposta negativa é selecionada quando a empresa transmite dados para outras empresas, indiscriminadamente.

Um exemplo é o caso da empresa que transmite inclusive dados sensíveis, por acreditar que "não tem problema fazer isso, já que é em prol de benefícios econômicos".

São realizados cursos e outras atividades, em matéria de proteção de dados, para profissionais e empresas que trabalham com a sua empresa?

As empresas que respondem “sim” são as que planejam ou já realizam ações de formação e/ou conscientização sobre o respeito à privacidade dos usuários, e que estão atentas à adaptação dessas ações à LGPD.

Os donos de negócio que respondem “não” normalmente são os que ainda precisam começar a capacitar e a orientar os profissionais e os parceiros que lidam com informação das pessoas, na empresa.

Há algum tipo de gestão para prevenir ou minimizar falhas de segurança, como o vazamento de dados?

O “sim” é dado por empresas que, de alguma forma, já estão antenadas aos temas análise de riscos e gestão de incidentes. Essas empresas também costumam saber que, conforme o artigo 48 da LGPD, a autoridade nacional e afetados por um incidente deverão ser comunicados sobre o fato.

O “não” é a resposta usual das empresas que não conhecem, até o momento, qual é a importância dos assuntos análise de riscos e gestão de incidentes, e que não sabem bem o que a lei determina em relação a falhas de segurança.

“Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.” (artigo 46)

A LGPD prevê, em seu artigo 52:
“I - advertência, com indicação de prazo para adoção de medidas corretivas;
II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III - multa diária, observado o limite total a que se refere o inciso II;”

RESULTADO

Gostou das informações extras citadas anteriormente? Mas não acabou! A seguir você encontra todos os resultados possíveis da avaliação de conformidade.

E lembre-se: o objetivo desse diagnóstico não é ser conclusivo, mas sim um ponto de reflexão para que você possa iniciar ou mudar a rota rumo à adequação de seu negócio à LGPD.

De 0 a 2* perguntas respondidas com SIM:
** Contagem das respostas a partir da segunda pergunta.*

RISCO ELEVADÍSSIMO
Sua empresa apresenta uma conformidade bastante baixa em relação aos requisitos da LGPD. Provavelmente repensar processos, cultura e tecnologias é bem necessário.

De 3 a 4 perguntas respondidas com SIM:
RISCO ELEVADO
Sua empresa apresenta uma conformidade baixa em relação aos requisitos da LGPD. Provavelmente, uma vigorosa reforma é necessária.

De 5 a 6 perguntas respondidas com SIM:
RISCO MÉDIO
Sua empresa apresenta uma conformidade razoável em relação aos requisitos da LGPD. Mas, ainda assim, uma significativa reforma é necessária.

De 7 a 8 perguntas respondidas com SIM:
RISCO BAIXO
Sua empresa apresenta uma conformidade alta em relação aos requisitos da LGPD. Você está num bom ponto do caminho, mas fique atento, ainda há diferentes ajustes a fazer.

De 9 a 10 perguntas respondidas com SIM:
RISCO BAIXÍSSIMO
Sua empresa apresenta uma conformidade muito alta em relação aos requisitos da LGPD. Você está adiantado no caminho, mas fique atento, ainda há o que fazer.

SERPRO lgpd

Serpro LGPD
O Serpro já possui soluções para te ajudar a ajustar seus negócios à LGPD.

Conheça mais em
www.loja.serpro.gov.br/lgpd

SERPRO