LGPD

Lei Geral de Proteção
de Dados Pessoais

Fortics

Sumário

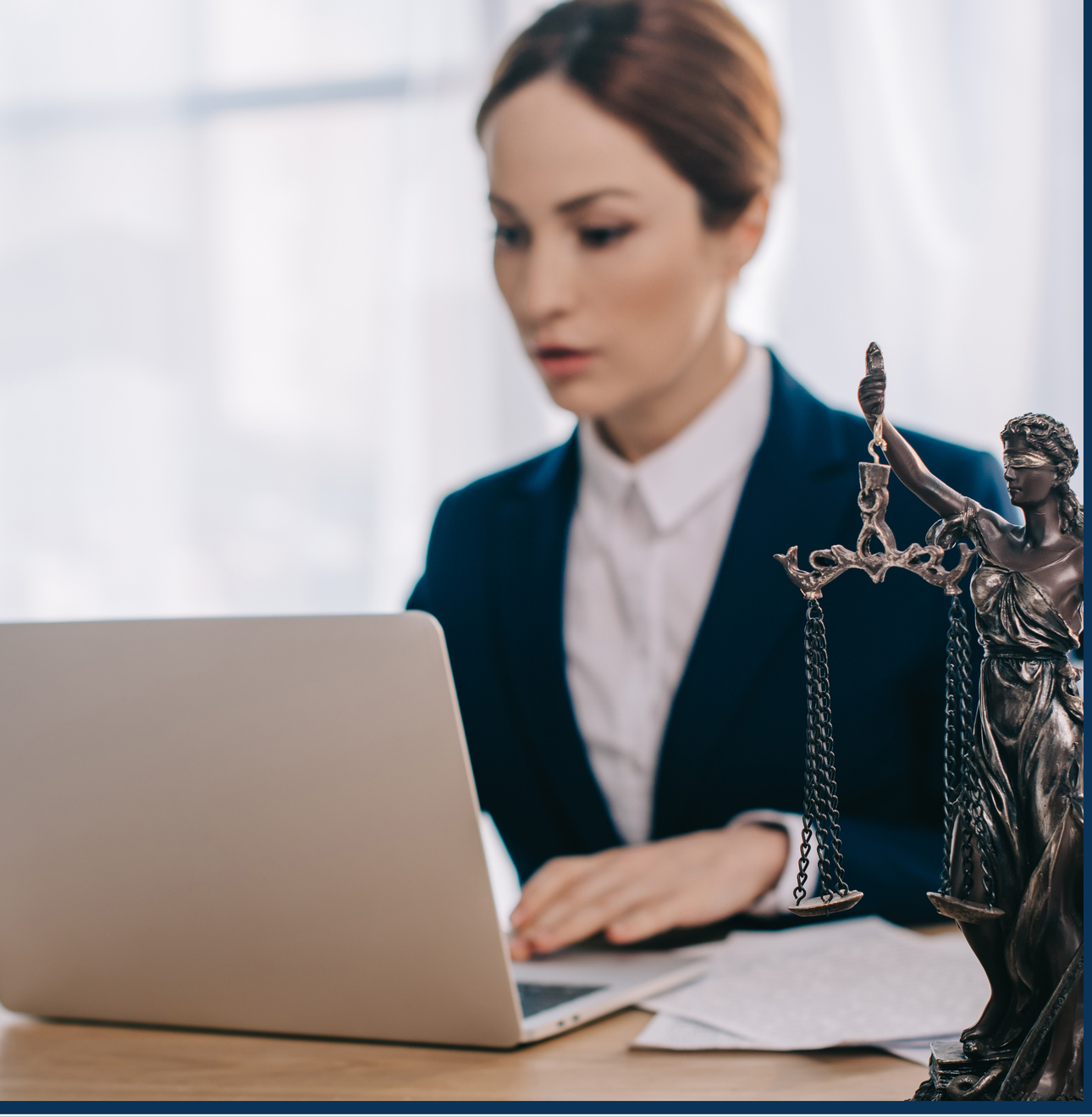
A Lei nº 13.709/2018 – mais conhecida como Lei Geral de Proteção de Dados Pessoais, ou, simplesmente, pela sigla LGPD– é uma legislação que veio para transformar o cotidiano de grande parte das empresas no Brasil, uma vez que impacta na forma como estas tratam os dados pessoais.

A LGPD traz novas regras e conceitos, que precisam ser observados pelas empresas, e uma série de novos direitos para os titulares, acarretando maiores responsabilidades para os agentes de tratamento de dados.

Para a **Fortics**, a compreensão da nova legislação aplicada ao seu modelo de negócio é fator fundamental para a continuidade das atividades. Valorizamos a relação com nossos clientes e fornecedores e temos como prioridade zelar pela privacidade e proteção dos dados compartilhados.

Para isso, temos como diretrizes um conjunto de boas práticas e padrões de segurança, técnicos e organizacionais, a fim de cumprir e fazer cumprir as exigências legais, além dos demais requisitos normativos externos e internos, fomentando o desenvolvimento de uma nova cultura corporativa de segurança da informação, privacidade e proteção de dados pessoais.

Diante do exposto, elaboramos este documento com alguns aspectos importantes relacionados ao tema. Se mesmo após a leitura deste conteúdo você ainda tiver dúvidas a respeito do assunto, entre em contato com nosso time de privacidade, por meio do e-mail dpo@fortics.com.br



O que é LGPD?

A LGPD, promulgada em 14 de agosto de 2018, é a primeira legislação do Brasil que trata especificamente do uso de dados pessoais. A nova lei estipula uma série de obrigações para empresas, organizações e órgãos do governo sobre a coleta, armazenamento, compartilhamento e tratamento dos dados pessoais, tanto *online* quanto *offline*.

Quando a lei entrou em vigor?

Com exceção das penalidades administrativas, a LGPD entrou em vigor em setembro de 2020. Isso significa que a partir daquela data, empresas e órgãos públicos teriam de garantir a seus usuários, obrigatoriamente, procedimentos bem definidos e informações claras sobre a coleta, o armazenamento e o uso de seus dados pessoais, entre outros aspectos.

Quais as sanções para quem não se adequar a legislação?

A LGPD prevê aplicação de multas que variam de 2% do faturamento bruto do grupo empresarial até R$ 50 milhões (por infração). No entanto, além das multas, está prevista uma série de outras sanções, como advertência, publicização da infração, bloqueio, eliminação e suspensão parcial e total do uso dos dados, que impactam diretamente no modelo de negócios e na reputação da empresa.

Essas sanções administrativas começaram a ser aplicadas a partir de agosto de 2021.

CONCEITOS FUNDAMENTAIS

O que são dados pessoais?

O conceito de dado pessoal adotado é bastante amplo: qualquer dado, isolado ou em conjunto com outros dados, que possa ter ou tenha o potencial de tornar a pessoa identificável. Portanto, a LGPD não se aplica a qualquer tipo de informação, mas tão somente aos ‘dados pessoais’, o que implica que o dado esteja intrinsecamente vinculado a uma pessoa natural identificada ou identificável.

O que são dados pessoais sensíveis?

Uma das categorias de dados presente na lei é a dos ‘dados pessoais sensíveis’. A LGPD indica uma lista dos dados considerados sensíveis: aqueles 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”. Como regra geral, toda informação que possa submeter o titular a algum tipo de preconceito ou discriminação pode ser considerada dado sensível e ser passível de proteção legal mais rigorosa.

O que pode ser considerado tratamento de dados?

Tratamento é qualquer operação realizada com um dado — da coleta ao descarte. A LGPD estipula normas para toda e qualquer ação de tratamento de dados pessoais. Seu art. 5.º traz uma extensa lista de ações que podem ser consideradas como tratamento. São exemplos: coleta, classificação, utilização, compartilhamento, reprodução, processamento, arquivamento, armazenamento etc.

Fortics

Quem são os agentes de tratamento?

Existem dois principais agentes de tratamento previstos pela LGPD: o controlador e o operador.

Controlador

É a empresa/organização que toma as decisões em relação aos dados pessoais. É o responsável por definir quando e como os dados serão coletados, para quais finalidades serão utilizados, onde e por quanto tempo serão armazenados etc.

Operador

É a empresa/organização que realiza o processamento de dados pessoais sob as ordens do controlador. O operador não toma decisões em relação ao uso dos dados.

Fortics

BASES LEGAIS

O que são bases legais?

Você sabe como e em quais casos a LGPD autoriza sua empresa a utilizar os dados pessoais de um contato? Para responder a essa pergunta é necessário entender o conceito de bases legais.

As bases legais são hipóteses da LGPD que autorizam o tratamento de dados pessoais. É importante destacar que a relação de bases legais que a LGPD cita são taxativas – o que significa dizer que não existe nenhuma outra hipótese, além das expressamente descritas ali. A lei prevê que para uma pessoa (física ou jurídica) realizar qualquer operação com um dado pessoal – seja coletar, transmitir ou processar — é necessário ter, pelo menos, uma base legal que legitime o tratamento desses dados.

A LGPD estabelece dez bases legais que autorizam o tratamento de dados pessoais. Essas bases não têm dependência ou predominância entre si, sendo que para cada caso de tratamento de dados, existe uma base legal mais apropriada.

Consentimento

Consentimento é uma manifestação livre, informada e inequívoca de uma pessoa que concorda com o uso dos seus dados para as finalidades propostas pela empresa. No entanto, o consentimento, como previsto na LGPD, pressupõe o atendimento a alguns requisitos para que possa ser considerado válido:

O consentimento precisa ser livre – o titular não pode ser forçado a fornecer consentimento. Essa deve ser uma escolha sem qualquer tipo de pressão: se uma empresa insere um campo de consentimento em um formulário, mas exige preenchimento obrigatório, o titular não terá escolha sobre fornecer ou não o consentimento, sendo, portanto, esse consentimento ilícito, uma vez que não foi obtido livremente.

O consentimento precisa ser informado – antes da coleta dos dados, o titular deve entender o que está consentindo, quais dados serão coletados e o ciclo de vida destas informações pessoais. As organizações devem se certificar de que explicam com o que a pessoa está concordando, de forma clara. Incluir informações em uma política de privacidade densa e complexa ou incluí-las em letras pequenas, difíceis de encontrar, difíceis de entender ou raramente lidas, não será suficiente para estabelecer o

consentimento informado.

O consentimento precisa ser inequívoco – depende de manifestação por meio de um ato positivo do usuário. Em outras palavras, deve haver uma ação do usuário indicando sua aceitação, ou pelo envio de e-mail ou por assinatura eletrônica ou até mesmo por um clique em local determinado. Não pode haver dúvidas acerca de o consentimento ter sido fornecido ou não. Opções pré-selecionadas ou o mero silêncio passivo do titular não podem ser considerados manifestações do consentimento inequívoco. O consentimento precisa ser fornecido para fins específicos e determinados.

O consentimento precisa ser fornecido para fins específicos e determinados – o consentimento deve ser fornecido para uma finalidade específica e determinada. Faz parte de toda a lógica da LGPD especificar o motivo pelo qual um dado pessoal é usado. A empresa não pode utilizar os dados para uma finalidade diferente daquela que foi consentida pelo contato.

Atenta a esses conceitos, a empresa cumpre com os princípios da finalidade, da necessidade e da transparência.

Legítimo Interesse

Outra base legal que autoriza o uso dos dados é o 'legítimo interesse'. Para sua utilização é importante observar dois pontos que devem ser sempre respeitados, obrigatoriamente, quando se pretender realizar o tratamento utilizando essa base legal. O primeiro é a finalidade legitima, ou seja, somente com propósitos legítimos, específicos e devidamente informados ao titular. O segundo, por sua vez, é a existência da situação concreta, ou seja, o titular deve ter a efetiva expectativa de que seus dados serão tratados em decorrência de relação prévia existente entre ele e o controlador.

Execução de contratos

No caso da base legal de execução de contratos, os dados de uma pessoa podem ser processados em dois casos: o primeiro é para que seja cumprida uma obrigação prevista em contrato, e o segundo, quando o tratamento de dados serve para a validação e início de vigência de um acordo.

Por exemplo, para contratar os serviços de novo colaborador, a empresa X precisa fornecer uma série de informações pessoais (como dados do contratante, dados para faturamento etc.), necessárias para formalizar o contrato, as quais farão parte do futuro contrato de emprego do titular dos dados.

Obrigação Legal ou Regulatória

Nesse caso, o tratamento de dados pessoais é justificado por exigência de outras leis ou normas setoriais. São situações nas quais a empresa precisa utilizar, compartilhar ou armazenar dados pessoais para cumprir obrigações legais ou atos normativos como, por exemplo, determinações

do Banco Central e de agências reguladoras, entre outros.

Execução de Políticas Públicas

Quando o tratamento de dados pessoais é resguardado pelo interesse público ou por necessidade de uma autoridade oficial, exercendo o papel de controlador daquele dado.

Estudos por órgãos de pesquisa

Dados pessoais podem ser tratados para fins de estudos de órgãos oficialmente credenciados como de pesquisa. Nesse caso, sempre que possível o dado deve ser anonimizado garantindo ao máximo a privacidade dos titulares.

Processo Judicial

Dados pessoais ainda podem ser tratados para exercício de direito em processos em geral, podendo ser administrativos, judiciais ou arbitrais.

Proteção da Vida

É possível justificar o tratamento de dados pessoais quando o seu uso é de interesse vital seja do titular do dado ou ainda de outra pessoa.

Tutela da Saúde

Quando profissionais de saúde, serviços de saúde ou autoridade sanitária precisam tratar dados pessoais.

Proteção de Crédito

É possível que dados pessoais sejam consultados avaliando o perfil de pagador do cidadão para a aprovação de crédito e redução dos riscos da transação.

Fortics

PRINCÍPIOS

O que são princípios?

Os princípios são orientações gerais, decorrentes das exigências de equidade, de justiça ou de moralidade. No campo da proteção dos dados pessoais, são padrões de boas práticas que sua empresa deve aplicar em todos os fluxos e práticas envolvendo dados pessoais.

Finalidade

Contanto com grande relevância prática, o princípio da finalidade busca acabar com a utilização de dados pessoais para fins genéricos ou indeterminados. O tratamento de cada informação pessoal deve ser feito para fins específicos, legítimos, explícitos e previamente informados. Ou seja, as empresas devem explicar ao usuário para que usarão cada um dos dados pessoais coletados.

Adequação

Este princípio está amplamente vinculado ao da finalidade, pois prevê o tratamento dos dados somente pode ocorrer quando houver compatibilidade com as finalidades informadas ao titular, de acordo com o contexto do tratamento, ou seja, dados devem ser tratados apenas para a finalidade que foi informada ao usuário e que este autorizou.

Necessidade

Este princípio guarda relação direta com a finalidade e a adequação, visto que enfatiza que a delimitação da licitude do tratamento de acordo com a sua finalidade, ou seja, a coleta e utilização de dados pessoais deve se restringir ao mínimo necessário para a realização das finalidades pretendidas pela empresa. O questionamento da empresa sempre deve ser: Este dado é realmente necessário?

Transparência

Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comerciais e industriais. Para a redução dos riscos, é importante que os controladores considerem os titulares sempre vulneráveis quanto ao entendimento do tratamento dos dados. Por isso, quanto mais informações, quanto mais transparente for todo o processo, mais a empresa estará em conformidade com a legislação.

Livre Acesso

Para que a lei possa ser efetiva, o titular deve ter a possibilidade de controlar o uso de seus dados pessoais (fundamento da autodeterminação afirmativa). Para isso, é necessário lhes garantir o livre acesso aos seus dados, bem como sua integridade.

Qualidade dos Dados

Se isoladamente vistas, em princípio, as informações pessoais coletadas, dificilmente afetariam o titular, mas quando colocadas em conjunto e processadas por mecanismos qualificados formam um compilado da personalidade de cada pessoa. Por essa razão os dados devem ser precisos, exatos e relevantes.

Segurança

Visando impedir acessos não autorizados a dados e ocorrências acidentais ou propositais de destruição, perda, alteração, comunicação ou difusão dos dados pessoais, a LGPD traz como princípio que as empresas adotem medidas técnicas e administrativas para proteção desses dados.

Prevenção

O princípio da prevenção determina a adoção de posturas preventivas e medidas proativas e não reativas, de modo a evitar incidentes de violação à privacidade.

Não Discriminação

Por este princípio, a proteção dos dados pessoais supera o da privacidade, abarcando também os direitos de personalidade diante da possibilidade de estigmatização do ser humano, em razão de sua classificação e segmentação baseada no tratamento de seus dados.

Responsabilização e Prestação de Contas

Prever a responsabilização e a prestação de contas como princípios demonstra a intenção da lei em alertar de que os agentes de proteção de dados são os responsáveis pelo fiel cumprimento de todas as exigências legais. É importante destacar que, por este princípio, é necessário que os agentes mantenham o registro de operações de tratamento de dados e o cumprimento da legislação.

DIREITOS

O que são direitos

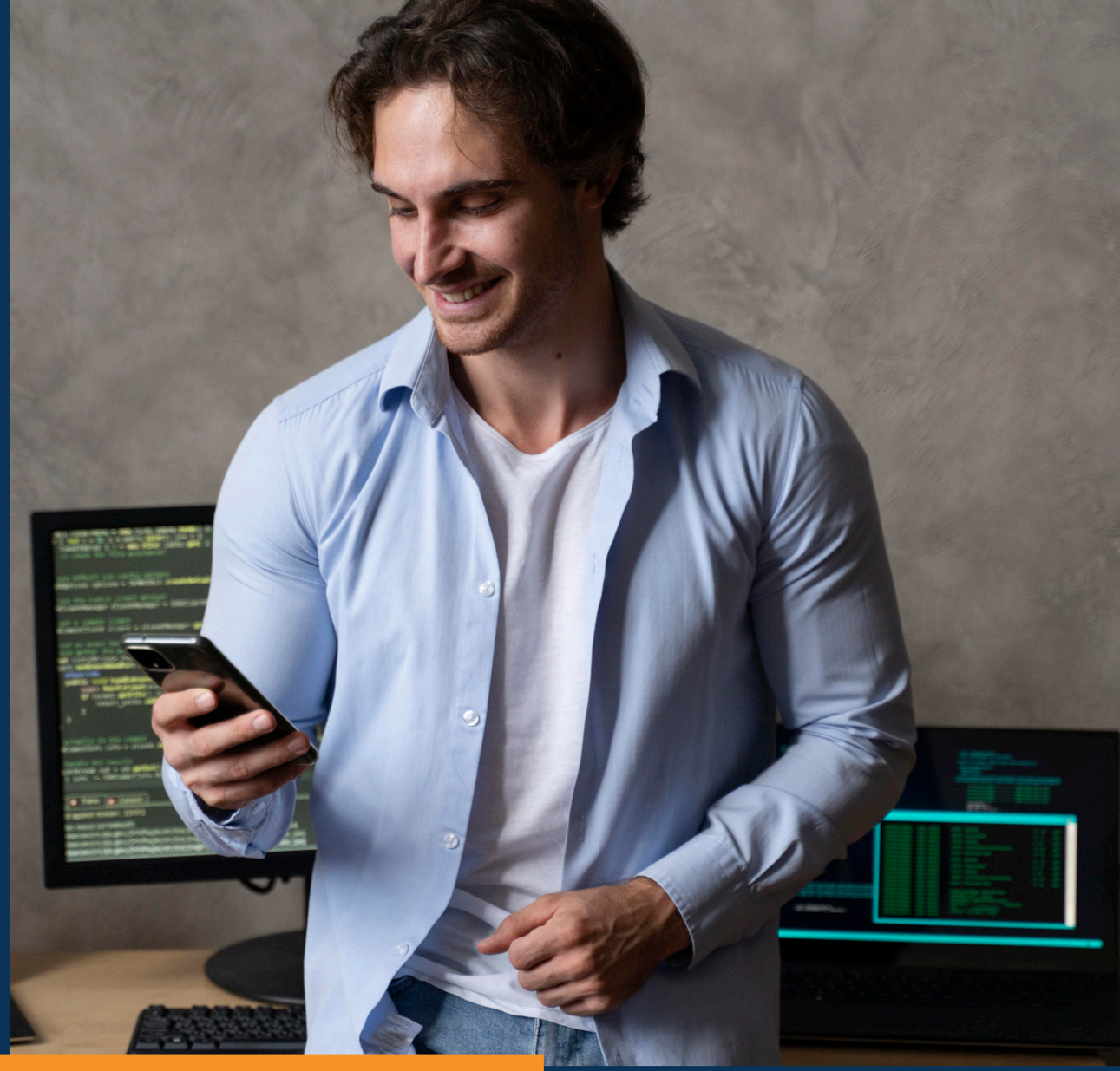
Os direitos são espécies de garantias que a lei fornece ao titular. O objetivo é dar às pessoas o controle sobre as suas próprias informações. Por isso, o titular tem direito de, por exemplo, requerer que uma empresa disponibilize acesso/alteração/exclusão dos dados que possui sobre essa pessoa, dentre outros direitos e garantias.

Direito de Acesso

O titular de dados pode solicitar à empresa/organização o acesso a todos os dados pessoais que a empresa possui sobre ele, além de outras informações entre as quais a finalidade, categorias, destinatários, os prazos de conservação, entre outros

Direito de Correção

O titular de dados tem o direito de solicitar a correção dos dados incompletos, inexatos ou desatualizados armazenados pela empresa.



Fortics

Direito de Anonimização, Bloqueio e Eliminação

Neste item a legislação elenca três direitos de natureza diversa. Direito de anonimização, bloqueio e eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD.

Direito de Revogação do Consentimento e Informação sobre a Possibilidade de Não Fornecer Consentimento

Nestes dois direitos vinculados ao consentimento a legislação determina, com base no princípio da transparência, que o titular tem direito de ser informado sobre as consequências de não fornecer o consentimento para tratamento de seus dados pessoais. Da mesma forma, também possui direito de revogar o consentimento previamente concedido para determinado tratamento.

Direito a Informação sobre Compartilhamento de Dados

Uma vez que a lei permite o compartilhamento dos dados pessoais, ela também garante ao titular buscar informação sobre com quais entidades públicas e privadas esses dados foram compartilhados.

Fortics

A LGPD SE APLICA A FORTICS?

Em seu art. 3.º, a legislação dispõe sobre sua aplicação material, deixando claro que não importa a tecnologia empregada no tratamento dos dados, se digital ou analógica. Ela também tem aplicação extraterritorial, o que significa dizer que a lei se aplica independentemente da localização da sede da empresa em que os dados são processados. Se a empresa ou organização processa dados pessoais de cidadãos brasileiros, se os dados pertencem a indivíduos localizados no Brasil e se os dados foram coletados no momento que o titular dos dados estava no Brasil, a LGPD se aplica.

Como os dados pessoais são tratados?

O tratamento dos dados pessoais pela **Fortics** segue os princípios previstos na LGPD, garantindo a qualidade, considerando uma finalidade clara e bem definida, boa-fé e a existência de hipóteses, que nos permitem realizar esse tratamento.

Fortics

Como funciona o uso e o tratamento dos dados pela Fortics?

A **Fortics** atua única e exclusivamente como operadora dos dados pessoais dos usuários. Nos termos da legislação aplicável, os procedimentos de compartilhamento de dados pessoais são realizados de acordo com as melhores práticas de privacidade e proteção de dados, levando em consideração os pilares da segurança da informação: confidencialidade, integridade e disponibilidade, bem como os demais requisitos de segurança da informação previstos nas normas e legislações aplicáveis.

A **Fortics não** realiza o tratamento de dados pessoais sensíveis sem que tenha a expressa instrução do controlador, sendo este o único e exclusivo responsável pela finalidade e base legal para o tratamento.

Todos os dados pessoais são tratados com base na execução contratual para as finalidades previamente definidas pelo controlador, respeitada a legislação aplicável à hipótese.

As disposições sobre confidencialidade previstas em nossas relações contratuais se aplicam aos dados pessoais em relação às partes e todos os seus sócios, empregados, colaboradores e prepostos em geral. No caso de ocorrer solicitação dos titulares, requisição de autoridades administrativas ou judiciais, a **Fortics** notificará o contratante acerca da existência e do conteúdo da solicitação/ordem/requisição correspondente, em tempo razoável para que este possa, caso deseje, apresentar suas medidas ou contrarrazões perante o juízo ou autoridade competente, sendo certo que a **Fortics** se compromete a cumprir uma ordem legal estritamente nos limites do que lhe for requisitado.

Em conformidade com as melhores práticas de mercado, o contratante deve informar os titulares dos dados pessoais, sempre que necessário, sobre o procedimento detalhado para desativar a coleta, o tratamento e/ou o compartilhamento de seus respectivos dados, assim como para solicitar o descarte ou a exclusão correspondente, disponibilizando, se e quando cabível, links ou utilidades análogas que viabilizem a respectiva solução na via digital, em cumprimento com o disposto na legislação vigente.

Os dados são armazenados?

Sim. A **Fortics** mantém relação contratual com empresas de armazenamento em nuvem, pelas quais as informações pessoais são guardadas sob os mais rigorosos protocolos e padrões internacionais de segurança.

Qual o tempo de retenção dos dados?

O prazo de retenção de dados utilizado pela **Fortics** é de cinco anos. Caso você decida excluir sua conta e apagar seus dados, eles serão anonimizados ou excluídos definitivamente. É importante ressaltar que os dados serão apagados para cumprimento de obrigação legal ou para exercício regular de direitos em processo judicial ou extrajudicial.

Findo o prazo de cinco anos, decorrido o prazo de 30 dias depois de encerrado o contrato (ou em prazo diferente, conforme determinação do controlador), os dados serão excluídos da base de dados dos sistemas da **Fortics**. Os dados poderão ser mantidos para finalidades diversas somente nos casos em que houver uma base legal que a justifique, ou se ocorrer a anonimização.

SEGURANÇA DOS PRODUTOS FORTICS

A **Fortics** atua de forma sistemática, preventiva e proativa, e tem como preceito fundamental no desenvolvimento de seus produtos, a segurança, a proteção e a privacidade dos dados. Para isso, trabalha com infraestrutura projetada para fornecer segurança em todo o ciclo de vida das informações. Nesse modelo de segurança priorizamos ações de privacidade e proteção de dados do usuário final, comunicações seguras entre serviços, além da comunicação particular e segura com clientes na Internet e com os respectivos administradores.

Privacy by Design – Privacy by Default

Nosso time de desenvolvimento segue o conceito de *privacidade by design*, tendo como padrão a privacidade e proteção dos dados. Com atitude proativa, nossos desenvolvedores inserem os elementos de privacidade a partir da concepção do produto. Além do conjunto de práticas e políticas de *compliance* adotadas rigorosamente no desenvolvimento dos produtos da **Fortics**, em virtude da utilização e integração das tecnologias de alguns de nossos parceiros, também herdamos o conjunto de conformidades preconizado em suas políticas de segurança e privacidade.

Hospedagem

Nossa plataforma funciona no modelo SaaS (Software as a Service), tanto em relação à hospedagem quanto aos serviços que utilizam o Google Cloud Platform e o MS Azure. Ambos os *clouds* estão hospedados nos Estados Unidos.

Segurança em Nuvem

Os ambientes utilizados pela **Fortics** para a prestação dos serviços atendem aos mais rígidos requisitos de segurança, os quais são auditados e certificados.

Política de Senhas

Nossa política de senhas preconiza a utilização de senhas fortes, que contenham números e letras, sem possibilidade de repetição, e um caractere especial. Essa informação está disponível no (i) do campo Complexidade de Senha.
Por padrão, as configurações de segurança de senha são:

- Número mínimo de caracteres: 8
- Tempo de expiração: 90 dias
- Complexidade de senha: ativada
- Histórico de senha: 6

Criptografia

O armazenamento dos dados utiliza o conceito de Data Lake (repositório de armazenamento e *engine* para processamento de grandes volumes de dados) criptografado, pelo qual o cliente tem autonomia sobre a chave sem a necessidade de ser reconhecido pela **Fortics**.

Anonimização dos Dados

Os dados são anonimizados sempre que possível, em respeito à privacidade. A anonimização, quando necessária, é realizada em razão de mapeamento dos dados sensíveis existentes nas bases relacionais.

Logs de Ações e Trilha de Auditoria

Nossa plataforma mantém o registro dos acessos e permite sua auditoria e a gestão dos logs do sistema, que possuem as seguintes informações de registro:

- IP;
- *Login*;
- Data/Horário;
- Sucesso/Falha;

Web Application Firewall

Nosso ambiente está protegido por *firewall* de aplicação altamente escalonável (WAF - Web Application Firewall), que minimiza riscos de ataques e protege nossa infraestrutura contra ameaças e vulnerabilidades.

Autenticação Remota

Utilizamos a integração de autenticação por meio do protocolo SAML 2.0. Ela é registrada no Cadastro de Servidores de Autenticação Remota e possui integração com o AD (Active Directory) e o Google Identity.

Repositório de Código Fonte Seguro

Todos os códigos-fontes são armazenados em repositório seguro, com acesso autorizado utilizando autenticação integrada.

Backups

Os *backups* referentes aos bancos de dados de produção são realizados diariamente com retenção de sete dias.

Pentest

A **Fortics** realiza a execução independente de Pentest (testes de penetração), com o objetivo de identificar fragilidades (vulnerabilidades) de cibersegurança no ambiente tecnológico que suporta seus processos de negócio, de modo a mapear os principais riscos a que a organização possa estar exposta. Os testes são realizados semestralmente por empresa independente e altamente especializada.

Análise Estática de Código (sast) e Gestão de Vulnerabilidades

Sempre comprometido com a segurança e privacidade, nosso time de desenvolvimento adota um *pipeline* de validações automatizadas que sempre passam por análise estática de código. Com essa ferramenta são avaliadas categorias de defeitos de *software*, entre eles: *code smells,* vulnerabilidades e *security hotspots*.

São realizados testes de segurança a cada versão, sendo possível avaliar vulnerabilidades em aplicações, redes e serviços frente aos diferentes tipos de ataques de segurança: ataques de negação de serviço (DOS), SQL *Injection* e ataque *man-in-the-middle (MITM)*, entre outros, e descobrir novas vulnerabilidades antes que sejam exploradas por atacantes.

MEDIDAS TÉCNICAS E ADMINISTRATIVAS DE SEGURANÇA

SEGURANÇA DAS ESTAÇÕES E TRABALHO REMOTO

Controle de inventário de aplicativos e programas do sistema

Monitoramento em tempo real na instalação de *softwares* de terceiros, de origem duvidosa, inventário de todos os aplicativos instalados por dispositivo ingressado no AD.

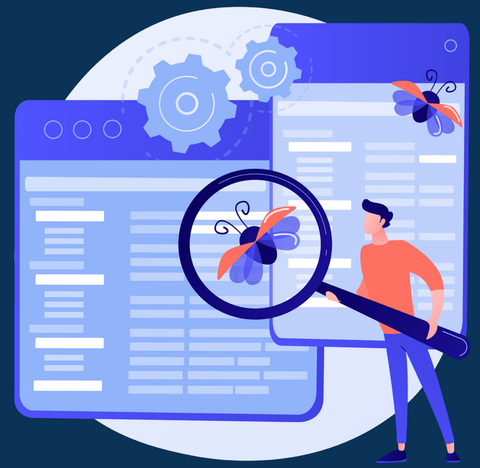
Antivírus

Antivírus atualizado e configurado para gerência e controle das ameaças mais recentes, tendo sua configuração centralizada nas políticas do Azure e sincronização com o sistema em nuvem da Microsoft.

Firewall

O *firewall* do sistema operacional é integrado diretamente com o antivírus para melhor proteção de ataques oriundos de redes desconhecidas.

Como já informado, trabalhamos com um *firewall* de aplicação altamente escalonável, que minimiza riscos de ataques e protege contra ameaças e vulnerabilidades.



Área de trabalho

Todos os equipamentos da **Fortics** vêm com configurações padrão para a área de trabalho do usuário, com o conceito de menor privilégio, a fim de impedir que este acesse configurações particulares principais do sistema e venha a expor o seu sistema.

Fortics

SEGURANÇA DO AMBIENTE

(USUÁRIOS)

Azure Active Directory

O acesso e autenticação ao ambiente em todas as estações e todos os dispositivos dos colaboradores da **Fortics** é monitorado e controlado pelo AD do Azure, que tem pleno controle sobre as aplicações em nuvens utilizadas.

Acesso Condicional

Todos os acessos são monitorados pelo AD e as autenticações são concedidas conforme o atendimento de regras, como localidade, IP, tempo de sessão, fatores de risco e MFA (Autenticação multifator).

MFA (Autenticação Mutifator)

Todos os colaboradores da Fortics possuem habilitado em seu usuário a MFA (Autenticação multifator). A MFA impede que o usuário realize a conexão em máquina/estação diferente ou em localização distinta sem antes confirmar algo que possui, por meio de um código enviado por SMS ao celular ou ao seu *e-mail* pessoal.

PROCESSO E CULTURA DA PRIVACIDADE

Gestão de Incidentes

A gestão de incidentes e o acompanhamento das não conformidades são realizados de acordo com as boas práticas, tendo como referência as normas ISO/IEC 27001:2013 e ISO/IEC 27.701:2019.

Ambientação e Treinamentos

Os colaboradores da **Fortics** assinam contrato de confidencialidade e realizam treinamentos relacionados à confidencialidade e privacidade, bem como treinamento no nosso código de conduta. Nosso código trata especificamente das responsabilidades e do comportamento esperado em relação à proteção das informações.

Comunicação

A equipe responsável pela segurança da informação utiliza os canais de comunicação interna da **Fortics** para manter todos os colaboradores informados sobre temas relacionados à segurança, buscando, assim, a conscientização e fomentando a cultura de privacidade e proteção de dados.

Comissão da Privacidade e Proteção de Dados

A **Fortics** possui uma comissão responsável por assegurar a implementação e o acompanhamento de um programa robusto de gestão de segurança de informação e privacidade, atenta à necessidade de consolidação do seu programa de governança em privacidade, nos termos da legislação vigente.

Data Protection Officer

A data protection officer da Fortics é a advogada Laura Cristina de Quadros Carvalhal e certificada CIPM (Certified Information Privacy Manager) e CDPO/BR (Certified Data Protection Officer) pela IAPP e DPO (Data Protection Officer) pela Exin.

LINKS ÚTEIS

Links de informações complementares sobre os nossos produtos

Portal do Cliente https://support.fortics.com.br/pt-BR/support/home

Política de Privacidade https://www.fortics.com.br/politica-de-privacidade

Política de Cookies https://www.fortics.com.br/politica-de-cookies

Declaração de Conformidade https://www.fortics.com.br/declaracao-de-conformidade

Status Page https://fortics.statuspage.io

Portal da Privacidade https://www.fortics.com.br/portal-da-privacidade

Fortics

Fortics

www.fortics.com.br

0800 367 8427

@forticstecnologia

/fortics

/fortics

/fortics

/forticsoficial