INTEREST
ENGENHARIA

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

0	13/05/2025	Emissão Inicial
Nº	**Data**	**Motivo da Revisão**

MENSAGEM DA DIRETORIA

Prezados (as) colaboradores (as), Clientes, Fornecedores e demais titulares de dados,

Comprometidos com o direito à privacidade de dados, reafirmamos o nosso compromisso com a proteção de dados pessoais. Entendemos que a privacidade é um valor essencial para a sociedade contemporânea e, por isso, temos adotado uma governança atenta à postura proativa e transparente no tratamento das informações pessoais.

Esta política representa mais do que a conformidade com normas legais: simboliza o respeito à liberdade e à autonomia informativa.

Estamos nos empenhando em assegurar que todos os nossos colaboradores, parceiros e prestadores de serviço atuem com responsabilidade, garantindo a segurança e a integridade dos dados confiados à nossa organização.

Atenciosamente,

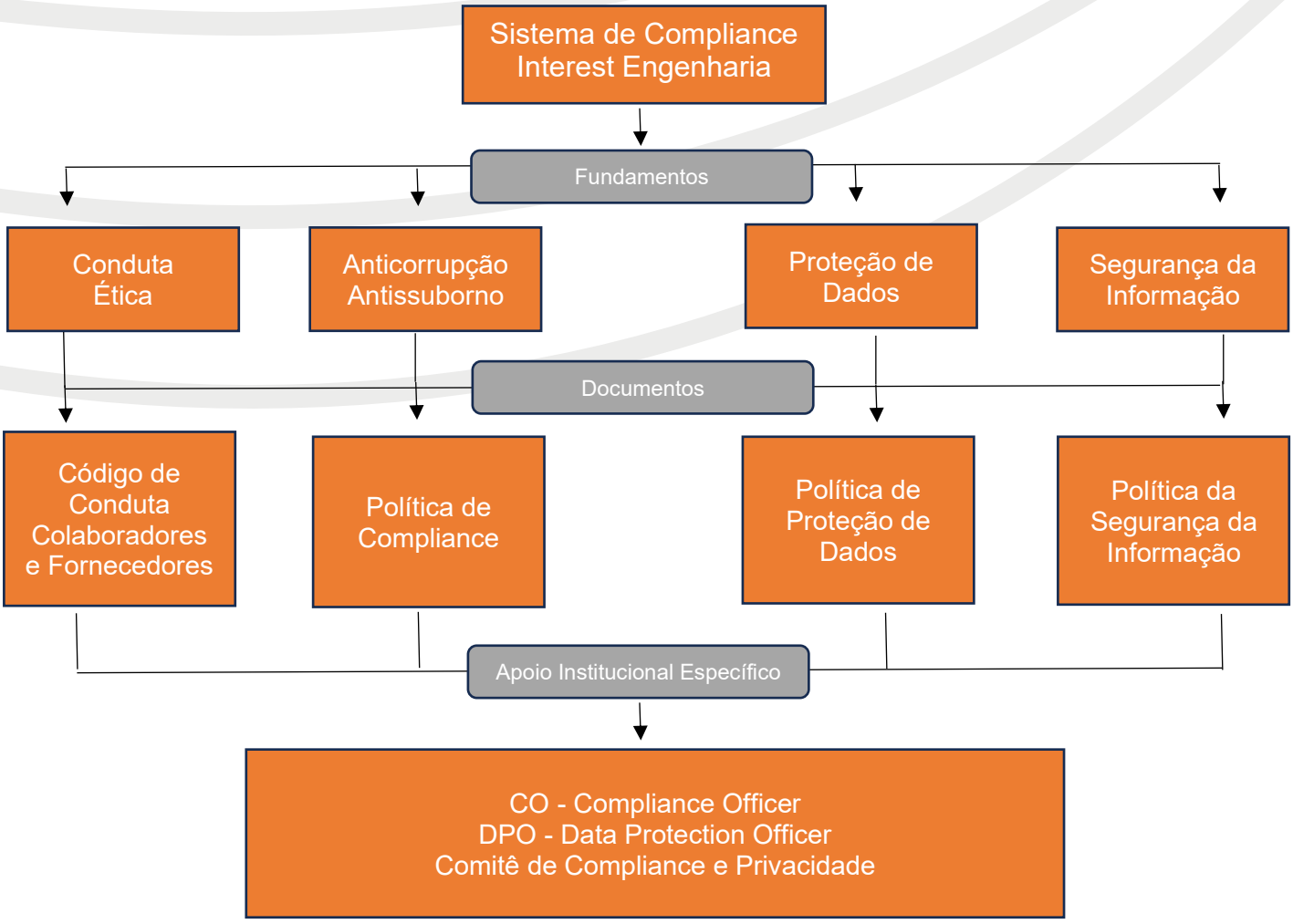
Diretoria Interest Engenharia

SISTEMA DE COMPLIANCE DA INTEREST

O Sistema de Compliance da Interest Engenharia conta com o apoio inequívoco e contínuo da Direção e foi construído nas bases sólidas de ética e integridade já existente na organização desde a sua constituição há trinta e cinco anos.

O desenvolvimento se deu a partir de reuniões com a Diretoria, com diversos setores, aplicação de treinamentos e avaliações de riscos de conformidade, a partir dos ditames da Lei Anticorrupção e Lei Geral de Proteção de Dados.

Preponderantemente, utiliza-se tais normativos para embasar a sua documentação interna e externa, que será monitorada e aperfeiçoada quanto à aplicação e engajamento organizacional pelo apoio institucional específico representado pelo Compliance Officer, Data Protection Officer e Comitê de Compliance e Privacidade.



INSTRUÇÕES PARA UMA MELHOR EXPERIÊNCIA NA LEITURA

Como devo consultar esta Política de Proteção de Dados?

É necessário que seja lida com atenção e cautela em toda a sua extensão, mas também está dividido em cinco grandes blocos para beneficiar consultas rápidas, caso necessário:

Considerações Iniciais, você encontra aspectos introdutórios para sua inserção no contexto da INTEREST.

Conceitos Importantes sobre Proteção de Dados, será concedido ao leitor ter conhecimento de aspectos importantes da LGPD para que entenda sobre obrigações e direitos frente a esta legislação.

Governança de Dados, aqui você vai encontrar o que a empresa adotará como medidas de governança de dados, em destaque, informações sobre o Comitê de Compliance e Privacidade e o Canal de Compliance e Privacidade, onde está aberto à comunicações, dúvidas, denúncias e quaisquer informações necessária à melhoria contínua da governança da INTEREST.

Apoio Institucional Específico, aqui você conhece todos os formadores do apoio ao Sistema de Compliance, Data Protection Officer, Compliance Officer e Comitê de Compliance e Privacidade da Interest e suas atribuições, com ênfase no Canal de Compliance e Privacidade: compliance@interest.com.br

Disposições Finais, são os temas relacionados a posicionamentos éticos da Interest, medidas disciplinares e exposição das aplicações de atualização desta Política.

Agora é só começar!

1. CONSIDERAÇÕES INICIAIS

1.1 A proteção de dados pessoais é essencial para garantir a privacidade e a segurança das informações em um cenário cada vez mais digitalizado, no qual o tratamento de dados se torna parte integrante das atividades cotidianas. Em conformidade com a Lei Geral de Proteção de Dados (LGPD), proteger essas informações vai além do cumprimento legal: trata-se de um compromisso ético que fortalece a confiança entre indivíduos, organizações e o poder público.

1.2 A adoção de medidas eficazes de proteção de dados contribui para a prevenção de usos indevidos, como fraudes, roubo de identidade e outras formas de violação da privacidade. Dessa forma, assegura-se a integridade, a confidencialidade e a transparência no tratamento de dados pessoais, conforme os princípios estabelecidos pela LGPD.

1.3 A principal finalidade da Política de Proteção de Dados Pessoais é assegurar a privacidade, a segurança e a integridade das informações dos titulares, regulando de forma clara e transparente como os dados pessoais são coletados, tratados, armazenados e compartilhados.

1.4 Essa política está, portanto, alinhada com os princípios e diretrizes da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), garantindo o respeito aos direitos fundamentais de liberdade, privacidade e à livre formação da personalidade de cada indivíduo.

1.5 Devem observar as diretrizes estabelecidas nesta Política de Proteção de Dados Pessoais todas as pessoas jurídicas ou físicas, que tenham operações com a INTEREST e que possam realizar o tratamento de dados pessoais, tendo a INTEREST como agente de tratamento, seja como controladora de dados, ou então, como operadora de dados pessoais, incluindo, mas não se limitando a: **Organizações Privadas:** Empresas de diferentes portes que operem com a INTEREST, que coletem, tratem ou armazenem dados pessoais no desempenho de suas atividades; **Entidades Públicas:** Órgãos ou instituições públicas que operem com a INTEREST, manipulando dados pessoais no exercício de funções como prestação de serviços públicos, segurança ou administração; **Organizações Sem Fins Lucrativos:** ONGs, associações, fundações ou outras entidades sem fins lucrativos que se relacionem com a INTEREST que realizem o tratamento de dados pessoais para cumprir suas finalidades institucionais; **Titulares dos Dados:** Indivíduos a quem os dados pessoais se referem; **Fornecedores de Serviços e Terceiros:** Parceiros comerciais, prestadores de serviços, consultores, e quaisquer terceiros que, por força

contratual ou operacional, tenham acesso a dados pessoais no contexto de suas atividades com a INTEREST e, **Autoridades Reguladoras:** Órgãos governamentais ou entidades independentes com competência para fiscalizar o cumprimento da legislação de proteção de dados, incluindo a Autoridade Nacional de Proteção de Dados (ANPD), com os quais a INTEREST se compromete a cooperar.

1.6 A política da INTEREST tem como objetivo proteger os direitos e liberdades fundamentais desses titulares, especialmente no que diz respeito à privacidade, à autodeterminação informativa e ao controle sobre seus dados. Para maiores informações também consultar: **CÓDIGO DE CONDUTA e CÓDIGO DE CONDUTA DE FORNECEDORES**.

2. CONCEITOS IMPORTANTES SOBRE PROTEÇÃO DE DADOS

2.1 Identificação e Classificação de Dados Pessoais**:** A LGPD classifica os dados pessoais em duas categorias principais: dados pessoais e dados pessoais sensíveis. A identificação e classificação desses dados são cruciais para a adequação e o cumprimento da lei.

2.1.1 **Dados Pessoais:** São informações relacionadas a pessoa natural identificada ou identificável. Isso inclui uma ampla gama de informações que, direta ou indiretamente, podem identificar uma pessoa. Exemplos de dados pessoais incluem, não se limitando a: Nome completo, Número de identidade (RG, CPF), Endereço de e-mail, Endereço residencial, Número de telefone, Informações de localização, Identificadores digitais (como endereços IP, cookies), dados de comportamento e preferências pessoais.

2.1.2 **Dados Pessoais Sensíveis:** São um subconjunto de dados pessoais que estão relacionados a características específicas que podem ser utilizadas de forma discriminatória. A LGPD dá especial atenção a esses dados devido ao potencial risco de causar danos aos titulares dos dados. Incluem: Origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

2.2 A correta identificação e classificação dos dados pessoais e sensíveis são fundamentais para determinar o nível de proteção e as medidas de segurança necessárias. A LGPD exige que as organizações adotem procedimentos e práticas que garantam a proteção desses dados, com atenção especial aos dados sensíveis, que exigem consentimento específico e destacado para seu tratamento, exceto em casos previstos por lei.

2.3 O tratamento de dados é qualquer operação ou conjunto de operações realizadas com dados pessoais ou conjuntos de dados pessoais. Isso inclui desde a coleta inicial dos dados até sua eliminação final, abrangendo uma ampla gama de atividades que podem ser realizadas manualmente ou por meios automatizados. Constitui tratamento de dados: a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

2.4 A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) define que o tratamento de dados pessoais somente pode ocorrer nas hipóteses legalmente previstas. A coleta e o uso de dados pessoais devem observar **pelo menos uma base legal legítima**, entre as quais destacam-se:

2.4.1 **Consentimento do Titular:** O tratamento pode ocorrer mediante consentimento livre, informado e inequívoco do titular, com a devida transparência quanto à finalidade específica dos dados coletados.

2.4.2 **Cumprimento de Obrigação Legal ou Regulatória:** Quando o tratamento for necessário para que o controlador atenda exigências legais ou regulatórias, nos termos da legislação vigente.

2.4.3 **Execução de Políticas Públicas:** Em situações previstas em lei, o tratamento pode ser realizado pela administração pública para fins de execução de políticas públicas.

2.4.4 **Estudos por Órgão de Pesquisa:** O tratamento é permitido para fins de pesquisa, desde que garantida, sempre que possível, a anonimização dos dados pessoais.

2.4.5 **Execução de Contrato ou Procedimentos Preliminares:** Quando os dados forem necessários para a celebração ou execução de contrato do qual o titular seja parte, ou para diligências pré-contratuais a pedido do titular.

2.4.6 **Exercício Regular de Direitos:** O tratamento é autorizado para assegurar o exercício de direitos em processos judiciais, administrativos ou arbitrais.

2.4.7 **Proteção da Vida ou da Incolumidade Física:** Quando for imprescindível para resguardar a vida ou a integridade física do titular ou de terceiros.

2.4.8 **Tutela da Saúde:** Exclusivamente para procedimentos realizados por profissionais ou entidades da área da saúde, ou ainda por autoridade sanitária, conforme a necessidade.

2.4.9 **Interesse Legítimo do Controlador ou de Terceiro:** É permitido o tratamento quando necessário para atender interesses legítimos, desde que não se sobreponham aos direitos e liberdades fundamentais do titular.

2.4.10 **Proteção do Crédito:** Inclui o tratamento de dados pessoais necessário para atividades legítimas voltadas à proteção do crédito, conforme a legislação aplicável.

2.5 Quem são os agentes que tratam estes dados e, portanto, devem submeter a uma base legal? Os agentes de proteção de dados são categorizados principalmente em dois grupos: o controlador e o operador.

Além destes, a figura do encarregado de proteção de dados (DPO - Data Protection Officer) também desempenha um papel crucial no ecossistema de proteção de dados. Cada um desses agentes tem responsabilidades específicas no tratamento de dados pessoais:

2.5.1 **Controlador:** É a pessoa natural ou jurídica, de direito público ou privado, que tem competências para tomar as decisões referentes ao tratamento de dados pessoais. O controlador é responsável por determinar as finalidades e os meios pelos quais os dados pessoais são processados. Isso inclui decidir sobre quais dados serão coletados, a finalidade da coleta e como os dados serão utilizados. O controlador tem a responsabilidade principal de garantir a conformidade com a LGPD, incluindo a proteção dos direitos dos titulares dos dados.

2.5.2 **Operador:** É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador atua sob as ordens do controlador, seguindo suas instruções para processar os dados pessoais para os fins determinados por aquele. Embora o operador não tome as decisões sobre os aspectos principais do tratamento de dados (como finalidade e meios), ele tem a responsabilidade de garantir a segurança dos dados durante o processamento e de seguir as diretrizes estabelecidas pelo controlador.

2.5.3 **Encarregado de Proteção de Dados** (Data Protection Officer - DPO): O DPO é a pessoa indicada pelo controlador e pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

2.6 O DPO tem várias responsabilidades, incluindo o monitoramento da conformidade da organização com a LGPD, a orientação de funcionários e contratados acerca das práticas de proteção de dados, para assegurar a conformidade e o atendimento às solicitações dos titulares dos dados e da ANPD.

2.7 Autoridade Nacional de Proteção de Dados (ANPD): órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no Brasil. Apesar de sua função reguladora, a ANPD também pode ser considerada agente de tratamento quando realiza operações com dados pessoais para exercer suas competências legais, como em atividades de fiscalização ou análise de denúncias, enquadrando-se assim nas definições previstas pela própria LGPD.

2.8. Quais são os Direitos dos Titulares dos Dados Pessoais? Alguns destes são:

2.8.1 **Confirmação da Existência de Tratamento:** O titular tem o direito de confirmar se seus dados pessoais estão sendo tratados pela INTEREST.

2.8.2 **Acesso aos Dados:** O titular pode solicitar acesso aos seus dados pessoais, incluindo informações sobre o tratamento realizado e a obtenção de cópias desses dados.

2.8.3 **Correção de Dados Incompletos, Inexatos ou Desatualizados:** Caso identifique inconsistências, o titular pode solicitar a correção ou complementação dos seus dados pessoais.

2.8.4 **Anonimização, Bloqueio ou Eliminação de Dados Desnecessários, Excessivos ou Tratados em Desconformidade com a LGPD:** Sempre que o tratamento não estiver de acordo com a legislação, o titular poderá requerer tais medidas.

2.8.5 **Portabilidade dos Dados:** Mediante requisição expressa, o titular poderá solicitar a portabilidade de seus dados a outro fornecedor de serviços ou produtos, respeitando a regulamentação da Autoridade Nacional e os segredos comercial e industrial.

2.8.6 **Eliminação dos Dados Tratados com Base no Consentimento:** O titular tem o direito de solicitar a eliminação dos dados tratados com base no consentimento, salvo quando houver outra base legal que justifique a manutenção do tratamento.

2.8.7 **Informação sobre Compartilhamento de Dados:** O titular pode solicitar informações acerca das entidades públicas ou privadas com as quais a INTEREST compartilhou seus dados pessoais.

2.8.8 **Informação sobre a Possibilidade de Não Fornecer Consentimento e Consequências da Negativa:** O titular deve ser informado sobre a opção de não fornecer consentimento e as consequências dessa escolha para o uso dos serviços.

2.8.10 **Revogação do Consentimento:** O titular poderá revogar o consentimento a qualquer momento, por meio de procedimento simples e gratuito. A INTEREST deverá eliminar os dados, salvo nos casos em que a legislação permita ou exija sua conservação.

2.9 A INTEREST compromete-se a disponibilizar os meios adequados e eficazes para que os titulares possam exercer plenamente esses direitos, conforme previsto na LGPD, inclusive, com contato direto com o DPO através do e-mail: compliance@interest.com.br.

3. GOVERNANÇA DE DADOS

3.1 A Governança de Dados Pessoais, conforme o artigo 50 da Lei Geral de Proteção de Dados Pessoais (LGPD), refere-se à adoção de boas práticas e políticas eficazes por parte dos agentes de tratamento de dados, com o objetivo de garantir a proteção de dados pessoais. Este artigo incentiva a implementação de medidas como planos de resposta a incidentes, auditorias regulares, e mecanismos de mitigação de riscos, promovendo a transparência e o aprimoramento contínuo das partes interessadas.

3.2 **Treinamento e Conscientização**: O treinamento e a conscientização sobre a Política de Proteção de Dados Pessoais são componentes essenciais para garantir a conformidade com leis como a Lei Geral de Proteção de Dados (LGPD). A seguir, detalhamos os aspectos cruciais desses processos de treinamento e conscientização que serão adotados pela INTEREST.

3.2.1 **Objetivos do Treinamento e Conscientização:** Compreender a Importância da Proteção de Dados: Sensibilizar todos os envolvidos sobre a importância de proteger os dados pessoais, destacando as consequências legais, financeiras e de reputação em caso de não conformidade;

3.2.2 **Conhecimento da Legislação:** Proporcionar um entendimento claro da LGPD e de outras leis aplicáveis, incluindo os princípios de tratamento de dados, as categorias de dados protegidos, e as obrigações legais;

3.2.3 **Práticas Seguras de Tratamento de Dados:** Instruir sobre as melhores práticas e procedimentos seguros para o tratamento de dados, incluindo coleta, armazenamento, processamento e eliminação de dados pessoais;

3.2.4 **Gestão de Incidentes:** Ensinar como identificar, reportar e responder a incidentes de segurança de dados, incluindo violações de dados pessoais.

3.3 **Monitoramento:** O monitoramento do programa LGPD envolve a revisão sistemática das práticas, políticas e procedimentos relacionados ao tratamento de dados pessoais dentro de uma organização que será realizada, prioritariamente, pelo Comitê de Compliance e Privacidade da INTEREST. O objetivo é verificar a conformidade com a lei, identificar lacunas e riscos, e

recomendar melhorias. Isso pode incluir, mas não se limita a:

a. Avaliação da adequação das políticas de privacidade e proteção de dados;

b. Verificação da existência e eficácia das medidas de segurança da informação;

c. Análise da legalidade, transparência e finalidade na coleta e uso dos dados;

d. Revisão dos processos de consentimento e das práticas de governança de dados;

e. Exame dos contratos com operadores e parceiros terceirizados, assegurando que estes também estejam em conformidade.

3.4 O monitoramento contínuo, que será realizada prioritariamente pelo Comitê de Compliance e Privacidade da INTEREST, é crucial para a detecção precoce de qualquer desvio ou não conformidade com a LGPD. Isso pode ser realizado por meio de sistemas automatizados e procedimentos regulares que incluem:

a. Acompanhamento constante das operações de tratamento de dados para assegurar que sejam executadas conforme as políticas estabelecidas;

b. Implementação de sistemas de gestão de incidentes para garantir respostas rápidas e eficazes a qualquer violação de dados;

c. Realização de análises de risco e avaliações de impacto à proteção de dados para novos projetos ou mudanças significativas nas operações;

d. Monitoramento da eficácia das medidas técnicas e organizacionais de segurança de dados.

3.5 O monitoramento não é apenas requisito legal, mas também práticas essenciais para a gestão de riscos, fortalecendo a confiança dos titulares dos dados e promovendo uma cultura de transparência e responsabilidade na proteção de dados pessoais.

3.6 A segurança de dados é um aspecto crítico da gestão de informações na era digital, envolvendo a implementação de medidas técnicas, físicas e administrativas para proteger dados pessoais e corporativos contra acessos não autorizados, perdas, alterações indevidas, divulgação, destruição ou qualquer outra forma de tratamento inseguro.

3.7 Essas medidas incluem, mas não se limitam:

a. Criptografia;

b. Controle de acesso;

c. Avaliações de vulnerabilidade;

d. Treinamentos de conscientização em segurança para funcionários;

d. Backups regulares e;

e. Planos de resposta a incidentes.

3.8 A segurança de dados não apenas salvaguarda as informações importantes das organizações e indivíduos contra ameaças cibernéticas, mas também assegura a conformidade com regulamentações de proteção de dados, como a GDPR na União Europeia e a LGPD no Brasil, fortalecendo a confiança dos stakeholders e mantendo a integridade e a reputação das entidades envolvidas. Observar ainda a: **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**.

3.9 O compartilhamento de dados deve respeitar os princípios da finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

3.10 Isso significa que qualquer compartilhamento de dados deve ter uma finalidade legítima, específica e informada ao titular, além de ser compatível com as finalidades originais para as quais os dados foram coletados.

3.11 A LGPD estabelece que o compartilhamento de dados pessoais deve ocorrer em situações específicas e sob condições claras:

3.11.1 **Com Consentimento do Titular**: O compartilhamento pode ocorrer com o consentimento explícito do titular dos dados, que deve ser informado sobre com quem os dados serão compartilhados e para quais finalidades;

3.11.2 **Sem Consentimento do Titular**: Em certas condições, o compartilhamento pode ocorrer sem o consentimento do titular, como para o cumprimento de uma obrigação legal, para a execução de políticas públicas, para a realização de estudos por órgão de pesquisa, para a proteção da vida ou da incolumidade física do titular ou de terceiros, para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias, ou para a proteção do crédito;

3.11.3 **Transparência e Direitos dos Titulares:** A transparência é um pilar fundamental, exigindo que os titulares dos dados sejam informados sobre o compartilhamento de seus dados, incluindo

as entidades com as quais os dados são compartilhados e os propósitos específicos do compartilhamento.

3.12 Além disso, os titulares têm o direito de acessar informações sobre o compartilhamento de seus dados e podem exercer outros direitos previstos na LGPD, como a correção de dados incompletos, inexatos ou desatualizados.

3.13 Medidas de Segurança: As organizações envolvidas no compartilhamento de dados devem adotar medidas de segurança, técnicas e administrativas adequadas para 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.

3.14 Responsabilidade e Prestação de Contas: Organizações que tratam dados pessoais devem não apenas cumprir com as obrigações estabelecidas pela LGPD, mas também demonstrar a qualquer momento que estão fazendo isso, adotando práticas e políticas que assegurem a conformidade com a lei, incluindo no contexto de compartilhamento de dados.

3.15 A LGPD enfatiza a importância da adoção de medidas preventivas, mas também reconhece que violações podem ocorrer e, quando isso acontece, é crucial ter um plano de resposta bem definido. Os procedimentos a serem seguidos incluem:

3.16 Detecção e Avaliação do Incidente: Imediatamente após a identificação de uma violação de dados, a INTEREST deve avaliar a extensão e a gravidade do incidente, determinando quais dados foram afetados e qual o potencial impacto para os titulares dos dados.

3.17 Contenção e Mitigação: Deve ser tomadas medidas imediatas para conter a violação e mitigar seus efeitos. Isso pode incluir a suspensão de sistemas específicos, a alteração de senhas ou o isolamento de partes da rede.

3.18 Notificação às Autoridades: A LGPD exige que a Autoridade Nacional de Proteção de Dados (ANPD) seja notificada em um prazo razoável, que, conforme a regulamentação, é de até 2 dias úteis, dependendo da gravidade do incidente e do risco ou dano aos titulares dos dados.

3.19 Comunicação aos Titulares dos Dados: Além de notificar a ANPD, a INTEREST deve comunicar o incidente de forma clara e adequada aos titulares dos dados afetados, especialmente se o incidente representar um risco elevado aos seus direitos e liberdades. A comunicação deve incluir informações sobre a natureza do incidente, os dados afetados, os possíveis impactos, as medidas que estão sendo tomadas para resolver a situação e como os titulares podem se proteger.

3.20 **Documentação e Avaliação:** Todo o processo de resposta ao incidente deve ser documentado, incluindo as decisões tomadas e as ações realizadas. Após a resolução do incidente, é recomendável realizar uma avaliação pós-incidente para identificar as causas, avaliar a eficácia das medidas de resposta e ajustar os planos de segurança e resposta a incidentes conforme necessário.

3.21 As Transferências Internacionais de Dados sob a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, são permitidas, mas estão sujeitas a condições específicas para assegurar que o nível de proteção de dados pessoais não seja comprometido quando estes são transferidos para fora do Brasil. A LGPD estabelece uma série de mecanismos e garantias que devem ser observados para que tais transferências sejam realizadas de forma legal e segura:

3.21.1 **Adequação de Proteção de Dados:** A transferência pode ocorrer para países ou organismos internacionais que proporcionem um grau de proteção de dados pessoais adequado ao previsto na LGPD. A Autoridade Nacional de Proteção de Dados (ANPD) é responsável por avaliar e declarar a adequação desses níveis de proteção.

3.21.2 **Garantias Contratuais:** Na ausência de uma decisão de adequação, a transferência internacional de dados pode ser realizada mediante a oferta de garantias suficientes de proteção, por meio de cláusulas contratuais específicas para a situação, cláusulas-padrão contratuais, normas corporativas globais ou selos, certificados e códigos de conduta aprovados.

3.21.3 **Consentimento Específico:** A transferência pode ocorrer com o consentimento específico e destacado do titular dos dados, após ser informado sobre as condições internacionais da transferência, a natureza dos dados a serem transferidos, e os riscos envolvidos.

3.21.4 **Cumprimento Legal e Proteção do Titular:** A LGPD também permite a transferência de dados para a proteção do crédito, bem como para o cumprimento de obrigação legal ou regulatória pelo controlador, para a execução de políticas públicas ou atribuição legal do serviço público, para a realização de estudos por órgão de pesquisa, para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido deste, ou para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

3.21.5 **Cooperação Internacional**: A transferência de dados pode ser necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e fiscalização, conforme os meios legais previstos em acordos internacionais.

3.22 A LGPD estabelece que qualquer transferência internacional de dados deve garantir que os dados pessoais estejam sujeitos a um regime de proteção compatível com a legislação brasileira.

4. APOIO INSTITUCIONAL ESPECÍFICO

4.1 A INTEREST Engenharia contará com um Comitê de Compliance e Privacidade atuante, cuja missão é assegurar que os princípios éticos e legais sejam respeitados em todas as esferas da organização. Este comitê desempenha um papel estratégico na promoção de uma cultura de integridade, transparência e responsabilidade, reforçando o compromisso da empresa com a conformidade e a boa governança, inclusive no que tange à Anticorrupção e a Lei Geral de Proteção de Dados. Maiores informações consultar: **REGIMENTO INTERNO COMITÊ DE COMPLIANCE E PRIVACIDADE** e **POLÍTICA DE COMPLIANCE**.

4.2 Entre as principais atribuições do Comitê de Compliance e Privacidade, destacam-se: I – Monitorar a implementação do Programa de Compliance e do plano de ação de conformidade à Anticorrupção e LGPD; II – Deliberar sobre medidas corretivas e preventivas em casos de não conformidade; III – Avaliar periodicamente os riscos éticos, legais e de privacidade; IV – Acompanhar denúncias recebidas por meio do canal institucional, zelando pela confidencialidade e integridade dos processos; V – Emitir pareceres e recomendações à Direção; VI – Propor treinamentos, campanhas de sensibilização e ajustes normativos; VII – Analisar relatórios de auditoria e conformidade, e VIII – Zelar pela cultura ética e pelo uso responsável de dados pessoais.

4.3 A atuação do Comitê de Compliance e Privacidade reforça o compromisso permanente da INTEREST com um ambiente negocial ético, seguro e em conformidade com a legislação vigente.

4.4 Fica instituído o Canal de Compliance e Privacidade da INTEREST Engenharia, destinado ao recebimento de dúvidas, denúncias, sugestões e quaisquer comunicações relacionadas à presente Política, ao Código de Conduta, Código de Conduta de Fornecedores, às Políticas Internas, à Lei Anticorrupção e à Lei Geral de Proteção de Dados (LGPD). Este canal garante sigilo, confidencialidade e imparcialidade na apuração dos fatos relatados e não-retaliação contribuindo para a manutenção de um ambiente negocial ético, transparente e em conformidade com os princípios da empresa.

4.5 As comunicações devem ser encaminhadas para o e-mail: compliance@interest.com.br

5. DISPOSIÇÕES FINAIS

5.1 Apenas pessoas formalmente (por escrito) autorizadas pela INTEREST podem representar, assinar documentos, responder a questões legais e/ou financeiras e dar declarações. A INTEREST não se responsabiliza por qualquer situação que não tenha a forma de representação aqui estabelecida.

5.2 Quanto à comunicação oficial, na transmissão de mensagens, divulgação de valores e visão, etc. para o público interno e externo, são porta-vozes da INTEREST apenas a sua Diretoria, cada um em sua área de atuação.

5.3 A INTEREST declara que não tolera nenhum tipo de desrespeito, discriminação, trabalho análogo à escravo e assédio de qualquer tipo e qualquer violação aos direitos humanos, cabendo aplicar as medidas contratuais e legais por estas violação.

5.4 A divulgação da presente Política deve fazer parte das atividades de integração de novos colaboradores e contratação de novos fornecedores. A reciclagem da divulgação deverá ser realizada a cada dois anos ou quando houver revisão do seu conteúdo.

5.5 Em caso de violação às leis e a presente Política da INTEREST é preciso informar que medidas podem ser adotadas, já previstas em lei, tais como: Advertência Verbal ou Escrita: Para infrações leves ou como primeira medida; Suspensão: Temporária das atividades do colaborador, sem remuneração, como forma de penalidade por infrações mais graves; Treinamento ou Reciclagem Obrigatórios: Para reforçar a importância das políticas de proteção de dados e evitar reincidências; Demissão por Justa Causa: Para casos de descumprimento grave e intencional das políticas de proteção de dados, que coloquem em risco significativo a segurança das informações ou violem direitos de titulares de dados e, Ações Legais: A organização pode tomar medidas legais contra o colaborador, buscando reparação por danos causados à empresa devido ao descumprimento do presente acordo de conduta.

5.6 Em caso de violação por fornecedores à LGPD e/ou a presente Política da INTEREST é preciso evidenciar que podem ser adotadas medidas, já previstas em lei ou em contrato, inclusive rescisão de contratos firmados, sem que configure violação contratual por parte da INTEREST ou qualquer imposição de multas, eventuais perdas e danos.

5.7 Dúvida de Enquadramento: Quaisquer situações vividas, testemunhadas ou com potencial de infração, sobre as quais você tiver dúvida de configurar quebra da conduta que se espera, devem

ser levadas ao conhecimento do Comitê de Compliance e Privacidade, Compliance Officer ou Canal de Compliance e Privacidade: compliance@interest.com.br

5.8 Revisão desta Política: Anual como prática padrão, mesmo na ausência de mudanças significativas, para garantir que a Política permaneça relevante e atualizada; Após Mudanças Significativas nas Operações ou na Legislação; Em Resposta a Denúncias ou Colaborações e Após um incidente de conduta antiética, é importante revisar esta Política para identificar quaisquer lacunas ou deficiências que possam ter contribuído para o incidente e atualizá-la para prevenir futuras ocorrências

5.9 O Comitê de Compliance e Privacidade poderá, em reunião extraordinária, deliberar sobre revisão fora do prazo anual, em havendo denúncias e colaborações sobre a presente Política que deva mudar a sua estrutura e/ou inserção de novos apontamentos de conduta.