

	<b>POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS</b>	
	Periodicidade de Revisão: Anual	Proprietário: Philip Propes, Diretor Sênior, Segurança Global de TI e Serviços Técnicos

## SUMÁRIO

OBJETIVO.....	2
ESCOPO .....	2
INTERESSADOS .....	2
RESPONSABILIDADE .....	2
COMUNICAÇÕES .....	3
POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS.....	3
1. INTRODUÇÃO .....	3
2. ESCOPO DA POLÍTICA .....	4
3. DEFINIÇÃO DOS TERMOS DE PROTEÇÃO DE DADOS .....	5
4. PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS.....	7
5. FINALIDADES ESPECÍFICAS DE NEGÓCIOS.....	7
6. AVISO AOS TITULARES DE DADOS.....	8
7. COMPARTILHAMENTO DE DADOS PESSOAIS.....	8
8. TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS .....	9
9. DADOS PRECISOS .....	10
10. RETENÇÃO DE DADOS .....	10
11. SEGURANÇA DE DADOS .....	10
12. REPORTE DE INCIDENTES DE SEGURANÇA.....	11
13. DIREITOS E REQUERIMENTOS DE TITULARES DE DADOS.....	11
14. POLÍTICAS RELACIONADAS.....	12
15. ALTERAÇÕES NESSA POLÍTICA.....	12
16. AVISO SOBRE RESTRIÇÕES AOS DIREITOS DOS FUNCIONÁRIOS.....	12
VIOLAÇÕES .....	12
RECURSOS .....	13
DOCUMENTOS RELACIONADOS.....	13
REVISORES.....	13
APROVADORES.....	13
HISTÓRICO DE REVISÃO / CONTROLE DE ALTERAÇÃO.....	13

	<b>POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS</b>	
	Periodicidade de Revisão: Anual	Proprietário: Philip Propes, Diretor Sênior, Segurança Global de TI e Serviços Técnicos

## OBJETIVO

O objetivo da Política de Proteção de Dados Pessoais é regulamentar como a Mosaic, incluindo todas as afiliadas, subsidiárias, representantes e funcionários lida com os Dados Pessoais de nossos clientes, fornecedores, funcionários, consultores e outros terceiros.

## ESCOPO

Esta Política se aplica a todos os Dados Pessoais que coletamos, mantemos, transmitimos, armazenamos, retemos ou usamos de outra forma, independentemente da mídia sobre a qual esses dados são armazenados ou se fazem referência a funcionários, clientes ou quaisquer outros Titulares de Dados. Este documento e outros documentos aqui mencionados, criam a base para nossos funcionários, agentes e representantes, incluindo nossos contratados independentes e prestadores de serviços de terceiros que têm acesso aos Dados Pessoais que detemos, tratem quaisquer Dados Pessoais que coletamos de Titulares de Dados, ou os que são fornecidos a nós por Titulares de Dados ou por outras fontes. Essas regras de proteção de Dados Pessoais e condições legais devem ser seguidas quando obtivermos, manusearmos, processarmos, transferirmos ou armazenarmos Dados Pessoais. Esta Política não faz parte do contrato de trabalho de qualquer empregado, e podemos alterá-la a qualquer momento com ou sem aviso prévio.

## INTERESSADOS

As Partes Interessadas e o órgão de revisão desta Política incluem as seguintes equipes:

- Tecnologia da Informação e Segurança Cibernética
- Rede de TI
- Sistemas Corporativos de TI
- Departamento Jurídico da Mosaic

## RESPONSABILIDADE

O Encarregado Global/Local pelo Tratamento de Dados Pessoais ("Global/Local Data Protection Officer – DPO") e o Diretor Global de Segurança Cibernética ("Diretor de Segurança de TI") são coletivamente responsáveis por garantir o cumprimento de toda a legislação aplicável e desta Política. O DPO também é responsável pela administração e supervisão da implementação desta Política e, conforme aplicável, no desenvolvimento de procedimentos operacionais, processos, Políticas, avisos, Normas e Diretrizes relacionados. Especificamente, o Diretor de Segurança de TI implementa medidas tecnológicas, físicas e políticas para garantir a segurança e a integridade dos Dados Pessoais que detemos, bem como os requisitos técnicos necessários para o cumprimento desta Política. O DPO é responsável por garantir que esta Política e as medidas empreendidas para implementar esta Política estejam em conformidade com as leis, regulamentos, práticas da Mosaic aplicáveis e por supervisionarem a implementação desta Política dentro da organização.

	<b>POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS</b>	
	Periodicidade de Revisão: Anual	Proprietário: Philip Propes, Diretor Sênior, Segurança Global de TI e Serviços Técnicos

Entre em contato com o DPO, Diretor de Segurança de TI ou com o Departamento Jurídico da Mosaic se tiver quaisquer dúvidas sobre o funcionamento desta Política ou quaisquer preocupações de que a Política não esteja sendo ou não tenha sido seguida:

- Philip Propes, Diretor Sênior de Segurança Global e Serviços Técnicos, DPO Global, Philip.Propes@mosaicco.com, +1 (813) 284-1703
- Rob Arnold, Diretor de Segurança Cibernética Global, [Rob.Arnold@mosaicco.com](mailto:Rob.Arnold@mosaicco.com), +1 (813) 557-8611
- Murici Ferreira Martins, Diretor Jurídico e DPO local para Brasil e Paraguai, [Murici.Martins@mosaicco.com](mailto:Murici.Martins@mosaicco.com), +55 11 4950-2806
- Shannon Hern, Vice-Presidente de *Compliance* e Conselheira Sênior de Trabalho e Emprego, [Shannon.Hern@mosaicco.com](mailto:Shannon.Hern@mosaicco.com), +1 (813) 500-6780

Será responsabilidade de *designers*, engenheiros, empreiteiros, fornecedores, gerentes e gestores de fornecedores envolvidos na especificação, compra, instalação, ou manutenção de qualquer equipamento de Tecnologia da Informação (TI), Tecnologia Operacional (TO) ou Sistemas de Controle Industrial (SCI) para aderir ao estabelecido nesta Política.

## COMUNICAÇÕES

O desenvolvimento e manutenção deste documento é de responsabilidade do Departamento de TI da Mosaic. Solicitações de modificações, acréscimos ou exclusões serão encaminhadas para a equipe de Especialistas em Assuntos de Revisão de Segurança Cibernética.

## POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS

### 1. INTRODUÇÃO

- 1.1 Esse esta Política de Proteção de Dados Pessoais ("Política") rege como a Mosaic, incluindo todas as afiliadas, subsidiárias, representantes, diretores estatutários e funcionários ("você", "nós" ou "Mosaic") tratamos Dados Pessoais de nossos clientes, fornecedores, funcionários, e outros terceiros.
- 1.2 Durante nossas operações de negócios, podemos coletar e tratar Dados Pessoais. Isso pode incluir dados que recebemos diretamente de uma pessoa (por exemplo, preenchendo formulários ou por correspondência conosco por correio, telefone, e-mail ou de outra forma) e dados que recebemos de outras fontes (incluindo, por exemplo, parceiros de negócios, subcontratados em serviços técnicos, de pagamento, de entrega, agências de referência de crédito, e outros).
- 1.3 Reconhecemos que o tratamento correto e lícito desses dados manterá a confiança na Mosaic e resultará em operações de negócios bem-sucedidas. A proteção da confidencialidade e da integridade dos Dados Pessoais é uma responsabilidade crítica que devemos sempre levar a sério. A Mosaic valoriza o direito dos indivíduos de manter o controle e a confidencialidade sobre as informações sobre si mesmos e adotou esta Política em consonância com esses valores.

	<b>POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS</b>	
	Periodicidade de Revisão: Anual	Proprietário: Philip Propes, Diretor Sênior, Segurança Global de TI e Serviços Técnicos

- 1.4 Você deve cumprir esta Política ao tratar Dados Pessoais em nosso nome. Nós vamos realizar revisões periódicas e auditorias para avaliar o cumprimento da política. Qualquer violação desta Política ou de Diretrizes, procedimentos operacionais ou processos relacionados destinados a proteger Dados Pessoais pode resultar em ações disciplinares, até e incluindo rescisão.
- 1.5 Todo o pessoal da Mosaic com acesso a Dados Pessoais ou responsabilidade para supervisionar pessoal com acesso a Dados Pessoais deve ler esta Política e participar regularmente do treinamento sobre seus requisitos.
- 1.6 Devemos também garantir a gestão e supervisão adequadas sobre qualquer terceiro a quem se confia Dados Pessoais que detemos por meio de contratos apropriados. Todo o pessoal da Mosaic que gerencia relacionamentos de terceiros envolvendo Dados Pessoais também deve ler esta Política e receber treinamento sobre suas exigências.

## 2. ESCOPO DA POLÍTICA

- 2.1 Dados Pessoais estão sujeitos a certas salvaguardas legais, que variam dependendo do escopo da legislação aplicável, por exemplo, onde reside o Titular dos Dados. Dependendo de onde reside o Objeto de Dados, por exemplo, essas salvaguardas legais podem incluir o seguinte:
  - Lei de Privacidade de Informações Biométricas ("BIPA") - Illinois
  - Lei Geral de Proteção de Dados Pessoais ("LGPD") - Brasil
  - Lei de Proteção de Informações Pessoais e Documentos Eletrônicos ("PIPEDA") - Canadá
  - Lei de Proteção de Informações Pessoais ("PIPL") - China
  - Outras leis aplicáveis (coletivamente "legislação aplicável").
- 2.2 Esta Política e quaisquer outros documentos nela referidos, estabelece a base na qual nossos funcionários, agentes e representantes, incluindo nossos contratados independentes e prestadores de serviços de terceiros que tenham acesso aos Dados Pessoais que detemos, tratarão quaisquer Dados Pessoais que coletamos de Titulares de Dados, ou que nos sejam fornecidos por Titulares de Dados ou outras fontes.
- 2.3 Esta Política não faz parte do contrato de trabalho de qualquer empregado, e podemos alterá-la a qualquer momento com ou sem aviso prévio.
- 2.4 Esta Política estabelece as regras de proteção de Dados Pessoais e as condições legais que devemos seguir quando obtemos, manuseamos, tratamos, transferimos ou armazenamos Dados Pessoais.
- 2.5 O Encarregado Global/Local pelo Tratamento de Dados Pessoais ("Global/Local Data Protection Officer – DPO") e o Diretor Global de Segurança Cibernética ("Diretor de Segurança de TI") são coletivamente responsáveis por garantir o cumprimento de toda a legislação aplicável e desta Política. O DPO também é responsável pela gestão e supervisão da implementação desta Política e, conforme aplicável, no desenvolvimento de procedimentos operacionais, processos, políticas, avisos e diretrizes relacionadas. Especificamente, o Diretor de Segurança de TI implementa medidas tecnológicas, físicas e políticas para garantir a segurança e a integridade dos Dados Pessoais que

	<b>POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS</b>	
	Periodicidade de Revisão: Anual	Proprietário: Philip Propes, Diretor Sênior, Segurança Global de TI e Serviços Técnicos

detemos, bem como os requisitos técnicos necessários para o cumprimento desta Política. O DPO é responsável por garantir que esta Política e as medidas empreendidas para implementar esta Política estejam em conformidade com a legislação aplicável e com as práticas da Mosaic e por supervisionar a implementação desta Política dentro da Mosaic. O atual DPO Global é Philip Propes, Diretor Sênior de Segurança Global e Serviços Técnicos, Philip.Propes@mosaicco.com, sendo que para o Brasil e Paraguai o DPO é Murici Martins, Diretor Jurídico, murici.martins@mosaicco.com. O atual Diretor de Segurança de TI é Rob Arnold, Rob.Arnold@mosaicco.com. Por favor, entre em contato com estas pessoas, ou com o Departamento Jurídico da Mosaic se tiver quaisquer perguntas sobre o funcionamento desta Política ou quaisquer preocupações de que a Política não esteja sendo seguida ou não tenha sido seguida.

### 3. DEFINIÇÃO DOS TERMOS DE PROTEÇÃO DE DADOS

- 3.1 **Titular de Dados** significa o indivíduo sobre o qual se referem os dados pessoais. Os Titulares de Dados podem ser nacionais ou residentes de qualquer país e pode ter direitos sobre seus Dados Pessoais.
- 3.2 **Dados Pessoais** significa informações que identificam um Titular de Dados ou informações relacionadas a um Titular de Dados que podemos identificar (direta ou indiretamente) a partir desse dado isoladamente ou em combinação com outros dados que possuímos ou podemos acessar razoavelmente. Dados Pessoais podem ser factuais (por exemplo, um nome, endereço de e-mail, local ou data de nascimento) ou uma opinião sobre as ações ou comportamento dessa pessoa.

Os Dados Pessoais incluem especificamente, mas não se limitam às seguintes categorias de dados:

- a) Identificadores e Informações Pessoais Gerais: nomes, pseudônimos, endereço postal, endereços de e-mail, nomes de contas, IDs de usuário, número de Previdência Social, número da habilitação de motorista, número do passaporte, números de identificação do governo, identificação fiscal, placas de veículos, características físicas ou descrição, número da apólice de seguro, e números de telefone.
- b) Informações comerciais e financeiras: registros de bens pessoais individuais de propriedade de clientes da Mosaic, registros de bens e ativos coletados em conexão com aceite de uma garantia pessoal, números de contas bancárias e financeiras, números de identificação associados a contas bancárias, informações sobre folha de pagamento, informações de crédito, informações e pagamentos sobre convênio de saúde, dados salariais e informações da instituição bancária.
- c) Informações biométricas: registros de impressões digitais associados ao TWIC (Carteira de Identificação do Trabalhador no Transporte) para os empregados que detêm cartões TWIC; *scans* de retina ou íris, impressão de voz, e *scans* de geometria da mão e rosto para aqueles funcionários que fornecem essas informações para a Mosaic; e registros de movimento dentro de uma instalação Mosaic para esses funcionários que fornecem dados de movimento para a Mosaic.
- d) Internet ou Atividades em Redes Similares: histórico de navegação e histórico de pesquisa em dispositivos de propriedade da Mosaic, informações sobre a interação de um Titular de Dados

com sites Mosaic e informações coletadas e fornecidas pelo Google Analytics sobre a interação de um Titular de Dados com sites.

- e) Dados de geolocalização: informações de localização coletadas a partir do uso do cartão de acesso, informações de registro de visitantes, histórico de condução e informações de condução coletadas de veículos Mosaic e locais dentro de uma instalação Mosaic para funcionários que fornecem dados de movimento para Mosaic.
- f) Dados Sensoriais: fotografias de funcionários e visitantes, gravações de áudio e vídeo capturadas nas instalações da Mosaic e *scans* de temperatura na entrada das instalações da Mosaic.
- g) Dados Profissionais ou Relacionados ao Emprego: registros de treinamento, avaliações de desempenho, registros de emprego fornecidos por ex-empregadores à Mosaic, informações fornecidas como parte de verificações de antecedentes e testes de drogas e álcool, e outros dados relacionados ao emprego com a Mosaic.
- h) Informações de Educação: identificação das escolas(s) atendidas, verificações de escolaridade e diplomas conquistados.
- i) Inferências extraídas de Informações Pessoais: perfis que refletem preferências de funcionários e clientes, avaliações de desempenho, perfis de gestão de relacionamento com o cliente, resultados de seleção pré-contratação e acomodações solicitadas.

3.3 **Dados Pessoais Sensíveis** são Dados Pessoais relativos à origem racial ou étnica, opiniões políticas, crenças religiosas ou similares, filiação sindical ou religiosa, dados relativos à saúde ou à vida sexual (por exemplo, condição de saúde física ou mental, *status* de vacinação, orientação sexual ou informações genéticas familiares). Em algumas jurisdições, também pode incluir todos os Dados Pessoais sobre pessoas menores de 16 anos e informações sobre a idade de uma pessoa se acima de 40 anos. Dados Pessoais Sensíveis, em algumas jurisdições, também incluem conta financeira, ou informações de crédito, número de cartão de crédito ou débito, código de acesso de segurança ou senha quando informações suficientes são fornecidas para permitir que um terceiro tenha acesso às contas financeiras do Titular dos Dados. Em certas jurisdições fora dos Estados Unidos, o tratamento de Dados Pessoais Sensíveis só pode ocorrer sob condições estritas e pode incluir uma condição que exija a permissão expressa da referida pessoa. Dados Pessoais Sensíveis são tratados pela Mosaic conforme necessário, e o acesso aos dados pessoais sensíveis é restrito apenas às pessoas que precisam desse acesso como parte de suas responsabilidades de trabalho.

3.4 **Tratamento** significa qualquer atividade que envolva o uso de Dados Pessoais. Inclui a obtenção, gravação, a detenção dos dados, a realização de qualquer operação ou conjunto de operações sobre os dados, incluindo organizar, alterar, recuperar, usar, divulgar, apagar ou destruí-los. O Tratamento também inclui a transferência de Dados Pessoais para terceiros.

3.5 **Incidente de Segurança** significa qualquer ato ou omissão que comprometa a segurança, confidencialidade, integridade ou disponibilidade de Dados Pessoais ou as salvaguardas físicas, técnicas, administrativas ou organizacionais que nós ou nossos fornecedores de serviços terceirizados colocamos em prática para protegê-los. A perda ou o acesso não autorizado, divulgação ou aquisição de Dados Pessoais é um incidente de segurança.

- 3.6 **Controlador de Dados** é a pessoa ou organização que determina quando, por que e como tratar Dados Pessoais e é responsável por estabelecer práticas e políticas em consonância com a Legislação Aplicável. Somos o Controlador de Dados de todos os Dados Pessoais usados em nosso negócio para nossos próprios fins comerciais.

#### 4. PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS

- 4.1 Aderimos aos princípios gerais de Privacidade de Dados ao coletar e tratar pessoalmente Dados que exigem:
- Coletar e usar Dados Pessoais de forma justa e única para fins legais e especificados relacionados com nossos objetivos de negócios legítimos.
  - Limitar nossa coleta de Dados Pessoais ao que é adequado, relevante e não excessivo para a finalidade pretendida.
  - Notificar os indivíduos sobre nossas práticas de Tratamento de Dados Pessoais de forma clara e transparente.
  - Certificar-se da exatidão dos Dados Pessoais que coletamos, detemos e utilizamos.
  - Reter Dados Pessoais apenas pelo tempo necessário para cumprir a finalidade estabelecida.
  - Respeitar os direitos dos Titulares de Dados.
  - Proteger os Dados Pessoais que armazenamos e não os transferir para dispositivos pessoais e/ou a terceiros sem autorização aplicável.

#### 5. FINALIDADES ESPECÍFICAS DE NEGÓCIOS

- 5.1 Você só pode acessar Dados Pessoais para o exercício de suas funções de trabalho e sob a base na necessidade de saber. Você não pode acessar Dados Pessoais por qualquer razão não relacionada aos seus deveres de trabalho. Acessar Dados Pessoais por razões fora do desempenho de suas funções de trabalho pode sujeitar você à ação disciplinar, resultando inclusive em rescisão.

- 5.2 Você só pode coletar e processar dados pessoais para fins específicos razoavelmente necessários para realizar nossos legítimos Objetivos de Negócios. A Legislação Aplicável pode restringir ainda mais nossas ações relativas a Dados Pessoais a propósitos legais específicos. Estas restrições não são destinadas a impedir o tratamento de dados pessoais, mas a garantir que tratamos Dados Pessoais de forma justa e sem afetar negativamente os direitos dos Titulares de Dados.

Os fundamentos do tratamento lícito podem incluir o seguinte:

- O Titular de Dados consentiu inequivocamente, quando necessário.
- O Tratamento é necessário para a execução de um contrato com o Titular de Dados.
- Para cumprir nossas obrigações legais.
- Proteger os interesses vitais do Titular de Dados.
- Quando necessário para o desempenho de tarefas de interesse público, incluindo, mas não limitado ao compromisso da Mosaic com a segurança e a sustentabilidade.
- Para atender aos legítimos interesses comerciais da Mosaic. Uma lista não exaustiva destes interesses incluem prevenção de fraudes, listas de vigilância contra lavagem de dinheiro, defesa de requerimentos, verificação de crédito e avaliações de risco, garantia de rede e informações de segurança, resposta a questões de negócios, marketing direto, tratamento de dados de funcionários ou de clientes, indicação de possíveis atos criminosos ou ameaças à segurança



## POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS

Periodicidade de  
Revisão: Anual

Proprietário: Philip Propes, Diretor Sênior, Segurança Global de TI e Serviços  
Técnicos

pública, realizar transferências administrativas para e entre afiliados da Mosaic, execução do Código de Conduta Ética de Negócios, Canal de Ética e relatórios sob o Sarbanes-Oxley Act (SOX), sanções econômicas e triagem de controle de exportação, prevenção de perdas de dados, cumprimento de pedidos de divulgação à aplicação da lei, tribunais e órgãos reguladores, processamento de sinistros de seguros, privacidade e prevenção de malware, desenvolvimento e aprimoramento de produtos, *due diligence* e autorregulação.

- 5.3 Conforme exigido pela Legislação Aplicável para a localização do Titular de Dados aplicável, notificaremos o Titular de Dados das finalidades comerciais específicas quando coletarmos pela primeira vez os dados ou o mais rápido possível posteriormente (ver Seção 6, Notificação dos Titulares de Dados). Qualquer coleta e Tratamento de Dados Pessoais que você conduz também deve cumprir esse aviso e quaisquer outras divulgações de privacidade relacionadas. Você não pode usar Dados Pessoais para finalidades novas, diferentes ou incompatíveis com as quais você os coletou, a menos que o Titular de Dados concorde com o novo uso depois de receber um Aviso de Privacidade revisado.
- 5.4 Ao tratar Dados Pessoais Sensíveis, você deve atender a quaisquer condições adicionais exigidas pela Legislação Aplicável, como o consentimento explícito do Titular de Dados.
- 5.5 Manter e reter registros corporativos precisos que refletem nossas atividades de tratamento de dados, incluindo, mas não se limitando ao Registro Brasileiro de Operações de Tratamento (“ROPA”).

## 6. AVISO AOS TITULARES DE DADOS

- 6.1 Quando os Dados Pessoais são coletados diretamente dos Titulares de Dados, inclusive para recursos humanos ou finalidades de emprego, quando exigido pela legislação aplicável, informaremos os Titulares de Dados sobre como e por que vamos utilizar, processar, divulgar, proteger e reter esses dados por meio de um Aviso de Privacidade aprovado apresentado quando a pessoa fornece os dados. O Aviso de Privacidade também fornecerá informações do contato do Time de Privacidade, incluindo a identidade do Diretor de Segurança de TI e DPOs da Mosaic.
- 6.2 Quando exigido pela legislação aplicável, quando você coleta Dados Pessoais diretamente do Titular dos Dados, você lhes fornecerá informações sobre como e por que vamos usar, processar, divulgar, proteger e reter seus Dados Pessoais por meio de um Aviso de Privacidade aprovado.
- 6.3 Entre em contato com o Diretor de Segurança de TI da Mosaic ou com o DPO apropriado, caso não tenha certeza se um uso específico é apropriado, se tiver dúvidas sobre os Avisos de Privacidade que se aplicam a Dados Pessoais coletados, ou se você precisa obter um Aviso de Privacidade aprovado antes de coletar Dados Pessoais.

## 7. COMPARTILHAMENTO DE DADOS PESSOAIS

- 7.1 Você só pode compartilhar os Dados Pessoais que temos com outro funcionário, agente ou representante do nosso grupo, que inclui subsidiárias Mosaic e a matriz de nossa empresa, juntamente com suas subsidiárias, se o destinatário tem um trabalho relacionado ou uma



	<b>POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS</b>	
	Periodicidade de Revisão: Anual	Proprietário: Philip Propes, Diretor Sênior, Segurança Global de TI e Serviços Técnicos

necessidade de saber essas informações e a transferência cumpre com quaisquer restrições aplicáveis a transferências internacionais (ver seção 8, Transferências Internacionais de Dados Pessoais).

- 7.2 Você só pode compartilhar os Dados Pessoais que detemos com terceiros, como nossos fornecedores de serviços se **todas** as seguintes condições se aplicarem:
- Eles precisam saber as informações para a finalidade de fornecer os serviços contratados.
  - O compartilhamento dos Dados Pessoais está em conformidade com o Aviso de Privacidade fornecido ao Titular de Dados e, se necessário, o consentimento do Titular de Dados foi obtido.
  - Eles concordaram em cumprir o *Anexo de Segurança da Mosaic*.
  - A transferência está em conformidade com quaisquer restrições aplicáveis de transferência internacionais (ver seção 8, Transferências Internacionais de Dados Pessoais).
  - Você tem um contrato por escrito totalmente executado, revisado e aprovado de acordo com as políticas da Mosaic.
- 7.3 Você também pode compartilhar os Dados Pessoais de um Titular de Dados com terceiros se receber uma aprovação prévia por escrito do DPO ou do Departamento Jurídico da Mosaic, indicando que as circunstâncias especiais se aplicam, como uma divulgação necessária para cumprir com obrigações legais, executar um contrato ou outro acordo com o Titular de Dados, responder ou se defender contra um requerimento, fornecer informações relacionadas a sinistros de seguro, proteger a segurança de nossos funcionários, clientes ou outros, ou proteger nossos direitos ou propriedades. Isso **inclui** a troca de informações com terceiros para fins de proteção contra fraudes e redução do risco de crédito.
- 7.4 Se você não tem certeza se uma divulgação específica é apropriada ou permitida, você deve consultar o DPO apropriado ou o Departamento Jurídico da Mosaic.

## 8. TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS

- 8.1 Você transfere internacionalmente Dados Pessoais originários de um país para outro quando você transmitir, enviar, visualizar ou acessar esses dados dentro ou para um país diferente. A legislação aplicável em certos países, como Brasil e China, podem restringir essas Transferências Internacionais de Dados Pessoais.
- 8.2 Você só pode transferir dados pessoais sujeitos a restrições de Transferências Internacionais se **uma** das seguintes condições se aplicam:
- O país para o qual transferimos os Dados Pessoais garante um nível adequado de proteção aos direitos e liberdades dos Titulares de Dados;
  - O Titular de Dados fornece consentimento informado para a transferência; ou
  - O Diretor de Segurança de TI da Mosaic ou o DPO apropriado conclui que a transferência cumpre todas as restrições de transferências internacionais relevantes e aprova por escrito.

	<b>POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS</b>	
	Periodicidade de Revisão: Anual	Proprietário: Philip Propes, Diretor Sênior, Segurança Global de TI e Serviços Técnicos

## 9. DADOS PRECISOS

- 9.1 Você garantirá que os Dados Pessoais que tratamos sejam precisos, completos, atualizados e relevantes para a finalidade para a qual os coletamos. Você verificará a precisão de quaisquer Dados Pessoais no ponto de coleta e em intervalos regulares posteriormente. Você tomará todas as medidas razoáveis para destruir ou alterar Dados Pessoais imprecisos ou desatualizados.
- 9.2 Embora garantir a exatidão e a completude dos Dados Pessoais seja de responsabilidade de todos os funcionários, a Gestão da Mosaic deve especificamente envidar esforços razoáveis para garantir que todos os Dados Pessoais mantidos pela Mosaic sejam precisos e completos. A Gestão também deve envidar esforços razoáveis para garantir que os termos desta Política sejam seguidos pelos funcionários sob sua supervisão, que todas as informações privadas sejam usadas apenas como pretendido, e que as precauções que previnem o uso indevido sejam eficazes e apropriadas.

## 10. RETENÇÃO DE DADOS

Você não deve manter os Dados Pessoais por mais tempo do que o necessário para a finalidade de negócios ou as finalidades para as quais originalmente os coletou. Você tomará todas as medidas razoáveis para destruir, ou apagar de nossos sistemas, todos os Dados Pessoais que não precisamos mais, para incluir backup de dados, em total conformidade com o *Registro Global da Mosaic e a Política de Gestão da Informação*.

## 11. SEGURANÇA DE DADOS

- 11.1 Você é responsável por proteger os Dados Pessoais que detém. Você deve adotar medidas de segurança razoáveis e apropriadas contra o tratamento ilegal ou não autorizado de Dados Pessoais e contra a perda acidental ou danos aos Dados Pessoais. Você deve exercer um cuidado especial na proteção de Dados Pessoais Sensíveis contra perdas e acesso, uso ou divulgação não autorizados.
- 11.2 Você deve seguir todos os procedimentos e tecnologias que colocamos em prática para manter a segurança de todos os Dados Pessoais do ponto de coleta até o ponto de destruição. Você só pode transferir Dados Pessoais para fornecedores de serviços de terceiros que concordam em cumprir com as políticas e procedimentos requeridos, incluindo, mas não se ao Anexo de Segurança da Mosaic, e que concordam em implementar medidas adequadas, se solicitado.
- 11.3 Você deve manter a Segurança de Dados protegendo a confidencialidade, integridade e disponibilidade dos Dados Pessoais, definidos da seguinte forma:
- Confidencialidade** significa que apenas as pessoas que têm uma necessidade de conhecer e são autorizadas a usar os dados podem acessá-los.
  - Integridade** significa que os Dados Pessoais são precisos e adequados para a finalidade para a qual são tratados.
  - Disponibilidade** significa que os usuários autorizados podem ter acesso aos dados quando eles forem necessários para finalidades autorizadas.

	<b>POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS</b>	
	Periodicidade de Revisão: Anual	Proprietário: Philip Propes, Diretor Sênior, Segurança Global de TI e Serviços Técnicos

11.4 Você deve cumprir e não tentar contornar todos os aspectos aplicáveis do nossas *Políticas de Segurança de TI Mosaic*, com as salvaguardas administrativas, físicas e técnicas que implementamos e mantemos de acordo com a legislação aplicável e com os Padrões de proteção de Dados Pessoais.

A Mosaic desenvolveu, implementou e mantém as salvaguardas adequadas a:

- a) Nosso tamanho, escopo, negócios e recursos disponíveis.
- b) A quantidade e a natureza dos Dados Pessoais que controlamos ou mantemos.
- c) Os riscos identificados associados aos Dados Pessoais.

## 12. REPORTE DE INCIDENTES DE SEGURANÇA

12.1 Se você sabe ou suspeita que um incidente de segurança ocorreu, não tente investigar o assunto você mesmo. Entre em contato imediatamente com a Tecnologia da Informação da Mosaic, o Departamento de Segurança de TI da Mosaic, ou Diretor de Segurança de TI. Além desse contato, você não deve discutir este incidente com qualquer outra pessoa, exceto se autorizado pelo Diretor de Segurança de TI da Mosaic ou como determinado pela *Política de Gestão de Incidente de Cibersegurança da Mosaic*.

12.2 Se o Diretor de Segurança de TI da Mosaic determinar que um incidente de dados tem ou pode ter ocorrido, o Diretor de Segurança de TI deve seguir a Política e/ou Plano de Gestão de Incidente de Cibersegurança. Você deve preservar todas as evidências relacionadas com o potencial incidente de segurança. Se as comunicações escritas forem trocadas relacionadas aos dados incidente, o Departamento Jurídico da Mosaic deve ser copiado (cc) em todas as correspondências.

## 13. DIREITOS E REQUERIMENTOS DE TITULARES DE DADOS

13.1 Os Titulares de Dados têm direitos quando ao que se refere em como lidamos com seus Dados Pessoais.

Esses direitos variam de acordo com a legislação aplicável, mas podem incluir os seguintes:

- a) Solicitar acesso aos seus Dados Pessoais que mantemos.
- b) Impedir o uso de seus Dados Pessoais para fins de *marketing* direto sem base legal.
- c) Pedir para excluir dados pessoais ou corrigir dados imprecisos (ver seção 9, Dados Precisos).
- d) Impedir o tratamento que possa causar danos ou angústia ao Titular de Dados ou qualquer outra pessoa.

13.2 Os Titulares de Dados devem fazer uma solicitação por escrito para acessar, corrigir ou excluir os Dados Pessoais que temos sobre eles. Antes de atender à solicitação do Titular de Dados, você deve verificar se a pessoa que faz a solicitação está autorizada a receber tal acesso ou fazer essa correção ou exclusão através de uma confirmação de identidade.

13.3 Todas as solicitações dos Titulares de Dados devem ser encaminhadas ao Encarregado pelo Tratamento de Dados (“Data Protection Officer – DPO”) apropriado da Mosaic, que irá:

	<b>POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS</b>	
	Periodicidade de Revisão: Anual	Proprietário: Philip Propes, Diretor Sênior, Segurança Global de TI e Serviços Técnicos

- i. Verificar a identidade do Titular que fez a solicitação para confirmar que é o mesmo indivíduo a quem a solicitação se refere ou que é uma pessoa autorizada a agir em nome de tal Titular;
- ii. Analisar a documentação de Proteção de Dados Mosaic (por exemplo, Registro de Operações de Tratamento Mosaic) e, se necessário, entrar em contato com outros departamentos da Mosaic para coletar as informações adequadas (por exemplo, Departamento de Recursos Humanos); e
- iii. Responder ao Titular de Dados dentro do prazo aplicável na jurisdição. Mesmo que o pedido não possa ser concedido, ele deve ser respondido com uma explicação.

13.4 Você deve cumprir as leis aplicáveis relativas aos direitos dos Titulares de Dados. Se você não tiver certeza dos requisitos legais aplicáveis ou da resposta adequada a qualquer solicitação ou reclamação do Titular de Dados, você deve solicitar assistência ao seu supervisor ou entrar em contato com o DPO apropriado. Não permita que terceiros o convençam a divulgar Dados Pessoais sem a devida autorização.

## 14. POLÍTICAS RELACIONADAS

Você também deve cumprir com quaisquer outras políticas da Mosaic que enderecem a coleta, uso, armazenamento, proteção e manuseio de Dados Pessoais. Você deve se familiarizar com as seguintes Políticas:

- a) Política de Segurança da Informação
- b) Política de Uso Aceitável
- c) Política Global de Registros e Gerenciamento de Informações
- d) Política de Gestão de Resposta a Incidentes da Mosaic.

## 15. ALTERAÇÕES NESSA POLÍTICA

Reservamo-nos no direito de alterar esta Política a qualquer momento.

## 16. AVISO SOBRE RESTRIÇÕES AOS DIREITOS DOS FUNCIONÁRIOS

16.1 Não pretendemos que esta Política obste ou dissuada os funcionários de se envolverem em atividades trabalhistas legalmente protegidas, incluindo quaisquer direitos ao trabalho e ao emprego e leis aplicáveis, como aquelas que regem a discussão de salários, benefícios ou termos e condições de emprego, formação, adesão ou apoio a sindicatos, negociação coletiva através de representantes de sua escolha, levantando reclamações sobre condições de trabalho para sua ajuda ou proteção mútua e seus companheiros de trabalho, ou outras atividades legalmente protegidas.

16.2 Os termos de emprego estabelecidos nesta Política funcionam em conjunto com, e não substituem, alteram, ou complementam quaisquer termos ou condições de emprego declarados em qualquer acordo coletivo de negociação que você pode ter com Mosaic.

## VIOLAÇÕES

Qualquer violação desta Política pode resultar em ações disciplinares, até e incluindo a rescisão do emprego. A Mosaic reserva-se no direito de notificar as autoridades policiais apropriadas de qualquer

	<b>POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS</b>	
	Periodicidade de Revisão: Anual	Proprietário: Philip Propes, Diretor Sênior, Segurança Global de TI e Serviços Técnicos

atividade ilícita e cooperar em qualquer investigação de tal atividade. Funcionários e consultores são encorajados a denunciar quaisquer violações desta Política imediatamente à gestão.

## RECURSOS

NIST (Instituto Nacional de Normas e Tecnologia) Publicação Especial (SP) 800-53 Revisão 5 – Controles de Segurança e Privacidade para Sistemas de Informação e Organizações.

## DOCUMENTOS RELACIONADOS

Política de Uso Aceitável da Mosaic  
 Política de Gestão de Incidentes de Cibersegurança da Mosaic  
 Plano de Incidentes de Cibersegurança da Mosaic  
 Política Global de Gerenciamento de Informações Mosaic  
 Programa de Segurança da Informação Mosaic  
 Política de Segurança da Informação Mosaic  
 Registro de Atividades de Tratamento Mosaic  
 Anexo de Segurança Mosaic

## REVISORES

NOME	TÍTULO
Glenn Salvo	Advogado Corporativo Sênior
Jatarra Warren	Líder de Segurança Cibernética TI
Beth Flasker	Analista Sênior de Segurança de TI

## APROVADORES

NOME	TÍTULO
Philip Propes	Diretor Sênior, Segurança Global de TI e Serviços Técnicos
Rob Arnold	Diretor, Risco de Segurança de TI e Conformidade

## HISTÓRICO DE REVISÃO / CONTROLE DE ALTERAÇÃO

VERSÃO #	DESCRIÇÃO DA MUDANÇA	NOME	TÍTULO	DATA DE REVISÃO
1.0	Inicial	Glenn Salvo	Conselho Corporativo Sênior	16 de março de 2022
1.1	Acrescentar Philip Propes como DPO	Beth Flasker	Analista Sênior de Segurança de TI	26 de outubro de 2022

	<b>POLÍTICA GLOBAL DE PROTEÇÃO DE DADOS PESSOAIS</b>	
	Periodicidade de Revisão: Anual	Proprietário: Philip Propes, Diretor Sênior, Segurança Global de TI e Serviços Técnicos

	Global e Remover Shannon Hern			
--	----------------------------------	--	--	--