

PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE

HANDSCHUHE do Brasil, deseja manter uma relação de confiança e transparência com todos àqueles com quem se relaciona.

Por isso, divulgamos e compartilhamos a todos os interessados as práticas e medidas adotadas pela **HANDSCHUHE** do Brasil visando a preservação da segurança da informação, bem como a legalidade dos processos adotados que amparam a operacionalização e gestão de suas atividades.

Nossa Política de Segurança e Informação poderá ser atualizada a qualquer tempo, em decorrência de eventual modificação normativa e/ou mudanças de procedimentos.

1 Objetivo

Explicar e divulgar a todos os interessados as práticas e medidas adotadas pela **HANDSCHUHE** visando a preservação da segurança da informação, bem como a legalidade dos processos adotados que amparam a operacionalização e gestão de suas atividades.

Esta Política poderá ser atualizada a qualquer tempo, em decorrência de eventual modificação normativa e/ou mudanças de procedimentos.

2 Definições

Para os fins desta Política, serão consideradas as seguintes definições:

LGPD – LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709)

Regulamenta o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos de liberdade e de privacidade através de normas criadas para serem seguidas por empresas e governos na coleta e tratamento de dados pessoais

DADOS PESSOAIS

É qualquer informação que permita a identificação direta ou indireta da pessoa, como: CPF, nome e sobrenome, RG, data e local de nascimento, endereço, e-mail, fotos, renda, hábitos de consumo, histórico de pagamentos, número de cartão bancário, número de telefone, dentre outras.'

DADOS PESSOAIS SENSÍVEIS

São os dados pessoais 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.

TRATAMENTO DE DADOS PESSOAIS

Toda e qualquer operação realizada com os Dados Pessoais dos TITULARES como coleta, recepção, acesso, reprodução, processamento, modificação, avaliação, classificação, utilização, compartilhamento, distribuição, comunicação, armazenamento, controle da informação, eliminação, difusão ou extração.

CONSENTIMENTO

Manifestação livre, informada e inequívoca pela qual o titular ou responsável concorda com o tratamento dos dados pessoais para uma finalidade determinada.

ANONIMIZAÇÃO

É a exclusão ou alteração de dados pessoais de tal forma que não possam mais ser atribuídos a um determinado indivíduo ou determinável, ou apenas com um esforço desproporcionalmente alto em termos de tempo, custo e trabalho.

PSEUDONIMIZAÇÃO

É a substituição do nome de um indivíduo e outras características identificáveis por um rótulo para evitar sua identificação por pessoas não autorizadas ou para tornar essa identificação substancialmente difícil.

BASES LEGAIS

São as condições legais previstas na LGPD que autorizam a HANDSCHUHE a tratar dados pessoais.

TITULAR

É a pessoa natural à qual se referem os dados pessoais, por exemplo, colaboradores, clientes, fornecedores, prestadores de serviços e outros.

CONTROLADOR

É a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

OPERADOR

É a pessoa natural ou jurídica, de direito público ou privado que realiza o tratamento em nome do controlador.

ENCARREGADO / DPO

Responsável na empresa por cuidar da sua privacidade, e que atua como um canal de ligação e comunicação, entre o controlador, os titulares de dados, e a ANPD.

ANPD (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS)

Órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

3 Diretrizes

A **HANDSCHUHE** do Brasil está em conformidade com as boas práticas de segurança da informação e à Lei nº 13.709/2018 – Lei Geral de Proteção aos Dados, de forma a garantir a integridade e confidencialidade dos dados e informações de seus colaboradores, clientes, fornecedores, parceiros, prestadores de serviços, e-mails, contabilidade, finanças e arquivos, tendo como prioridade assegurar que os dados pessoais e demais informações relativas ao negócio estejam seguras e em sigilo.

CONTROLADOR

Adriana Assaf, contato aassaf@handschuhe.com.br

BASE LEGAL - TRATAMENTO

Inciso II, do artigo 7º, da LGPD com a finalidade exclusiva de atender aos propósitos legítimos e específicos da **HANDSCHUHE** para a produção e comercialização de luvas de EPI.

DADOS PESSOAIS TRATADOS E SUAS FINALIDADES

Todos os dados e informações coletadas e tratadas pela **HANDSCHUHE** tem como finalidade exclusiva a de atender aos propósitos legítimos e específicos da **empresa** para a produção e comercialização de luvas de EPI e sempre em conformidade com a lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.

a. Dados dos Colaboradores

Os curriculuns recepcionados serão tratados exclusivamente para a análise da conformidade da qualificação e requisitos da vaga específica e, se for o caso, para o contato para da oferta de trabalho.

Para a **SELEÇÃO** de Colaboradores, são tratados os seguintes Dados Pessoais:

Nome Completo, RG, CPF, Nacionalidade, Estado Civil, Endereço, CEP, Cidade, E-mail, Telefone, Telefone Celular, Formação, Histórico Escolar/Acadêmico, Estado Civil, Data de Nascimento, Idade, Cargo, Relação das Empresas em que manteve vínculo de trabalho com o respectivo endereço, Referências, Remuneração, Data de Contratação, Jornada de Trabalho e Foto.

Para a **ADMISSÃO** dos Colaboradores, Gestão de Folha de Pagamentos e de Recursos Humanos são solicitados os seguintes Documentos para a coleta de dados pessoais:

- a. Cópia do RG, CPF, Título de Eleitor; e Comprovante de Endereço;
- b. Original e cópia da carteira de trabalho (CTPS);
- c. Inscrição no PIS/Pasep;
- d. Original e cópia do registro profissional emitido pelo órgão da classe;
- e. Cópia da certidão de nascimento ou certidão de casamento, se casado;
- f. Cópia do certificado de reservista;
- g. Original do atestado de saúde ocupacional
- h. Cópia da certidão de nascimento de filhos de até 21 anos;
- i. Original e cópia da carta de referência;
- j. Comprovante de abertura de conta bancária para o pagamento de salário.

Também são solicitadas informações para contato, tais como endereço completo, telefone fixo e /ou celular e e-mail.

Como regra geral, a **HANDSCHUHE** não coleta **DADOS PESSOAIS SENSÍVEIS**. No entanto, poderá coletar tais dados para cumprir obrigações legais ou regulatórias e atender às políticas públicas de acordo com as exigências legais, observando o prévio consentimento do TITULAR Colaborador.

O período de armazenamento dos documentos das relações trabalhistas é de:

- a. **10 (dez) Anos:** Recibos diversos (salários, 13º salário, férias); Controle de ponto; Registro PIS/PASEP; Guia da Segurança Social; Contribuição sindical

- (GRCSU); Recibo de pagamentos de salários, férias, 13º salário e controle de ponto; Cadastro Geral de Empregados e Desempregados (CAGED); Relação Anual de Informações Sociais (RAIS), Folhas de pagamento; Guias de recolhimento do INSS, salário educação, PIS/PASEP; Atestado médico; Sistemas eletrônicos de dados trabalhistas e previdenciários, Contrato de trabalho, Livro ou ficha de registro de empregado.
- b. **20 (vinte) Anos:** Exames Médicos, Contrato de trabalho, Livro ou ficha de registro de empregado
 - c. **30 (trinta anos):** Fundo de Garantia do Tempo de Serviço (FGTS); Informações à previdência social (GFIP); Guia de recolhimento rescisório do FGTS e da contribuição social (GRFC).

b. Dados dos Clientes, Fornecedores e Prestadores de Serviços

Nas relações comerciais, os dados coletados e tratados são: Empresa / Razão Social, CNPJ, Endereço comercial completo, Dados e Referências Bancárias, Histórico de Pagamentos, Score de Crédito, Histórico de Compras, Monitoramento de reclamações, levantamento de sugestões e demandas, e para trocas e devoluções com o **OBJETIVO** de:

- a. Criar um cadastro para a gestão comercial, de compras e vendas, facilitando e agilizando nosso relacionamento, prestando suporte e oferecendo nossos produtos conforme o histórico de uso através de um canal de contato ativo e analisar e avaliar nossos parceiros e fornecedores;
- b. Gestão de cobrança e pagamentos.
- c. Dar andamento em devoluções/trocas, e efetuar correções por problemas de vendas não efetuadas;
- d. Analisar produto e serviço fornecido;
- e. Gerir contratos;
- f. Monitorar o status da entrega de mercadorias,
- g. SEFAZ, emissão de notas fiscais.

SISTEMAS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS UTILIZADOS

a. OMIE

Todos os dados coletados nas relações comerciais e com os colaboradores são processados em ambiente instalado, configurado e mantido pela OMIE onde são armazenados na Amazon Web Service AWS. Através do backup “a quente”, em que os serviços não são interrompidos, ou seja, a cada dado digitado é feito um backup em tempo real.

Os dados estão protegidos contra perda, mau uso, acesso não autorizado, divulgação, alteração ou destruição (“Incidentes”) e estão em conformidade aos

padrões e procedimentos de segurança e confidencialidade estabelecidos pela legislação brasileira.

As medidas de proteção e segurança oferecidas pela Omie são:

- a. Controle de acesso restrito aos administradores;
- b. Criptografia dos dados em repouso (AES-256);
- c. Criptografia no tráfego dos dados (HTTPS / TLS 1.3);
- d. Prevenção e detecção de intrusão;
- e. Firewall de proteção para o Sistema de Gestão que monitora filtra e bloqueia tentativas de ataque;
- f. Backup em real time;
- g. Política de senha e autenticação de múltiplo fator;
- h. Políticas e normas de segurança da informação;
- i. Acordo de Confidencialidade para os colaboradores.

Para atestar a efetividade da proteção de dados, anualmente o sistema de gestão é submetido a um teste de penetração para validar a efetividade das medidas adotadas, bem como são realizadas varreduras no ambiente para identificar e tratar as vulnerabilidades. Através da Amazon são realizadas auditorias, para avaliar a segurança do ambiente hospedado na AWS. A OMIE conta com um plano de resposta a incidentes para que, no caso de eventual incidente de violação de dados pessoais, possa conter e responder ao evento, realizando as devidas comunicações aos clientes e partes interessadas.

a.1. Compartilhamento

A **HANDSCHUHE** valoriza e preserva a segurança e confidencialidade dos dados pessoais, cujos acessos estão restritos a colaboradores indicados e devidamente autorizados, observando o mínimo necessário para o cumprimento das solicitações e/ou prestação dos serviços.

A **HANDSCHUHE** proíbe a divulgação de dados pessoais compartilhados com prestadores de serviços, exceto na medida necessária para cumprir os serviços contratados, bem como, para as obrigações legais.

Observando a necessidade e boa-fé, poderá compartilhar dados pessoais nos seguintes casos:

- a. Cumprir uma lei, regulamento ou ordem judicial;
- b. Responder solicitações de informação realizadas por órgão regulador, autoridade policial e demais autoridades públicas, inclusive em casos relativos à segurança nacional;
- c. Fazer cumprir e/ou proteger propriedade ou direitos da **HANDSCHUHE**, inclusive para investigar fraudes, ajudar a prevenir ameaças de segurança a informação, ou outras atividades criminosas ou maliciosas;

- d. Proteger os interesses legítimos e de terceiros, incluindo a segurança pessoal dos colaboradores A. Cumprir uma lei, regulamento ou ordem judicial.

Recorrentemente são realizadas auditorias pela **OMIE** para avaliar a segurança do ambiente hospedado na AWS. Rapidamente é comunicado a HANDSCHUHE e partes interessadas eventual incidente de violação de dados pessoais.

a.2. Encarregado / DPO

E-mail ciso@OMIE.com.br

b. OneDrive Corporativo

A **HANDSCHUHE** utiliza o **OneDrive Corporativo** - serviço de nuvem da Microsoft, para armazenar e proteger arquivos e para o acesso ao e-mail corporativo. O login é associado ao e-mail corporativo e somente os colaboradores indicados e autorizados poderão acessar o ambiente através do seu login.

A residência de dados da **HANDSCHUHE** é na região Sul do Brasil (Estado de São Paulo) da área geográfica do Brasil.

A Microsoft não armazenará nem processará os dados da **HANDSCHUHE** fora da área geográfica do Brasil sem nossa autorização prévia. A Microsoft poderá copiar nossos dados entre as regiões em determinada área geográfica para redundância de dados e outros fins operacionais. Por exemplo, o armazenamento com redundância geográfica replica dados de blob, de arquivo, de fila e de tabela entre duas regiões da mesma área geográfica, de modo a fornecer durabilidade aprimorada de dados no caso de um desastre de grandes proporções em um datacenter.

b.1. Medidas de Proteção e Segurança

- a. Protocolo TLS e o protocolo IPsec.
- b. Cada arquivo é criptografado em repouso com uma chave única AES256. Estas chaves únicas são criptografadas com um conjunto de chaves mestres armazenadas no Azure Key Vault.
- c. Os dados que transitam são protegidos com criptografia TLS. Não são permitidas conexões autenticadas através de HTTP, mas em vez disso é redirecionado para HTTPS.
- d. Rápida notificação se confirmada uma violação de dados.
- e. O mecanismo antimalware do Windows Defender verifica documentos no momento do download para obter conteúdo correspondente a uma assinatura AV (atualizada de hora em hora).

- f. Monitoramento de atividades suspeitas para impedir o acesso não autorizado com bloqueio de tentativas suspeitas de entrada.
- g. Detecção e recuperação de Ransomware;
- h. Histórico de versões para todos os tipos de arquivo - No caso de edições indesejadas ou exclusões acidentais, é possível restaurar arquivos excluídos da lixeira ou restaurar uma versão anterior de um arquivo no OneDrive.

b.2. Indicadores de monitoramento que atestam a efetividade da proteção de dados

A Microsoft monitora constantemente seus centros de dados começando pelo inventário. Um agente de inventário executa uma captura de estado de cada máquina. Após, monitoram e remediam a saúde das máquinas. A implantação contínua garante que cada máquina receba patches, assinaturas antivírus atualizadas e uma configuração válida salva.

A Microsoft 365 "Equipe Vermelha" dentro da Microsoft é composta por especialistas em intrusão que procuram qualquer oportunidade de obter acesso não autorizado. A "Equipe Azul" é composta por engenheiros de defesa que focam na prevenção, detecção e recuperação. Eles constroem tecnologias de detecção de intrusão e resposta.

b.3. Compartilhamento

A **HANDSCHUHE** valoriza e preserva a segurança e confidencialidade dos dados pessoais, cujos acessos estão restritos a colaboradores indicados e devidamente autorizados, observando o mínimo necessário para o cumprimento das solicitações e/ou prestação dos serviços.

Somente colaboradores indicados e autorizados pela **HANDSCHUHE** possuem acesso ao **OneDrive Corporativo** que conta com medidas de proteção em conformidade aos padrões e procedimentos de segurança e confidencialidade estabelecidos pela legislação brasileira.

b.4. Encarregado / DPO

O canal através do preenchimento do formulário da Web em <https://aka.ms/privacyresponse>. O DPO também pode ser contatado por postagem:

Diretor de proteção dos dados da Microsoft da UE
One Microsoft Place
Sul County Business Park
Leopardstown

Dublin 18
D18 P521
Irlanda
Telefone: + 353 (1) 706-3117

c. Site Corporativo

O **site** da **HANDSCHUHE** não coleta e não armazena dados de fornecedores e clientes e nem utiliza cookies. Seu objetivo é exclusivamente corporativo e de caráter informativo sobre a história, missão e valores da empresa, apresentando o portfólio dos produtos fabricados e disponíveis para venda, Certificados de Aprovação emitidos pelo Ministério do Trabalho, Ficha técnica dos Produtos , Política de Troca e Devoluções, canal de contato, dentre outros.

O **site** *www.handschuhe.com.br* está hospedado na plataforma HostGator cujos servidores estão protegidos de ataques DOS e DDOS.

A **HANDSCHUHE** utiliza, adicionalmente, o AVAST e McAfee como sistema anti-vírus.

d. Mídias Digitais

As **mídias digitais** utilizadas pela **HANDSCHUHE** não dispõem de canais de coleta de cadastro.

4. Atualização

Pode ser que as informações aqui disponibilizadas sejam atualizadas ou alteradas, para refletir a realidade das nossas operações. Por isso, aconselhamos que você consulte esse Aviso periodicamente.

Última Atualização: 23 de outubro de 2023