Política de Privacidade e Proteção de Dados – OmniSec

Essa é uma versão reduzida e pública da nossa **Política de Privacidade**, cobrindo apenas os principais macro assuntos de forma mais sucinta. Caso tenha necessidade de acessar a versão completa, pedimos que entre em contato pelos canais oficiais deste site institucional que enviaremos o documento completo.

1. Objetivo

A **OmniSec** valoriza a privacidade e a proteção de dados pessoais como princípios fundamentais de sua atuação. Esta política, em versão reduzida, tem como objetivo apresentar diretrizes para garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações, em conformidade com a **Lei Geral de Proteção de Dados (LGPD)** e outras normas internacionais de privacidade, retenção e proteção.

2. Abrangência

Aplica-se a todos os colaboradores, parceiros, fornecedores e afiliadas que operem, processem dados pessoais ou façam uso das infraestruturas e serviços da **OmniSec**.

3. Diretrizes de Privacidade e Proteção de Dados

3.1 Princípios Garantidores

Adotamos os princípios de privacidade previstos na **LGPD** com base nos **10 princípios garantidores**, permitindo que o tratamento de dados pessoais seja realizado em linhas as leis e normativos existentes. Como titular de dados, são seus direitos e podem ser requeridas informações sobre como empregamos:

1) **Finalidade** – o uso real para propósitos legítimos, específicos e informados ao titular;
2) **Adequação** – a compatibilidade do tratamento com as finalidades informadas;
3) **Necessidade** – a limitação do uso e suas operações ao mínimo necessário;
4) **Livre acesso** – a garantia de consulta fácil e gratuita sobre o tratamento dos dados;
5) **Qualidade dos dados** – a exatidão, clareza, completude e atualização dos dados;
6) **Transparência** – informações claras sobre o tratamento e seus relacionamentos;
7) **Segurança** – nossas proteções contra acessos não autorizados e incidentes;
8) **Prevenção** - medidas para evitar danos, mal uso e acessos indevidos;
9) **Não discriminação** - uso dos dados sem fins discriminatórios, ilícitos ou abusivos; e
10) **Responsabilização** - prestação de contas quando acionado e/ou necessário.

3.2 Coleta e Uso de Dados

- Dados pessoais não são coletados por padrão, e se necessário em algum processo posterior, somente de forma proporcional à necessidade, da forma mais reduzida possível.
- Em aplicações internas como CRM e funis de vendas e formulário de contato, apenas parte do nome é registrada (e recomendado que seja feito desta maneira) de forma a não se ter uma identificação completa propositalmente.
- O uso de cookies em nosso site é limitado ao necessário para navegação, sempre com possibilidade de consentimento pelo usuário.

- Não realizamos a coleta de dados pessoais nem sensíveis por padrão em nenhum serviço ou atividade, mas uma vez que venha ser necessário, sempre em linha a base legal adequada.

3.3 Conscientização e Cultura de Privacidade

- Promovemos treinamentos regulares, campanhas de sensibilização e revisões periódicas de nossos processos, reforçando a importância da privacidade e da segurança da informação para todos.

3.4 Inventário, Avaliações e Governança

- Mantemos **inventário de dados pessoais** tratados pela organização, indicando as principais fontes, suas informações e riscos/controles associados.
- Realizamos **Relatórios de Impacto à Proteção de Dados (DPIA)** de forma simplificada quando aplicável aos fluxos e atividades que envolvam dados.
- Contratos, emails e outros documentos que possam ser trocados e transferidos durante nossas atividades/serviços, são armazenados em provedor de nuvem autorizado, certificado e com cláusulas conhecidas sobre acordos de transferência de dados e similares.
- Contratos com fornecedores, terceiros e parceiros incluem cláusulas de proteção de dados específicas e outras complementarem que colaborar com a segurança, compliance e proteção.
- Embora não necessário pelo porte da empresa conforme orientações da ANPD, temos o canal do **Encarregado pelo Tratamento de Dados (DPO)** que pode ser acionado através das informações ao final deste documento.

3.5 Incidentes, Segurança e Resposta

- A OmniSec possui plano de **Resposta a Incidentes**, baseado em metodologias reconhecidas, baseadas no NIST e utilizadas pelos Centros de Respostas (CERTs) globais
- Em caso de incidente, garantimos análise, mitigação, recuperação e comunicação aos titulares e autoridades competentes em tempo legal.
- Os canais de contato em caso de suspeita de violação ou necessidade de comunicação se encontram no final deste documento.

Sendo empresa de segurança da informação, lidamos, treinamos, aplicamos e ajudamos empresas do país na organização de suas estruturas de Segurança e Privacidade, aplicando e prezando pelas melhores práticas em cada setor de atuação.

3.6 Retenção e Armazenamento

O processo de retenção de dados e informações pode variar conforme seu contexto e finalidade, se **mercado regulado**, tipo de atividade, contratos, solicitante do serviço e outras variáveis. Em linha, utilizamos **3 anos** como período padrão interno, reforçando que, dependendo da necessidade externa do cliente, solicitações e cláusulas contratuais, denúncias, tipo de serviço ofertado, este prazo sofrer alterações acordadas entre as partes. Quando está informação inexista, não estiver clara, exista interdependência por parte da **OmniSec e/ou da Contratada**, a referência a ser utilizada interna/externamente, se baseará em recomendações de mercado globalmente aceitas e recomendadas.

Contexto		Retenção	
Regulador	**Setor**	**Online**	**Offline**
ANBIMA	Financeiro/Investimentos	N/A	5 anos
B3	Ordem, custódia, trilhas etc.	N/A	5 anos*
BaCen 4.474	Transações Financeiras	N/A	5 anos
California CCPA	Privacidade	N/A	2 anos
CFM/ANS	Médico, clínico e laboratorial	N/A	20 anos (físico e digital)
Código Civil	Sociedade, Contratos e acordos.	N/A	10 anos
COPPA - Children's Online Privacy	Sociedade – Menores de 13 anos	N/A	Mínimo necessário
CVM	OMS - Order Mgmt System	N/A	5 anos**
EU Data Retention	Telecomunicações & Internet	N/A	6 meses - 2 anos
FISMA - USA	Agências e contratantes federais	N/A	3 anos
GLBA - Gramm-Leach-Blile	Financeiro	N/A	6 anos
HIPAA	Médica/Saúde	N/A	6 anos
LGPD/GDPR	Proteção a Dados Pessoais	N/A	7 anos – 10 anos
Marco Civil Internet	Internet/Provedores	N/A	6 meses - 1 ano***
Master SDP	Meio de Pagamentos	N/A	< a definir >
OpenBanking	Transações Financeiras	N/A	5 anos
PCI-DSS	Cartões de crédito	3 meses	1 ano
Ministério Trabalho	RH (Contratações)	N/A	5 anos****
RSFN/SFN/BC	Transações Financeiras	N/A	5 anos -10 anos*****
Sarbanes Oxley	Financeiro	N/A	7 anos
SEC USA	Corretoras, investimentos e fundos	N/A	6 anos
Susep	Seguros	N/A	5 anos
The Basell II	Financeiro	N/A	7 anos
UK - DRIP	Telecomunicações & Internet	N/A	Até 2 anos******

*Com replicação diária fora do ambiente de produção.

**Ou por prazo superior por determinação expressa do regulador.

***Todos os logs por 6 meses, exceto entidades administradoras de ASs (Autonomous System).

****Após finalização das relações trabalhistas, demais finalidades de acordo com contexto regulador.

*****Contexto de Know Your Customer, Lavagem de Dinheiro e Terrorismo explicitamente é 10 anos.

******Proporcional ao volume de dados gerados pelo provedor (maior volume, menor retenção).

Ainda assim, titulares podem requisitar a **exclusão e exercer seus direitos indicados,** respeitada a base legal aplicável e sua respectiva necessidade de retenção. Importante ressaltar que, a exclusão poderá não ser realizada ou ser factível caso existem impedimentos legais, pendências entre as partes que necessitem desta informação, investigações, outras exigências legais e/ou processos em curso.

4. Responsabilidades e direitos

Todos os colaboradores e terceiros que tenham acesso a dados pessoais estão obrigados a cumprir esta política e os demais normativos internos, mantendo sigilo e promovendo o uso responsável das informações em linhas aos seus direitos e deveres.

Consumindo nossos serviços, atividades e recursos oferecidos por nossas ferramentas e/ou site institucional, o usuário, cliente e/ou visitante, confirma estar de acordo e ciente das recomendações desta política.

5. Sanções

O descumprimento das regras desta política pode resultar em sanções disciplinares, bem como em responsabilização administrativa, civil e criminal, conforme a gravidade da violação.

6. Referências

Esta política, em constante revisão, tem como referência:

- **LGPD – Lei nº 13.709/2018**
- **ISO/IEC 27701**
- **NIST Privacy Framework 1.1**

7. Atualizações e Revisões

Esta política será revisada periodicamente, sempre que houver alterações legais, regulatórias ou operacionais relevantes. O histórico de versões é mantido em nossos documentos e padrões para garantir a rastreabilidade e transparência em sua versão original e completa. Modificações com aplicabilidade imediata podem ocorrer sem prévio aviso e/ou pelo menos uma (1) vez ao ano conforme nossas políticas internas.

8. Contatos

Dúvidas, sugestões, recomendações e solicitações podem ser feitas diretamente por nossos canais oficiais, parcialmente mascarados para evitar coleta de emails por bots, cadastramentos indevidos e ferramentas de rastreamento web (web crawling).

- **dpo** [arroba] omnisecorp [ponto] com
- **security** [arroba] omnisecorp [ponto] com
- **csirt** [arroba] omnisecorp [ponto] com
- **denuncia** [arroba] omnisecorp [ponto] com