



Política de Proteção de Dados

Este documento foi redigido a fim de estabelecer como as políticas de proteção de dados na Shielder são adotadas, levando em consideração as seguintes leis e regulamentos:

- I. **GDPR - Regulation (EU) 2016/679 (General Data Protection Regulation)**, que regulamenta a proteção de informações pessoais para empresas no âmbito da União Européia (e a quem oferece produtos ou serviços à UE); o
- II. **Marco Civil da Internet no Brasil (Marco Civil) - Lei nº 12.965 de 23 de abril de 2014**, que descrevem como organizações devem coletar, manusear e armazenar informações pessoais;
- III. **Lei Geral de Proteção de Dados no Brasil (LGPD) - Lei nº 13.709 de 14 de agosto de 2018**, que dispõe sobre proteção de dados e faz alterações no Marco Civil da Internet no Brasil; e o
- IV. **Can-spam - Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (Pub.L. 108-187)**, que regulamenta aspectos fundamentais do combate ao Spam.

Atendendo ao princípio da transparência, nos dedicamos a fornecer “informações claras e completas sobre uso, armazenamento, tratamento e proteção de seus dados pessoais” (Marco Civil, Cap 1, Art. 7º, item VIII).

Com esta Política de Proteção de Dados, ficam garantidos:

- I. cumprimento de leis, regulamentos e boas práticas de privacidade de dados pessoais;
- II. proteção da equipe, clientes e parceiros;
- III. princípio da transparência de processos;
- IV. orientações para a eventualidade de violação de dados.

Para facilitar a compreensão deste documento, é preciso conhecer os seus atores:

"Data Controller (controlador)" ou **"Usuário"**: pessoa ou empresa que detém controle sobre dados pessoais que serão processados pelos serviços da Shielder (GDPR Art. 4, item 7 / LGPD Art 5º, item VI). O Data Controller torna-se Usuário quando cria uma conta no do Shielder.

"Data Processor (operador)": Shielder é o processador de dados pessoais que trabalha em nome do Data Controller, para realizar um conjunto de operações, automáticas ou não, como coleta de informações de registros, estruturação, armazenamento, adaptação, alteração,



consulta, transmissão, entre outros (GDPR Art. 4, itens 2 e 8 / LGPD Art 5º, item VII). Neste caso, trata-se da Shielder, apenas no escopo de seu propósito de serviço e nada além disso.

"Dados Pessoais": segundo o GDPR, trata-se de qualquer informação relacionada a uma pessoa, que possa identificá-la direta ou indiretamente, como nome, localização, identificador online, entre outros (GDPR Art. 4, item 1 / LGPD Art. 5º, item I)

"Dados Pessoais Sensíveis": A Lei Geral de Proteção de Dados indica esta informação como dados “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 vinculados a uma pessoa natural” (LGPD Art. 5º, item II).

"Dado anonimizado": dados relativos à alguma pessoa que não a identifiquem diretamente e que, portanto, não estão sujeitas à lei.

Responsabilidades

Em termos do escopo de nossos serviços e sua adequação às regulamentações de proteção e privacidade de dados, o Diretor de Tecnologia da Informação da Shielder se responsabiliza pela implementação integral desta política e atua como DPO (Data Protection Officer) para a Shielder, atendendo aos artigos 37, 38 e 39 do GDPR.

Mensagens podem ser enviadas ao DPO através do e-mail contato@shielder.com.br.

Todos os sócios, diretores e funcionários da Shielder são obrigados a assinar um Termo de Sigilo e Confidencialidade, englobando todos os dados e informações da empresa, seus parceiros, colaboradores, prospects, clientes e bancos de dados.

O acesso a bancos de dados e servidores do Data Center é proibido aos funcionários da Shielder, sendo realizado somente pelo DPO/CIO.

As equipes de atendimento e vendas são treinadas para compreender a importância da proteção de dados. Também são orientados a sempre consultar o DPO em caso de quaisquer dúvidas quanto à confidencialidade de alguma informação

Processamento e Armazenamento de Dados

Todas as conexões ao painel de controle da Shielder, assim como o seu website e demais subdomínios, estão protegidos por certificações SSL criptografadas da CloudFlare, Autoridade Certificadora em conformidade com a AICPA/CIA WebTrust.

Todas as informações armazenadas na Shielder estão protegidas em bancos de dados de servidores armazenados em Data Center da NACIONAL com certificação ISO/IEC 27001:2013, das atestações internacionais SOC 1 type II (SSAE 16 e ISAE 3401) e SOC 2 type II e ainda a certificação PCI DSS Nível 1.



Estas medidas visam proteger Usuários e Dados pessoais, atendendo às disposições da Lei Geral de Proteção de Dados (LGPD), Capítulo VII (Da segurança e das boas práticas), Seção I (Da Segurança de do Sigilo de Dados), Artigo 46.

Os serviços de Data Center são realizados nos seguintes países: Canadá, França e Alemanha. Os Usuários da Shielder dão ciência desta informação e consentimento para o processamento de dados ao aceitar os Termos de Uso.

A Shielder armazena as informações do Usuário, deletando estes arquivos automaticamente após fim do contrato. Se desejar, o Usuário poderá deletar suas próprias informações antes desse período, a qualquer momento (“Right to erasure (‘right to be forgotten’)”, GDPR Art. 17).

Nenhuma informação é armazenada em meios físicos transportáveis e pessoais, como CDs, DVDs, Pendrives, Notebooks ou similares.

Para realizar seus serviços de validação controle de acesso de moradores e visitantes, a Shielder precisa que seus Usuários compartilhem informações de documento, nome e foto em seu sistema. Sem elas, torna-se impossível realizar o processamento destas informações a fim de entregar seus resultados.

O Usuário, utilizando os serviços da Shielder, declara possuir consentimento para o armazenamento de dados pessoais e afirma que o tratamento das informações visa cumprir execução de contrato, procedimentos preliminares relacionados a contrato, ou quando necessário para atender aos seus interesses legítimos e/ou para proteção do crédito (LGPD, Capítulo II, Seção I, Art ° 7, Itens I, V IX e X), prevalecendo direitos e liberdades fundamentais do titular dos dados pessoais.

A Shielder necessita apenas de dados de identificação para realizar o escopo de seu serviço de controle de acesso. Embora o Usuário possa realizar o carregamento de suas informações contendo outros campos de informações pessoais e/ou sensíveis, eles não são necessários para a realização do processamento. A Shielder não provê qualquer tipo de informação que não seja relacionada ao controle de acesso, e não oferece qualquer serviço que adicione dados pessoais que identifiquem pessoalmente estes endereços, como nomes, endereços, redes sociais, entre outros.

Informações anonimizadas, ou seja, aquelas não sujeitas à lei, pois não identificam ou não são passíveis de identificação de uma pessoa natural (em outras palavras, que não violam a privacidade da pessoa natural e não ferem os regulamentos do GDPR e LGPD), podem ser oferecidas pela Shielder.

Qualquer utilização da Shielder através de uma integração via API (a partir de outras plataformas) exige permissão expressa do Usuário a fim de realizar o processo de validação e verificação de e-mails.

A instalação do app do Shielder para validação e verificação de e-mails em tempo real é de responsabilidade exclusiva do Usuário. O app é um recurso consultivo, informando apenas o status o controle de acesso consultado diretamente para o Usuário, não armazenando dados



diferentes digitados no formulário do cliente no banco da Shielder (como campo de nome, empresa, entre outros).

Em caso de vazamento de dados

A Shielder se prontifica a informar ao Usuário qualquer vazamento de dados em até 72 horas da ocorrência, se viável. (GDPR Art. 33, item 1 / (LGPD, Capítulo VII, Seção I, Art ° 48)

Compartilhamento de Dados

A Shielder não vende, aluga ou compartilha endereços de e-mails e outros dados que tenham sido fornecidos à Shielder em razão de seus serviços. (Leia nosso Termo de Sigilo e Confidencialidade)

A Shielder não realizará qualquer tipo de contato com os endereços de e-mails fornecidos à Shielder por seus Usuários a fim de promover seus produtos.

Em certas circunstâncias, por razão de força da lei e exigência das autoridades, e somente nestes casos, a Shielder poderá realizar a quebra de sigilo de dados, amparada pela lei. A Shielder tomará a precaução de, nestes casos, ter total certeza de que a solicitação foi realizada por meios legais.

Para contato com a Shielder a respeito de Proteção de Dados:

contato@shielder.com.br