LGPD - Lei Geral de Proteção de Dados

Área de Aplicação: Segurança
Responsável: Bruno Brustolin
Data: 16/02/2024

1. Introdução

Este documento foi criado com o intuito de balizar as questões dos termos da LGPD em relação a Winov detalhando as responsabilidades e papéis de cada parte entre “contratante” e “contratada”.

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais como é o caso de infraestruturas de Clouds Públicas, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2. Objetivo

Este documento visa descrever as responsabilidades referentes à aplicação da LGPD versus a Winov, na condição de provedor de serviços de infraestrutura em Cloud.

3. Escopo

Essa política se aplica a todos os colaboradores da WINOV, bem como fornecedores e outras pessoas que utilizam os recursos da WINOV

4. Papéis e Responsabilidades

A segurança e a conformidade com a LGPD constituem em uma responsabilidade compartilhada entre a Winov e o cliente. A Winov se faz responsável em gerenciar e controlar a camada de virtualização e a segurança física em que nossos equipamentos operam.

O cliente segue assumindo a responsabilidade e a gestão do sistema operacional convidado, dados e softwares contidos no mesmo. É de gestão do cliente a aplicação de patches de segurança e atualizações nos sistemas operacionais convidados, não sendo responsabilidade da Winov o acompanhamento por versões de sistemas operacionais vulneráveis e desatualizados, cada cliente deve examinar com cuidado os serviços a serem hospedados na Winov, visando sempre a integridade, disponibilidade e segurança de seus sistemas.

Responsabilidade da Winov: A Winov é responsável pela segurança da infraestrutura, composta por Hardware, redes e instalações que executam os serviços da nuvem Winov.

Responsabilidade do cliente: A responsabilidade do cliente é baseada nos serviços que ele possui junto a Winov. Por exemplo, os clientes que possuem uma instância W2C (Winov Cloud Compute) são responsáveis pelo gerenciamento do sistema operacional, bem como aplicação de patches de segurança e atualizações dos mesmos, estendendo ainda às configurações de firewall solicitadas (Bloqueios de portas, GeoIP, WAF, IPS, etc.). Os clientes são responsáveis por gerenciar seus próprios dados com opções de criptografia, classificação dos dados e permissões de acesso.

A Winov não possui acesso às instâncias dos clientes, todo suporte é monitorado e assistido, com dever do cliente conceder as permissões de acesso ao ambiente.

Nos comprometemos em não divulgar dados de clientes, a menos que sejamos obrigados a cumprir uma lei ou ordem judicial. Caso algum órgão governamental envie uma demanda requerendo dados de nossos clientes, tentaremos redirecionar a conversa para que o cliente trate diretamente com o órgão governamental que está requerendo os dados. Se formos obrigados a divulgar o conteúdo, enviaremos ao cliente, com antecedência, um aviso sobre a demanda, permitindo assim que o cliente busque meios legais para a proteção de seus dados.

5. Informações Pessoais que coletamos

Coletamos informações pessoais que são fornecidas para a criação ou administração de contas de acessos para os sistemas da Winov. As informações de conta, por exemplo, incluem nomes, nomes de usuários, números de telefones, endereços de e-mail e informações para cobrança.

6. Como utilizamos essas informações

Utilizamos as informações coletadas para monitorar o ambiente e prestar suporte. Temos a obrigação de coletar dados pessoais ou reter suas informações para fins de cobrança e verificação de identidade.

Utilizamos suas informações para nos comunicarmos com você, seja por meios eletrônicos, ferramentas de suporte e comunicação.

7. Termo de eliminação ou alteração

Observada a lei, é direito do cliente a solicitação de correção de seus dados cadastrais, desde que não interfiram nas obrigações legais contratuais entre cliente e Winov.

Solicitar a exclusão de informações pessoais que não estejam mais em uso, processadas com base em um consentimento retirado ou em desconformidade com a lei atual.

Opor-se ao processamento de dados pessoais

Solicitar informações sobre o uso de suas informações e como elas são processadas

Solicitar informações sobre a possibilidade de recusar o processamento de dados pessoais e as consequências dessa atitude.

8. Encarregado de dados

O Encarregado pelo Tratamento de Dados Pessoais na Winov é responsável por assegurar que nossa instituição esteja em conformidade com a Lei nº 13.709, de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), garantindo que o tratamento de dados seja sempre realizado de forma adequada. A necessidade de indicação de Encarregado pelo Tratamento de Dados Pessoais está prevista no art. 41 da LGPD.

Desse modo, quaisquer dúvidas a respeito do tratamento de dados pessoais realizado pela Winov devem ser encaminhadas para o encarregado, por meio do e-mail seguranca@winov.com.br

Encarregado:
Adriel Pereira
CEO

Endereço:
Winov
Rua Buenos Aires, 73
CEP 80250-070| Curitiba | PR

Telefone
(41) 3122-9619

E-mail

seguranca@winov.com.br

Previsão legal
LGPD, art. 5º, VIII

Atribuições
Artigo 41, §2º, da LGPD

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

9. Resposta a incidentes

Uma resposta a um incidente deve ser decisiva e executada rapidamente, ao mesmo tempo, preservando todas as evidências forenses que possam ajudar na identificação do ocorrido ou prevenção futura.

Após a identificação do incidente, o mesmo deve ser contido e isolado, a fim de evitar que outros sistemas ou clientes sejam afetados.

É de extrema importância que todo o processo permita a documentação e o registro do ocorrido, evitando a perda de provas ou dados forenses que possam auxiliar na identificação futura.

O processo de recuperação e continuidade do negócio deve ser iniciado após a contenção do incidente, removendo as ameaças e restaurando sistemas e serviços afetados.

Deve-se realizar verificações, testes e validações antes do retorno do ambiente à produção, garantindo que não há mais ameaças presentes no ambiente.

Todo incidente deve ser documentado, contendo explicações do ocorrido, sistemas afetados, ações tomadas para remediação e processo de recuperação.

No caso do incidente contar vazamento de dados, deverá ser avaliado e fazer as comunicações obrigatórias por lei, se houverem.