UGPBRASIL
Assessoria em Projetos, Licitações e Contratos

MANUAL DE BOAS PRÁTICAS DE PROTEÇÃO DE DADOS PESSOAIS

INTRODUÇÃO

A **UGP BRASIL** é uma Empresa que presta serviços de consultoria e assessoria organizacional e possui seu Programa de Integridade, composto pelo conjunto de mecanismos de prevenção, detecção e combate a irregularidades, ilegalidades e comportamentos profissionais antiéticos, e, para tanto, preza pela aplicação efetiva de seu Código de Ética, Código de Boa Conduta, Políticas, Manuais e procedimentos internos de integridade.

Sua Política de Proteção e Tratamento de Dados Pessoais tem como objetivo proteger os direitos fundamentais de liberdade, intimidade e de privacidade, além de promover o livre desenvolvimento da personalidade, explicitando os fundamentos e princípios para colher, tratar e utilizar dados pessoais que estejam sob sua responsabilidade.

O presente Manual de Boas Práticas de Proteção de Dados Pessoais aprimorou ainda mais as atividades da Empresa relacionadas segurança da informação, governança de dados e gestão de riscos.

CONCEITOS ESSENCIAIS

O dado pessoal é a informação relacionada a pessoa natural, identificada ou identificável, e é sensível se estiver relacionado com a 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 vinculado a uma pessoa natural.

O tratamento de dados é toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utiliza-

ção, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados.

Os agentes de Tratamento de dados pessoais são o Controlador e o Operador.

O Controlador é quem toma as decisões referentes ao tratamento de dados pessoais e o Operador realiza o tratamento de dados pessoais em nome do Controlador.

A Segurança da informação é o conjunto de ações de preservação da confidencialidade, integridade e disponibilidade da informação pessoal dos titulares dos dados.

A governança de dados são as regras que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos.

O gerenciamento de riscos, por sua vez, consiste no processo de identificar, quantificar e gerenciar os riscos relacionados à segurança da informação dentro da Empresa, para minimizar as vulnerabilidades inerentes ao uso de dados pessoais

PRINCÍPIO DA SEGURANÇA

Um dos princípios norteadores da Política de Proteção de Dados da Empresa é o Princípio da Se-

gurança dos Dados, do qual decorre a adoção de medidas de segurança, técnicas e administrativas, para proteção das informações dos titulares contra tentativas de acesso não autorizado e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados ou outras formas de tratamento inadequado ou ilícito.

PRINCÍPIO DA PREVENÇÃO

O Princípio da Prevenção garante a adoção das mais atualizadas medidas para prevenir a ocorrência de danos no tratamento dos dados pessoais colhidos pela Empesa.

GOVERNANÇA DE DADOS

O Controlador de Dados é responsável pela adoção do Programa de Governança em Privacidade de Dados, aplicável a todo o conjunto de dados pessoais que estejam sob seu controle e que tem como objetivo estabelecer relação de confiança com o titular dos dados pessoais.

É responsável também por estabelecer políticas internas, com base em processo de avaliação sistemática de impactos e riscos à privacidade, que asseguram o cumprimento das normas e das boas práticas relativas à proteção de dados pessoais.

Sua atuação transparente estabelece mecanismos de participação do titular e de supervisão internos e externos, de forma que este monitoramento contínuo possibilita atualização constante do Programa.

BOAS PRÁTICAS

São consideradas boas práticas para a UGP Brasil:

- coleta e tratamento de dados em estrita obediência ao Princípio da Finalidade, da Adequação e da Necessidade
- controles de acesso e controles de segurança, inclusive relacionado ao trabalho diário
- o uso de senhas fortes para o acesso e tratamento de dados
- vedação à reutilização de senhas
- utilização de autenticação multi fatores (MFA), como o envio de código de segurança por *short message service* (SMS) ou por e-mail, o uso de aplicativos autenticadores e o uso de tokens de segurança
- acesso a dados compatível com a necessidade e finalidade da permissão do acesso
- procedimentos de autenticação, que identifica quem acessa o sistema ou os dados, e procedimentos de autorização, que determina o que o usuário identificado pode fazer
- manter a confidencialidade dos *logins* e das senhas de acesso das estações de trabalho
- bloquear os computadores quando se afastar das estações de trabalho
- confirmar a identidade do titular de dados e dar a ele o acesso às suas informações e sobre a forma de tratamento de seus dados pela Empresa
- garantir ao titular o acesso e o gerenciamento de seus dados
- tratar e compartilhar dados com transparência e segurança
- atualização de Softwares
- atualização de Hardwares
- utilização de rede interna de computadores

- correto uso do correio eletrônico
- correto uso de dispositivos móveis (celular e laptops)
- uso de serviços de armazenamento de dados em nuvem que sigam as recomendações internacionais sobre segurança da informação
- uso de anti vírus
- restrição de acesso a determinados sites
- identificação de *phishing*
- cuidados com *pop-up* e com acesso à links enviados à Empresa sob diversas formas
- manter constantemente atualizadas as cópias de segurança das informações
- realizar a transferência de dados pessoais para da estação de trabalho para dispositivo de armazenamento externo com pendrive, disco rígido externo caso estritamente necessário e mediante controles adicionais de segurança
- manter documentos físicos que contenham dados pessoais dentro de gavetas e não sobre as mesas
- gerenciar os contratos da Empresa no que toca às obrigações de confidencialidade, sigilo dos dados pessoais, segurança da informação, compartilhamento de dados, bem como quanto à distribuição de funções e responsabilidades das partes.
- treinar os colaboradores sobre como utilizar os controles de segurança de dados
- definir e divulgar as regras de relação entre os agentes

de dados (Controlador e Operador)
- definir e divulgar regras sobre compartilhamento de
- manter uma Política de Segurança da Informação
- manter um Programa de Governança em Privacidade de Dados
- zelar pelos princípios éticos da empresa e pelo cumprimento da Política de Proteção de Dados da Empresa e medidas de segurança da informação
- divulgar o Programa de Integridade da Empresa
- obedecer a legislação sobre proteção de dados e as regras da Agência Nacional de Proteção de Dados – ANPD
- manter procedimentos de Monitoramento, que monitora o tratamento dos dados, procedimentos de Auditoria, que registra o que foi feito pelo usuário
- informar ao Canal de Denúncia sobre a ocorrência de incidentes de segurança e também a existência de vulnerabilidades

POLÍTICA DE COMUNICAÇÃO E TREINAMENTO

A UGP Brasil conta com sua Política de Comunicação para disseminar a cultura ética da Empresa e o conteúdo de seu Programa de Integridade.

A Política de Treinamento, por sua vez, é direcionada especificamente para cada público alvo, utilizando-se de encontros, virtuais ou presenciais, sobre temas éticos relevantes para a capacitação dos que mantém vínculos profissionais com a Empresa.

Os temas que envolvem a segurança da informação e a proteção

de dados pessoais recebem especial atenção tanto com relação à comunicação da Empresa a respeito da importância da conscientização sobre as responsabilidades de cada um envolvido nos processos de tratamento de dados, quanto aos treinamentos para a realização das operações com a máxima segurança.

GERENCIAMENTO DE RISCOS

A Empresa adotará as medidas adequadas para reverter ou mitigar os dados envolvidos em caso de ocorrência de incidente, além de seguir seus planos de resposta e remediação de incidentes.

COMUNICAÇÃO DE INCIDENTES

Caso ocorra um incidente de segurança que possa acarretar risco ou dano relevante ao titular dos dados a Empresa comunicará, no menor prazo possível, a autoridade nacional e o próprio titular.

A comunicação conterá a descrição da natureza dos dados pessoais afetados, informações sobre os titulares envolvidos e indicará as medidas técnicas e de segurança utilizadas para a proteção dos dados e os riscos relacionados ao incidente.

CANAL DE DENÚNCIA

Por meio do Canal de Denúncia, amplamente divulgado no site da Empresa, é possível informar a ocorrência de incidentes e também a existência de vulnerabilidades, de forma a contribuir com o aprimoramento contínuo da Política de Proteção de Dados

CONCLUSÃO

A **UGP BRASIL** preza pela aplicação de sua Política de Proteção e Tratamento de Dados Pessoais e

pela adoção das melhores práticas para proteção dos dados pessoais que se encontram sob sua responsabilidade, e mantém seu foco nas medidas preventivas, a fim de proporcionar segurança e transparência para seus clientes e para todos que mantém um relacionamento profissional com a Empresa.

POLÍTICA DE PRIVACIDADE

O site da **UGP Brasil**, assim como suas mídias sociais, busca oferecer uma navegação com conteúdos de qualidade mantendo a segurança e integridade dos dados coletados dos seus usuários, em conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD).

Como não exigimos cadastros para o acesso aos dados de usuários, a UGP Brasil não coleta informações de natureza pessoal (art. 5º, inciso I, da LGPD), como nome, RG e CPF, salvo se consentido pelo usuário em casos de solicitação direta para recebimento de informativos ou conteúdos técnicos.

Acesse a política completa aqui.