Relatório de Impacto à Proteção de Dados Pessoais

julho de 2021

Versão: 1.0

14 de julho de 2021.

DPO: Diego Schiavenin

Sumário

Identificação dos agentes de tratamento e do encarregado

Controlador: Baah Serviços de Informática e Marketing LTDA-ME

Operador: Diego Schiavenin – Coordenador de Governança da Informação.

E-mail do Operador: diego@baah.com.br

Necessidade de elaborar o Relatório

Temos como objetivo assegurar que as atividades da empresa sejam conduzidas em conformidade com as normas aplicáveis da Lei Geral de Proteção de Dados Pessoais (LGPD) e a Autoridade de Proteção de Dados Pessoais (ANPD) pode determinar a empresa que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis. Surgiu, assim, a necessidade de se confeccionar este documento.

A empresa realiza o tratamento de dados pessoais que se relacionam a pessoa natural identificada ou identificável e a empresas (art. 5º, I, LGPD). Existem também os dados pessoais sensíveis, que dizem respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos, quando vinculados a uma pessoa natural (art. 5º, II, LGPD).

Considerando os fundamentos da proteção de dados pessoais (art. 2º e incisos, LGPD), a boa-fé e os demais princípios a serem observados nas atividades de tratamento de dados pessoais (art. 6º e incisos, LGPD), a empresa dispõe de diferentes sistemas de controles internos, que variam de acordo com a natureza do dado pessoal, para mitigar eventuais riscos de falha na proteção de dados pessoais.

Entretanto, apesar do elevado grau de maturidade da gestão de riscos da empresa, não se pode garantir a eliminação total dos riscos que, em caso de materialização, causariam impacto à privacidade dos dados pessoais existentes.

Descrição do tratamento

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019)

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Relatório de Impacto à Proteção de Dados Pessoais Nesta seção são descritos os processos de tratamento de dados pessoais, digitais ou físicos, que podem gerar riscos às liberdades civis e aos direitos fundamentais, envolvendo a especificação de natureza, escopo, contexto e finalidade do tratamento.

Dados digitais

Natureza do tratamento

São adotadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

O acesso às bases de dados é controlado por grupos de acesso limitado a determinados perfis de usuários. Há contínua busca por segurança da informação ao se fazer uso de softwares da empresa para cumprirem a Lei Geral de Proteção de Dados (LGPD).

Como medidas administrativas adotadas, citam-se: assinatura de acordos de responsabilidade para acesso a sistemas, por requisição formal ou por e-mail.

Tratamento dos dados

Existem diversas formas de tratamento dos dados pessoais na empresa, considerando a definição da LGPD:

Coletados/Enviados

Os dados são coletados principalmente por meio de sistemas de informação e por captação de informações por via impressa.

Retidos/Armazenados

Os dados são mantidos das seguintes formas:

- Bancos de dados (utilizando os sistemas gerenciadores de banco de dados MySql);
- Bancos de dados de SAAS (utilizando os sistemas gerenciadores de banco de dados MySql);
- Arquivos (planilhas Excel, apresentações Powerpoint, arquivos do tipo CDR, AI, PSD, JPG, PNG, HTML, PHP, JS e demais que sejam criados com dados de clientes).

Usados:

Os dados são usados em processos de trabalho dentro da empresa

Eliminados:

Os dados podem ser eliminados por meio de ações em sistemas de informação, comandos SQL nos bancos de dados e exclusão de arquivos.

Fonte dos dados

As formas de coleta de dados são:

- Captações de informações externas: são enviados arquivos de dados com informações pessoais por e-mail, site ou sistema ERP;
- Sistemas de informação e site;
- Recebimento de documentos e formulários: eletronicamente ou em papel
- Registro de informações pelos atendimentos: presencial, telefônico e digital;
- Captação de dados através de servidor de e-mail ou de site.

Compartilhamento dos dados

O compartilhamento de dados pessoais ocorre apenas com autorização expressa ou presumida do titular. Também ocorre compartilhamento dos dados protegidos pelo sigilo bancário com órgãos dos Poderes Judiciário, Executivo e Legislativo, e do Ministério Público, e do Banco Central para fins de apuração de irregularidades em que o titular das informações estiver envolvido, bem como com autorização judicial.

Medidas de segurança

As medidas de segurança adotadas pela empresa têm validade para qualquer tipo de informação.

Transferência de Arquivos

Para a transferência de arquivos eletrônicos, para destinatários internos, com informação sensível, devem ser utilizadas:

Pastas compartilhadas localizadas em servidor de arquivos sigilosos;

Mensagem de e-mail com anexos sensíveis, devem ser criptografados, com a senha do arquivo sendo transmitida por outro meio, como telefone.

Para transferência de arquivos para o cliente, com produção, artes, criação ou informações, serão enviados via meio eletrônico para o e-mail do cliente.

Mídias removíveis (pendrive, CD, DVD ou HD externo) podem ser utilizadas para a transferência de arquivos corporativos mediante justificativa, em especial em caso de impossibilidade de uso dos meios tecnológicos descritos acima. Nesse caso, é obrigatória a aplicação de criptografia para proteção da informação sempre que viável tecnologicamente.

Não são considerados meios adequados para a transferência de arquivos eletrônicos: pastas compartilhadas em estações de trabalho (desktops e notebooks), e-mail particular e serviços de terceiros na Internet (ex.: Dropbox e Wetransfer).

São considerados meios adequados para a transferência de arquivos eletrônicos: arquivos enviados diretamente para o cliente ou terceiros via link do OneDrive da empresa, quando não contiverem dados sensíveis.

Servidores de arquivos

Os servidores de arquivos possuem áreas de armazenamento reservadas para cada unidade. Os másters de cada unidade são responsáveis por conceder permissão de acesso às pastas e arquivos, observados os princípios da necessidade de conhecer e do privilégio mínimo.

Para as informações sigilosas, existe um servidor de arquivos sigilosos no OneDrive, esse servidor é administrado diretamente pela Microsoft.

Impressão de documentos

Não deverão ser impressos arquivos eletrônicos corporativos com informação sensível fora das dependências da empresa.

Descarte de informações

O descarte de informações corporativas gravadas em qualquer mídia deverá ser feito de maneira a impedir a sua recuperação.

Monitoramento

A empresa poderá monitorar os acessos, gravações de arquivos e as transferências e impressões de arquivos eletrônicos corporativos caso haja necessidade.

Fluxo de dados

Fluxo de dados de sistemas de comunicação com usuários.

ERP Bling, sistema de gestão da empresa:

Dados necessários para o cadastro do cliente para a emissão da NFS-e através do sistema ERP da empresa.

Bling LGPD: https://www.bling.com.br/politica-seguranca-privacidade

Fluxo de dados da hospedagem de sites e e-mail:

Temos o servidor dentro do datacenter da Kinghost, onde os dados e informações são enviados pelos clientes e tem a finalidade de abrir o site e trabalhar com os e-mails.

Kinghos (LGPD): https://king.host/contratos-e-politicas

Fluxo de dados do sistema Planest:

O Planest é um software de planejamento estratégico online para ajudar consultores, pequenas e médias empresas a organizarem seu planejamento.

Planest LGPD: https://www.planest.com.br/politica-de-privacidade-e-termos-de-servico/

Dados físicos

Nenhum dado pessoal é cadastrado ou gerenciado por arquivos físicos, entretanto todas as operações relativas a documentos físicos (localização, retirada, envio, entrega recebimento, arquivamento e eliminação) são feitas dentro da Lei Geral de Proteção de Dados (LGPD).

Escopo do tratamento

O escopo representa a abrangência do tratamento de dados.

Tipos de dados

Recebe dados de pessoas físicas e jurídicas, que contemplam as seguintes informações: Nome completo; número do CPF; data de nascimento; sexo; nome completo da mãe; endereço completo; telefone; CNPJ; inscrição estadual; endereço empresarial; nome de sócios; CPF de sócios; data de inscrição. Esses dados são armazenados em nosso sistema ERP e no documento de contrato.

Frequência de tratamento dos dados

A empresa recebe diariamente atualizações de dados cadastrais de pessoas físicas e jurídicas.

Titulares afetados pelo tratamento de dados

Qualquer pessoa física ou jurídica, cliente ou usuária de serviços financeiros/bancários, pode ser afetada pelo tratamento de dados da empresa.

Contexto do tratamento

Tratamos os dados pessoais de acordo com os propósitos legítimos e específicos de modo compatível com a sua finalidade e objetiva executar as competências legais ou cumprir as atribuições legais.

Métodos de controle pelo cliente

O cliente pode solicitar alterações de dados, inclusão de dados, exclusão de dados através do e-mail: baah@baah.com.br

Tratamento de dados que envolvem crianças, adolescentes ou outro grupo vulnerável

Não coletamos esses tipos de dados, caso seja necessário, será feito junto aos seus pais ou tutores legais.

Finalidade do tratamento

A finalidade do tratamento dos dados pela empresa relaciona-se ao estrito cumprimento de obrigação legal ou regulatória seguindo a Lei Geral de Proteção de Dados (LGPD).

Riscos à Proteção de Dados Pessoais

Destacam-se os riscos à proteção de dados e informações armazenadas pela empresa, em especial aos dados pessoais. Esse tipo de risco pode ser descrito como potencial evento que gera impacto sobre o titular de dados pessoais.

No Anexo I, "Gerenciamento dos Riscos à Proteção de Dados Pessoais", você encontrará mais detalhes da metodologia utilizada.

Categorias de riscos

Acesso não autorizado aos dados	Acesso aos dados pessoais sem o prévio consentimento expresso, inequívoco e informado do titular, salvo exceções legais.
Modificação não autorizada de dados	Modificação de dados pessoais sem a anuência do titular. Viola o princípio da segurança.
Perda de dados	Destruição ou extravio de dados pessoais. Viola os princípios da segurança e da prevenção.
Apropriação de dados	Apropriação ou uso indébito de dados de pessoais. Possibilidades de fraude e vazamento intencional de dados. Viola os princípios da segurança e da prevenção.
Remoção não autorizada de dados	Retirada de dados pessoais sem autorização do titular
Informação insuficiente sobre a finalidade do tratamento de dados	A finalidade declarada para o uso das informações pessoais é insatisfatória, não é específica ou pode suscitar interpretações diversas.
Tratamento sem consentimento do titular dos dados pessoais	Tratamento dos dados pessoais sem a devida prévia permissão expressa, inequívoca e informada do titular, salvo exceções legais.
Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	Compartilhamento dos dados pessoais com outras entidades privadas (fora da administração pública federal) sem a devida permissão do titular.
Retenção prolongada de dados pessoais sem necessidade	Manter os dados pessoais do titular para além do necessário ou do que estava consentido/autorizado. Viola o princípio da necessidade.
Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	Erro ao vincular dados do verdadeiro titular a outro. Viola o princípio da qualidade dos dados.

Falha ou erro de processamento	Processamento dos dados de forma imperfeita ou equivocada. Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc. Viola o princípio da qualidade dos dados.
Reidentificação de dados pseudonimizados	Anonimização insatisfatória de dados pessoais sensíveis possibilitando inferir quem é a pessoa em questão. Viola o direito à anonimização.

Identificação dos riscos

Apresentam-se a seguir exemplos iniciais de riscos identificados e mensurados, de acordo com a metodologia de gerenciamento de riscos operacionais à proteção de dados pessoais:

- vazamento intencional de dados pessoais;
- alteração intencional de dados pessoais;
- permissão indevida para acesso a dados pessoais;
- furto de informações confidenciais;
- divulgação não autorizada de dados pessoais contidos nos documentos e arquivos;
- invasão de sistemas para coleta de dados pessoais;
- invasão do site por hackers.

Medidas de tratamento dos riscos

A aplicação da metodologia de identificação e avaliação dos riscos permite classificá-los de acordo com critérios de priorização. Assim, após a validação do tratamento as ações necessárias para mitigar os riscos são formalizadas.

Conformidade à Lei Geral de Proteção de Dados Pessoais

Com a publicação da LGPD, que dispõe sobre tratamento de dados pessoais por pessoa natural ou jurídica de direito público ou privado, surgiu a necessidade da empresa rever seus processos no intuito de verificar o estágio atual de conformidade à referida norma.

Impacto da não conformidade e urgência para ação

Não foram encontrados impactados ou urgências necessárias de ações.

Acesso não autorizado aos dados

Setor: Sistema de Informação

Peso: 4 Projetos: 0 +

Modificação não autorizada de dados

Setor: Produção, Operações e Técnico

Peso: 1 Projetos: 0 +

Remoção não autorizada de dados

Setor: Produção, Operações e Técnico

Peso: 1 Projetos: 0 +

Informação insuficiente sobre a finalidade do tratamento de dados

Setor: Sistema de Informação

Peso: 1 Projetos: 0 +

Tratamento sem consentimento do titular dos dados pessoais

Setor: Administrativo

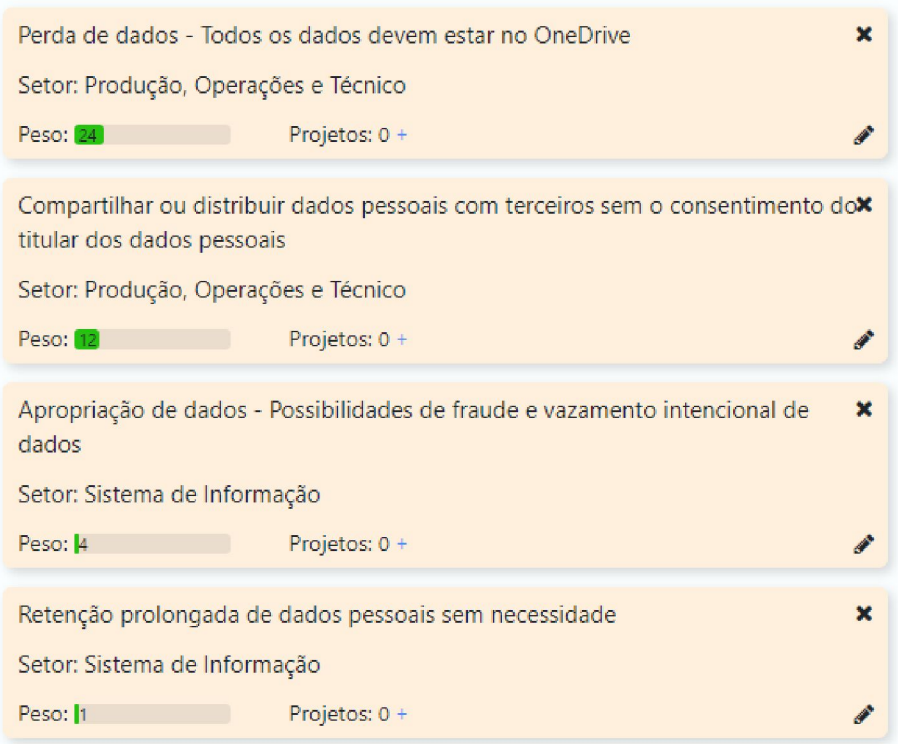
Peso: 1 Projetos: 0 +

Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular

Peso: 1 Projetos: 0 +

Criticidade

Não foram encontradas criticidades com pontuação elevada e já foram corrigidas as operações necessárias.



Possíveis causas de não conformidade

Outro fator importante para auxiliar o planejamento de ações é a identificação de possíveis causas de não conformidade.

Destacamos o sistema de informações e método de compartilhamento de arquivos.

Ações de conformidade

Como resultado das avaliações foi percebido que as ações já foram finalizadas.

Considerações finais

Este documento demonstra, em linhas gerais, como os dados pessoais são coletados, tratados, usados, compartilhados, bem como as medidas adotadas para o tratamento dos riscos que possam afetar as liberdades civis e os direitos fundamentais dos titulares desses dados. Além disso, foram apresentadas informações que denotam o estágio atual de conformidade da empresa à LGPD.

Aprovação

Responsável pela elaboração do Relatório de Impacto:

Diego Schiavenin

Flores da Cunha – RS – 14 de julho de 2021.

Anexo I – Gerenciamento dos Riscos à Proteção de Dados Pessoais

De acordo com a ISO 31.000, o risco pode ser definido como o efeito – positivo ou negativo – das incertezas nos objetivos da organização. A gestão de riscos, por sua vez, é o conjunto de ações coordenadas que buscam garantir que os objetivos sejam perseguidos dentro de limites aceitáveis de risco.

Riscos Corporativos

As informações provenientes da gestão de riscos servem de apoio à tomada de decisão e buscam o fortalecimento da defesa dos processos organizacionais.

No nível estratégico, o uso das informações de risco se apresenta como subsídio para a tomada de decisão, como, por exemplo, de alocação de recursos e de definição de ações estratégicas.

No nível operacional, por outro lado, as informações de risco se oferecem especialmente para implantação de medidas adicionais de mitigação e para análise dos potenciais impactos em caso de materialização de eventos de risco.

No nível tático da organização, por sua vez, esses dados de risco servem como abordagens complementares entre as visões de decisão e de defesa.

Metodologia de Gerenciamento dos Riscos à Proteção de Dados Pessoais

O processo de identificação e avaliação de riscos na metodologia Matriz GUT, os riscos (inclusive de integridade), e também problemas identificados, em geral não afetam o desempenho do processo da mesma forma ou com a mesma intensidade, sendo importante identificar quais devem ser atacados prioritariamente.

Eles diferem, principalmente, quanto ao impacto (gravidade), à probabilidade de ocorrência (ou urgência) e à tendência, caso nenhuma ação seja tomada. Para que esses aspectos de cada risco possam ser considerados, pode-se utilizar a uma variação da ferramenta denominada “Matriz GUT”.

Impacto (Gravidade): refere-se ao impacto do risco ou problema sobre os objetivos ou desempenho do processo; Probabilidade (Urgência): refere-se à velocidade com que as ações necessitam ser tomadas para a solução do problema. Para riscos, deve refletir a probabilidade deste acontecer; (Tendência): refere-se à tendência do risco de ser agravado ou atenuado ao longo do tempo, em caso de inação.

Os ganhos e respostas aos riscos apontados pelos gestores e validados pela Diretoria devem ser considerados na avaliação dos riscos e problemas, devendo ser priorizados aqueles com maiores pontuações na Matriz GUT. Por exemplo, se o ganho esperado do processo é

“agilidade”, deve-se considerar “elevar o tempo de resposta ao operador” um problema grave. Cada quesito (G, U e T) deve receber uma nota de 1 a 5.

A nota total de cada problema/risco será obtida pelo produto dos valores atribuídos aos critérios (GxUxT). Os problemas e riscos dos processos devem ser elencados em ordem decrescente de notas, isto é, dos mais prioritários aos menos relevantes.

Governança das Informações de Riscos Organizacionais

Após a devida identificação e mensuração, os riscos mapeados são apresentados e homologados. Na sequência do processo todos os riscos identificados e as respectivas propostas de tratamento são validadas.