Relatório de Impacto

à Proteção de Dados Pessoais

Agosto de 2021

1 Identificação dos agentes de tratamento e do encarregado

Controlador
ON LINE ENGENHARIA DE SISTEMAS LTDA.

Encarregado
Claudiney da Silva

E-mail Encarregado	Telefone Encarregado
operador.lgpd@onlinesistemas.net	65 3023 2800

2 Necessidade de elaborar o Relatório

De acordo com o art. 38, *caput*, da Lei 13.709, de 14 de agosto de 2018, ou Lei Geral de Proteção de Dados Pessoais (LGPD), a qualquer momento, a Autoridade de Proteção de Dados Pessoais (ANPD) pode determinar à On Line Sistemas (OLS) que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis. Surgiu, assim, a necessidade de se confeccionar este documento.

A On Line Sistemas, diariamente, realiza o tratamento[1] de dados pessoais que se relacionam a pessoas naturais identificadas ou identificáveis (art. 5º, I, LGPD). **Não existem, porém, dados pessoais sensíveis, que dizem respeito à 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 ou biométricos, 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 OLS 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 OLS, não se pode garantir a eliminação total dos riscos que, em caso de materialização, causariam impacto à privacidade dos dados pessoais existentes na instituição.

3 Descrição do tratamento

A Política de Segurança da Informação da On Line Sistemas, visa evitar que os riscos aos quais estão sujeitos os ativos de informação comprometam as atividades da OLS e o cumprimento de sua missão institucional.

Os ativos de informação compreendem os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal e os locais onde se encontram esses meios.

No que se refere especificamente às informações de caráter pessoal, os sistemas de controle interno implantados na OLS estão implantados para o tipo de suporte (digital) e natureza da informação (comum) tratada.

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.

3.1 Dados digitais

3.1.1 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 rede e acesso limitado a determinados perfis de usuários. Há contínua busca por segurança da informação ao se fazer uso de sistemas corporativos na OLS e ao dar cumprimento às disposições contidas na Política de Segurança da Informação, especialmente no que se refere ao acesso à informações.

Como medidas administrativas adotadas, citam-se: (i) assinatura de acordos de responsabilidade para acesso a sistemas (ii) registro dos acessos concedidos; e (iii) destacamento de funcionários dedicados às respostas das demandas dos clientes.

3.1.2 Tratamento dos dados

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

- Coletados/Enviados

Os dados pessoais coletados pela OLS se dividem em três grandes grupos: os dados dos funcionários da empresa; os dados eventualmente fornecidos por usuários dos sistemas quando do atendimento de suporte (nome, email); os dados critptografados constantes dos *backups* on-line dos bancos de dados dos cartórios clientes da OLS.

• Retidos/Armazenados

Os dados dos dois primeiros grupos são mantidos nos servidores da OLS, os do último em servidores da Amazon Web Services.

• Usados

Os dados são usados exclusivamente para: 1) controle de obrigações trabalhistas; 2) atendimento de suporte; 3) cumprimento de contrato de backup.

• Eliminados

Os dados podem ser eliminados por meio de ações em sistemas de informação, comandos SQL nos bancos de dados (no caso de bases de dados departamentais) e exclusão de arquivos.

3.1.3 Fonte dos dados

As formas de coleta de dados na OLS são:

···· captações de informações externas: quando os clientes fornecem seus dados para fins de suporte técnico, sempre de forma eletrônica;

···· recebimento de documentos e formulários: eletronicamente;

3.1.4 Compartilhamento dos dados

O compartilhamento de dados pessoais ocorre conforme determinação e instruções do Controlador e apenas com autorização expressa ou presumida do titular. O único compartilhamento de dados pessoais com terceiros se dá por meio da empresa de contabilidade, para os fins fiscais e trabalhistas.

O recebimento das informações do cliente são feitos por sistema especializado.

3.1.5 Medidas de segurança

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

• Transferência de Arquivos

Para a transferência de arquivos eletrônicos de/para destinatários externos, podem ser utilizados:

···· o sistema fornecido pelo cliente;

···· conexões criptografadas (https) com os websites das centrais de cartórios;

···· anexos de *e-mail*, caso não haja necessidade de garantia de entrega. Se a informação for sensível, o anexo deve estar criptografado, com a senha do arquivo sendo transmitida por outro meio, como telefone.

Mídias removíveis (*pendrive*, CD, DVD ou HD externo) podem ser utilizadas para a transferência de

arquivos corporativos mediante justificativa e com a anuência da chefia imediata, 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, Google Drive e Onedrive).

- Impressão de documentos

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

- Descarte de informações

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

A segurança da informação é constantemente revista e aprimorada com novas medidas de segurança. Uma das abordagens em discussão atualmente é garantir que os dados estejam protegidos durante todo o seu tratamento (desde a coleta até o descarte). Nesse processo, são utilizados diversos sistemas, tecnologias e ferramentas para permitir a criptografia e o controle de acesso de forma integrada.

3.1.6 Fluxo de dados

A seguir, será mostrado o fluxo de dados do sistema de comunicação com usuários externos à OLS:

1) Recebimento das informações (de funcionários ou clientes)	2) repasse das informações legalmente exigidas para a contabilidade	3) devolução aos clientes e funcionários dos documentos legais aplicáveis (ex: notas fiscais)

3.2 Escopo do tratamento

O escopo representa a abrangência do tratamento de dados. As seções seguintes mostram detalhes sobre a extensão do escopo para os dados digitais, os únicos tratados pela OLS.

3.2.1 Tipos de dados

A OLS recebe dados de pessoas físicas, que contemplam as seguintes informações: número do CPF; nome completo; endereço completo, RG e CTPS. Esses dados são armazenados no sistema de RH da empresa.

Os dados pessoais fornecidos durante prestação de serviço de suporte são armazenados no sistema de suporte.

3.3.2 Volume de dados

A base de dados pessoais na OLS está concentrada nos sistemas de RH e suporte, eles recebem cerca de 20 registros/dia.

3.3.3 Retenção dos dados

Os dados são retidos durante toda a duração da contratação pelo cliente ou do funcionário, podendo ser eliminados antes disso, a pedido do mesmo.

3.3.4 Titulares afetados pelo tratamento de dados

Os funcionários da OLS e os usuários do suporte da OLS podem ser afetados pelo tratamento de dados na OLS.

As pessoas físicas constantes no banco de dados dos cartórios clientes do serviço de backup online da OLS não são afetados pelo backup online pois os backups são criptografados dentro dos cartórios pelos mesmos antes do envio para os servidores na nuvem, de forma que a eventual cópia não autorizada de tais backups não implica no vazamento de dados, pois a criptografia só pode ser revertida com o uso da senha de conhecimento exclusivo do cartório.

3.4 Contexto do tratamento

A OLS trata os dados pessoais de acordo com os propósitos legítimos e específicos de modo compatível com a sua finalidade e objetiva executar as determinações do Controlador de Dados.

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

Não são realizados pela OLS.

3.4.2 Avanços em tecnologia e segurança

As seguintes ferramentas de proteção de dados estão implantadas:

Controle de acesso aos sistemas de informação, só permitindo o acesso aos mesmos para as pessoas diretamente envolvidas nos tratamentos de dados;

Utilização de sistemas antivírus atualizados;

Utilização de firewall;

Mecanismo de backup automatizado.

3.5 Finalidade do tratamento

A finalidade do tratamento dos dados pela OLS relaciona-se ao estrito cumprimento de obrigação contratual da OLS para com seus clientes e obrigações legais com os funcionários.

4 Partes interessadas consultadas

Para confecção deste Relatório, todas as áreas da OLS foram consultadas. A partir de maio de 2021, realizaram-se avaliações de conformidade à LGPD, baseadas nas melhores práticas de gerenciamento de conformidade.

5 Necessidade e proporcionalidade

O tratamento de dados é limitado ao mínimo necessário para a realização das finalidades contratadas e determinações legais. Quando necessário, tem abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

O tratamento é feito apenas quando é indispensável e com propósito de cumprimento de obrigação contratual do Controlador de Dados ou cumprimento de obrigação legal.

6 Riscos à Proteção de Dados Pessoais

Dentre os tipos de risco operacional, destacam-se os riscos à proteção de dados e informações armazenadas pela instituição, em especial aos dados pessoais. Esse tipo de risco pode ser descrito como potencial evento que gera impacto sobre o titular de dados pessoais e sobre a OLS.

6.1 Categorias de riscos

Em virtude da introdução da temática de proteção dos dados pessoais, a metodologia de gestão de riscos operacionais da OLS passou por recente alteração com a inclusão de novas taxonomias para identificação e mensuração dos riscos específicos a esse assunto. No levantamento dos riscos operacionais à proteção de dados pessoais, os eventos potenciais são analisados nas categorias a seguir:

1. Acesso não autorizado Acesso aos dados pessoais sem o prévio consentimento expresso, inequívoco e informado do titular, salvo exceções legais.

2. Modificação não autorizada Modificação de dados pessoais sem a anuência do titular. Viola o princípio da segurança.

3. Perda Destruição ou extravio de dados pessoais. Viola os princípios da segurança e da prevenção.

4. Apropriação Apropriação ou uso indébito de dados de pessoais. Possibilidades de fraude e vazamento intencional de dados. Viola os princípios da segurança e da prevenção.

5. Remoção não autorizada Retirada de dados pessoais sem autorização do titular.

6. Coleção excessiva Extração de mais dados do que o necessário para a realização do trabalho, ou do que é previsto em Lei ou foi autorizado pelo usuário. Viola o princípio da necessidade.

Outros

7. Informação insuficiente sobre a finalidade do tratamento

A finalidade declarada para o uso das informações pessoais é insatisfatória, não é específica ou pode suscitar interpretações

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. Reidentificação de dados pseudoanonimizados

Anonimização insatisfatória de dados pessoais sensíveis possibilitando inferir quem é a pessoa em questão. Viola o direito à anonimização.

6.2 Identificação dos riscos

Apresentam-se a seguir exemplos iniciais não exaustivos de riscos potenciais 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;

Uma avaliação completa desse tipo específico de risco está planejada em todos os processos da OLS que envolvem o armazenamento de dados pessoais.

6.3 Medidas de tratamento dos riscos

Após a validação do tratamento pela alta administração, as ações necessárias para mitigar os riscos são formalizadas pelos departamentos em Planos de Mitigação de Riscos (PMR). A elaboração desses PMR, quando os planos forem necessários, cabe ao setor responsável pelo processo na cadeia de valor. Dessa forma, vários planos de mitigação estão em andamento com o objetivo de reduzir a probabilidade de ocorrência e/ou os impactos dos riscos mapeados. A condução desses planos possui suporte organizacional, em termos de recursos, e apoio da alta administração.

7 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 On Line Sistemas (OLS) rever seus processos no intuito de verificar o estágio atual de conformidade à referida norma.

Dessa forma, ao longo deste ano foram realizadas avaliações de conformidade à LGPD e adotadas medidas de mitigação.

7.1 Impacto da não conformidade e urgência para ação

De acordo com os tipos de dados tratados (dados comuns publicamente acessíveis) se conclui que as possíveis não conformidades são de baixo impacto para a OLS, seus clientes e para a privacidade dos titulares de dados.

Assim, os controles implantados são considerados adequados para garantir o razoável cumprimento da LGPD.

7.2 Criticidade

A partir da composição do impacto da não conformidade e da urgência para ação, encontra-se o grau de criticidade da obrigação avaliada. Não há avaliações consideradas críticas.

7.3 Possíveis causas de não conformidade

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

A Tabela abaixo traz detalhes das possíveis causas de não conformidades indicadas pelas áreas nas avaliações críticas.

Tecnologia da informação	deve ser implantada a verificação periódica da segurança digital, em especial a realização de penetration test na rede da empresa

7.4 Ações de conformidade

Como resultado das avaliações realizadas, a OLS realizou atividades de implementação e testagem de políticas de backup e recuperação de desastres, bem como vem implementando avaliações de segurança digital.

8 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 OLS à LGPD.

Este Relatório será revisto e atualizado anualmente ou sempre que a Instituição implementar qualquer tipo de mudança que afete o tratamento dos dados pessoais. a OLS preocupa-se em avaliar continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações nos cenários tecnológico, normativo, político e institucional.

9 Aprovação

Responsável pela elaboração do Relatório de Impacto	**Encarregado**
JOSÉ PINTEIRO DA COSTA BISNETO OAB/PE 23.391	Claudiney da Silva