PROGRAMA DE GOVERNANÇA E COMPLIANCE DE PRIVACIDADE E PROTEÇÃO DE DADOS

Conteúdo

1 - Contexto

Entende-se por contexto sistêmico o tratamento dos dados pessoais pela organização tendo como prisma os sistemas de tecnologia da informação utilizados para gerenciamento das diversas categorias de dados (pessoais ou não), seus fluxos e processos dentro da organização para, então, identificar o ciclo de vida dos dados e seus respectivos gaps que possibilitarão as adequações necessárias para o programa de conformidade. O contexto sistêmico levará em consideração ainda a alocação dos dados em processamento para posterior aplicação dos preceitos inerentes à Segurança da Informação e procedimentos de adequação/mitigação e/ou aceitação de riscos à qual estejam os referidos bancos de dados expostos. Por sistema se compreenderá os softwares que possuam interface direta com os usuários bem como aqueles que não possuam interface direta com os usuários ou sirvam de base de dados possibilitando buscas integradas entre os respectivos softwares.

software: Trata-se de serviço digital fornecido como aplicativo desktop interno sendo também gerido através da Plataforma SimplificaCI, possui as mesmas funcionalidades e benefícios que o APP Mobile descrito anteriormente, mas com a diferença de ser utilizado em computadores corporativos disponíveis com sistemas operacionais Windows, sendo necessário a instalação e ativação dos empregados com o mesmo usuário da rede interna.

Quais são as responsabilidades inerentes ao tratamento de dados pessoais?

Visto que trata-se o presente Privacy Impact Assessment de relatório documental em sua versão de no 01 produzido pela SIMPLIFICACI, imperioso afirmar que trata-se o presente PIA de documento firmado nos moldes do artigo 37 da Lei 13.709/2018 ensejando à mesma o programa de conformidade exigido nos moldes da legislação em comento e a adoção de medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito nos moldes do artigo 46 da Lei 13.709/2018.

A SIMPLIFICACI enquanto OPERADORA primará, nos moldes do artigo 50 da Lei 13.709/2018 no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, pela formulação de regras de boas práticas e de governança 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 e outros aspectos relacionados ao tratamento de dados pessoais.

RESPONSÁVEL PELO TRATAMENTO	ENCARREGADO DA PROTEÇÃO DE DADOS
SIMPLIFICACI GESTAO DA COMUNICACAO INTERNA LTDA R JOAQUIM RODRIGUES, 1085, SALA 1, CEP 15.092-676, DISTRITO PARQUE TECNOLOGICO VANDA KARINA SIMEI BOLCONE, SÃO JOSÉ DO RIO PRETO, SP - CNPJ/MF sob n° 22.654.712/0001-67	Edelcio Molina E-mail: compliance@simplificaci.com Telefone: (17) 98125-7592

1.1 - Agentes de Tratamento

(Contexto)

SIMPLIFICACI: Operadora (Art. 5, IX, LGPD)
CLIENTES SIMPLIFICACI: Controladores (Art. 5, IX, LGPD)
TITULARES DE DADOS: CLIENTES SIMPLIFICACI e colaboradores dos CLIENTES SIMPLIFICACI

1.2 - Categoria de Dados

(Contexto)

- Dados do Empregado (USUÁRIO DO APLICATIVO)
- Dados de Usuário da Rede

1.3 - Visão Geral

(Contexto)

Qual é a finalidade de tratamento considerada no âmbito da análise?

O presente PIA desenvolvido pela **SIMPLIFICACI** enquanto desenvolvedora do software **Simplifica Desk**.

Quais são as responsabilidades inerentes ao tratamento de dados pessoais?

As responsabilidades são atribuídas na forma do artigo 5o da Lei 13.709/2018 levando em consideração o agente de tratamento. Para o presente PIA é considerado como agente de tratamento a SIMPLIFICACI tendo o papel de operadora enquanto provedora do software e seu cliente no papel de controlador conforme abaixo:

DESCRIÇÃO DO AGENTE DE TRATAMENTO	ENQUADRAMENTO DO AGENTE DE TRATAMENTO
CLIENTE SIMPLIFICACI	CONTROLADOR
USUÁRIOS DO APP NO CLIENTE SIMPLIFICACI E/OU COLABORADORES CLIENTES SIMPLIFICA	TITULARES DE DADOS
COMPARTILHAMENTO COM TERCEIROS PELA SIMPLIFICACI	SERVIÇOS E FORNECEDORES DE ARMAZENAMENTO: MICROSOFT AZURE AMAZON AWS CLOUD CONVERT HUBSPOT GITHUB ZENDESK WHATSAPP MESSAGEBIRD
BANCO DE DADOS	BASE SIMPLIFICACI (Cloud)
BACKUP DE BANCO DE DADOS NA OPERADORA	NÃO. SOMENTE NO MICROSOFT AZURE SQL.
COMPARTILHAMENTO	COM OUTROS SOFTWARES PRÓPRIOS

SUBCONTRATANTES/OPERADORES CONTROLADORES CONJUNTOS	CONTRATO DE PROCESSAMENTO	FINALIDADE DO PROCESSAMENTO

MICROSOFT AZURE	https://azure.microsoft.com/pt-br/support/legal/	Serviços de infra, segurança, processamento e armazenamento de objetos de curta e longa duração
AMAZON AWS	https://aws.amazon.com/pt/compliance/data-privacy-faq/	Serviços de infra, segurança, processamento e armazenamento de objetos de curta e longa duração
CLOUD CONVERT	https://cloudconvert.com/privacy	Serviços de processamento de curta duração para imagens e vídeos
HUBSPOT	https://legal.hubspot.com/br/privacy-policy	Serviços de gestão de contatos de clientes para fins comerciais de longa duração, não vinculada a base de dados principal
GITHUB	https://docs.github.com/pt/github/site-policy/github-privacy-statement	Serviços de gestão de chamados para níveis de suporte de longa duração, não vinculada a base de dados principal
ZENDESK	https://www.zendesk.com/company/privacy-and-data-protection/	Serviços de gestão de chamados e troca de mensagens para níveis de suporte de longa duração, não vinculado a base de dados principal
WHATSAPP	https://www.whatsapp.com/privacy/?lang=pt_br	Serviços de gestão de contatos e troca de mensagens para níveis de suporte de curta duração, não vinculado a base de dados principal

MESSAGEBIRD	https://www.messagebird.com/legal/privacy/	Serviços de gestão de contatos e troca de mensagens para níveis de suporte de curta duração, não vinculado a base de dados principal

1.4 - Normas Aplicáveis à Finalidade de Tratamento

(Contexto)

A **SIMPLIFICACI** observará bem como adotará às normas consubstanciadas na Lei 13.709/18, Lei 12.965/14, Lei 8.078/90, Lei 10.406/02, Lei 8.069/90, Lei 9.608/98, além de normas consubstanciadas em Políticas Nacionais de Proteção de Dados Pessoais à que esteja(m) vinculada(s) as empresas **controladoras** e que venham à ser chanceladas pela ANPD (Autoridade Nacional de Proteção de Dados) em formação no momento da escrita deste PIA v.2.0.

2 - Inventário de Dados, Data Mapping e Ativos

2.1 - Dados e Processos

(Inventário de Dados, Data Mapping e Ativos)

- **Quais são os dados tratados?**
  - Dados do Empregado (USUÁRIO DO APLICATIVO)
  - Nome
  - Foto
  - CPF ou Email Corporativo ou Matricula
  - Celular
- **Dados de Usuário da Rede [1]:**
  - Nome do Usuário
  - Nome do Domínio
  - IP Local
  - IP de Domínio

> *[1] A depender da configuração de rede utilizada pelo CONTROLADOR em sua ambientação possa ser que um nome de usuário vinculado à um nome de rede dentro do critério expansionista na forma do artigo 5o, I, da LGPD possa revelar o titular de dados pessoais.*

2.2 - Data Mapping por Categoria de Dados Pessoais

(Inventário de Dados, Data Mapping e Ativos)

CATEGORIA DE DADOS:

> *DADOS DE EMPREGADO (USUÁRIO DO APLICATIVO)*

Fonte de dados pessoais	Tipo de dado pessoal
Contrato de Prestação de Serviços entre SIMPLIFICACI (Operadora e CLIENTE SIMPLIFICACI (Controlador)	Todos *(Vide item 2.1)*
Dados Sensiveis	- - -
Dados de menores	- - -

Base legal para processamento	Finalidade do processamento	Tipo do dado pessoal
Execução de Contrato (Art. 7o, V,LGPD)	Cumprimento de Contrato; Adimplemento Financeiro (outorga da licença de uso do Software) e Integridade do Software	Todos

TEMPO DE RETENÇÃO

Tipo de dado pessoal	Anos	Meses	Semanas	Hora de Início
Todos *(Vide item 2.1)*	0	3	0	Após a rescisão contratual

MEDIDAS DE MITIGAÇÃO DE RISCOS EXISTENTES

- DESCARTE DE DADOS DESNECESSÁRIOS OU NÃO MAIS VINCULADOS ENTRE CONTROLADORA E OPERADORA POR RESCISÃO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS;
- SEGREGAÇÃO/SEPARAÇÃO DO BANCO DE DADOS ONDE ESTÃO ARMAZENADAS AS FOTOGRAFIAS DOS TITULARES DE DADOS PESSOAIS;
- MASCARAMENTO DE DADOS PESSOAIS DOS TITULARES EM TODOS OS ACESSOS INTERNOS PELO NOSSO TIME. SALVO SITUAÇÔES QUANDO AUTORIZADAS PARA DESEMPENHAR SUPORTE E MANUTENÇÃO DOS NOSSOS SERVIÇOS
- CRIPTOGRAFIA SSL/PKI (NO TRÁFEGO DAS COMUNICAÇÕES VIA HTTPS) RELATÓRIO DE ACESSO;
- CRIPTOGRAFIA DO BANCO DE DADOS EM REPOUSO
- CONTROLE DE EXPIRAÇÃO DE SESSÃO A PLATAFORMA SIMPLIFICACI A CADA 60 MINUTOS DE INATIVIDADE
- DISPONIBILIDADE DE CONTROLE DE NÍVEIS DE ACESSO AS FUNÇÕES ADMINISTRATIVAS NA PLATAFORMA SIMPLIFICACI
- ACESSO RESTRITO AO CÓDIGO FONTE DOS PRODUTOS DE ACORDO COM O PROFISSIONAL (DESENVOLVEDOR) ALOCADO
- CÓDIGO FONTE COM INFORMAÇÕES E TOKENS DE ACESSO CRIPTOGRAFADOS E ARMAZENADOS SOMENTE VIA ACESSO EM DUAS ETAPAS
- APLICATIVOS WINDOWS CERTIFICADOS POR MEIO DE AUTENTICAÇÃO (CODE SIGNING) ATRAVÉS DE CHAVE DE AUTENTICAÇÃO PRIVADA VIA TOKEN FÍSICO
- DISPONIBILIDADE DE RELATÓRIO DE STATUS DE FUNCIONAMENTO DOS SERVIÇOS DE CADA PRODUTO
- SERVIÇOS PROJETADOS PARA IMPLATAÇÃO, MONITORAMENTO DE FALHAS E RECUPERAÇÂO DAS APLICAÇÕES E/OU COMPONENTES AUTOMATICAMENTE EM CASO DE RECUPERAÇÃO DE DESASTRES
- ISOLAMENTO DE ACESSO A SERVIÇOS E SERVIDORES EM NÚVEM A PARTIR DE ACESSO CONTROLADO POR IPS
- ALTERAÇÃO PERIÓDICA DE SENHAS E TOKENS DE ACESSO INTERNO PELOS NOSSOS SERVIÇOS E SERVIDORES

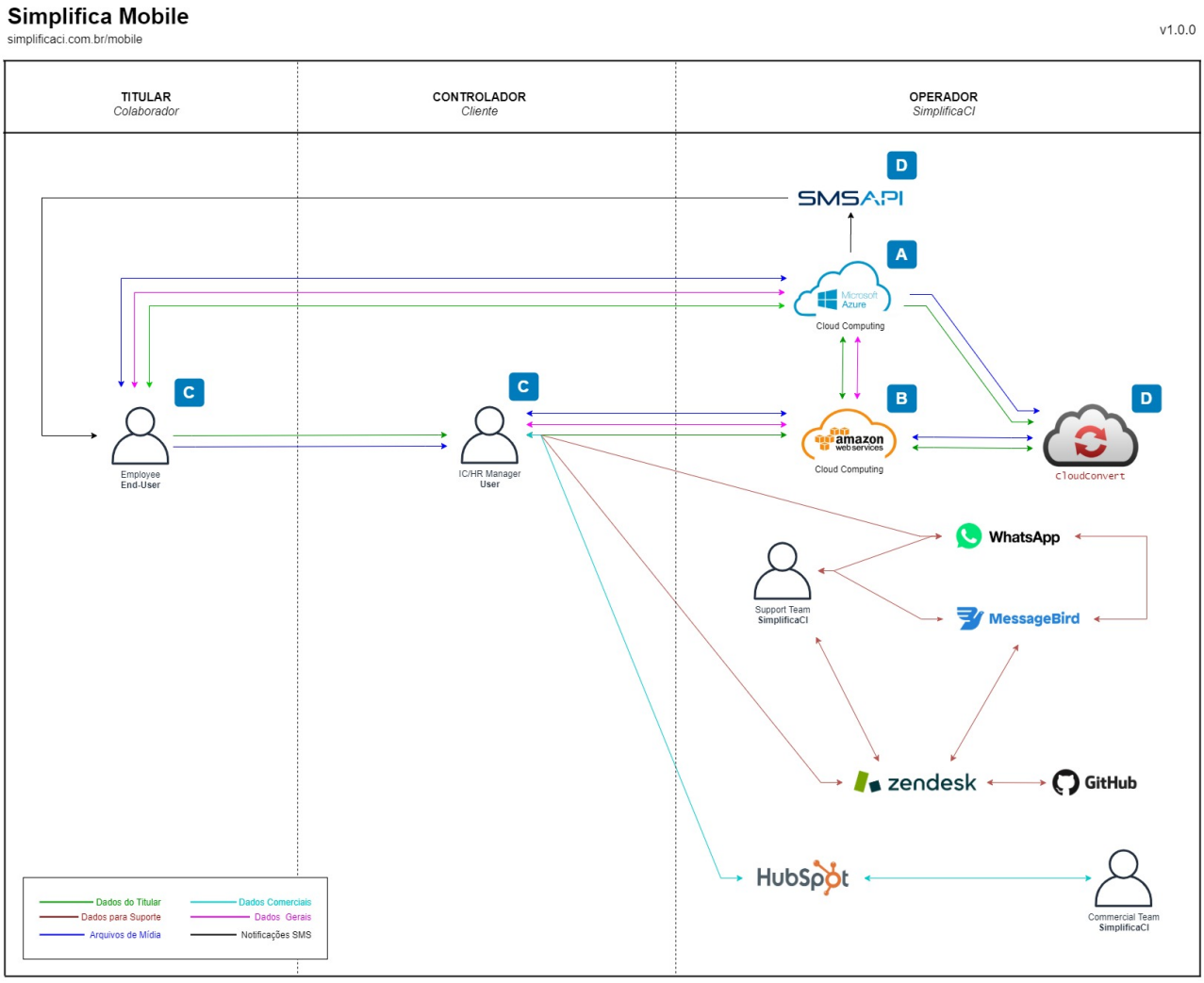
MEDIDAS DE MITIGAÇÃO DE RISCOS SUGERIDAS

- CRIPTOGRAFIA EXTRA NO BANCO DE DADOS PARA DADOS PESSOAIS QUANDO EM REPOUSO
- PENTEST CÍCLICO PARA VERIFICAÇÃO CONSTANTE DA SEGURANÇA
- ATUALIZAÇÃO DE DADOS DE EX-EMPREGADOS DOS CONTROLADORES
- PORTABILIDADE DE DADOS;
- AUTO SERVIÇO PARA ACOMPANHAMENTO E CONFIRMAÇÃO DE DOCUMENTOS E POLITICAS DE USO DE NOSSOS PRODUTOS
- AUTENTICAÇÃO A PLATAFORMA SIMPLIFICACI POR MEIO DE ACESSO VIA SINGLE SIGN-ON (SSO)
- AUTENTICAÇÃO A PLATAFORMA SIMPLIFICACI POR MEIO DE CONFIRMAÇÃO EM DUAS ETAPAS
- RESTRINGIR O CADASTRO DE SENHAS DE ACESSO QUE TENHAM NÍVEL DE SEGURANÇA BAIXO
- IMPLEMENTAÇÃO DE NOVAS METODOLOGIAS PARA TRIAGEM DE SEGURANÇA E VULNERABILIDADES SEGUINDO PADROES OWASP
- CONTENÇÃO DE DDOS A PARTIR DE SERVIÇOS DE FIREWALL PARA API (WAF)
- IMPLANTAÇÂO DE CONTROLE DE ATIVOS

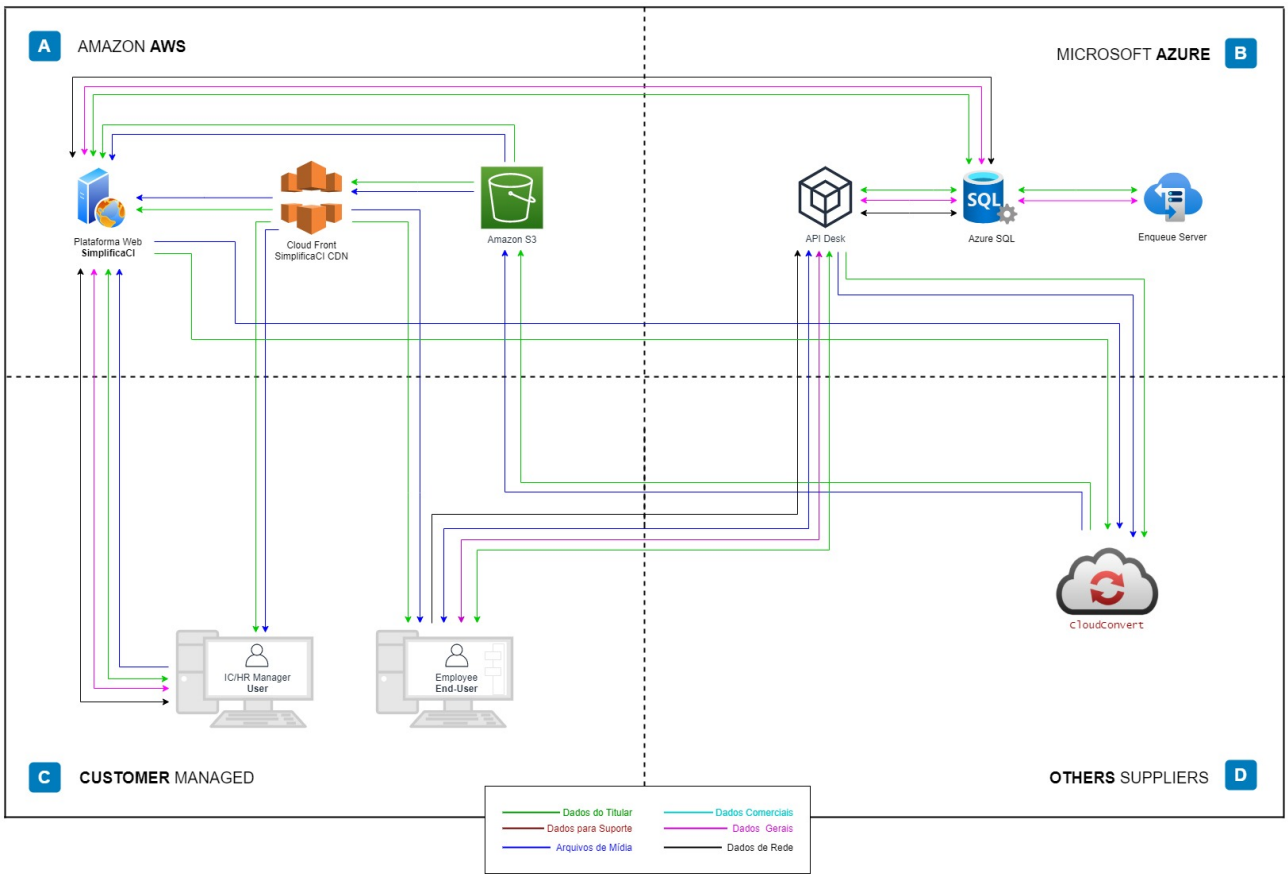
2.3 - Ciclo de Vida dos Dados Pessoais e Processos Inerentes

(Inventário de Dados, Data Mapping e Ativos)

Fluxo Macro dos Serviços



Detalhamento dos Serviços



2.4 - Ativos de Informação Utilizados na Finalidade de Tratamento

(Inventário de Dados, Data Mapping e Ativos)

DISPOSITIVOS DE ARMAZENAMENTO

ATIVOS DA OPERADORA	- Computadores dos desenvolvedores - Inventário de Ativos
ATIVOS DA CONTROLADORA (CLIENTE SIMPLIFICACI)	- Usuários Gestores c/ acesso limitado ao report de dados da própria controladora

POLÍTICA DE PRIVACIDADE	Política de Privacidade e Condições de Uso SimplificaCI
Nº DE TITULARES DE DADOS AFETADOS	100.000 a 200.000
DADOS PESSOAIS PROCESSADOS	PIA v.2.0

3 - Princípios Fundamentais

3.1 - Finalidade

(Princípios Fundamentais)

A SIMPLIFICACI enquanto operadora junto aos controladores que utilizam o software Simplifica Desk vincula-se estritamente à finalidade de tratamento embasada por meio de seu contrato de outorga de licença de uso de software (termos e condições de uso) não tendo tomada de decisão diversa do que a de prestação de serviços de serviços ali consubstanciada.

A finalidade de tratamento é legítima,específico, explícita específica e informada?

Na relação de operadora para com o(a) controlador(a) sim, o princípio da finalidade é devidamente atendido sem possibilidade de tratamento posterior de forma incompatível com suas finalidades. Na relação de operadora para com o titular de dado, a SIMPLIFICACI não se vincula diretamente ao

mesmo por outra forma que não a mantida estritamente com o controlador mediante cumprimento de contrato, e, ainda assim respeita os direitos dos titulares previstos na forma da Lei 13.709/2018

3.2 - Adequação

(Princípios Fundamentais)

Há compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento?

A SIMPLIFICACI na condição de operadora mantém plena compatibilidade do tratamento na forma específica do contrato de outorga de cessão de uso de software mantido junto ao cliente enquanto controlador.

3.3 - Necessidade

(Princípios Fundamentais)

Há limitação do tratamento ao mínimo necessário para a realização de suas finalidades?

Sim. A SIMPLIFICACI na condição de operadora mantém a coleta mínima de dados necessária para a integridade do software em questão.

3.4 - Livre Acesso

(Princípios Fundamentais)

É garantida aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento dos dados pessoais no referido software?

Primeiramente o software contempla a documentação necessária para atendimento à transparência prevista na LGPD em seu artigo 6º, seja pela confecção do Privacy Impact Assessment, Política de Privacidade e Termos e Condições de Uso.

3.5 - Qualidade dos Dados

(Princípios Fundamentais)

É garantida aos titulares a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento?

Sim. O software está em processo de adequação frente às premissas da LGPD e garantirá, inclusive em suas próximas versões as melhorias e otimizações previstas em lei.

3.6 - Transparência

(Princípios Fundamentais)

É garantida aos titulares de dados informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento?

Sim, a exemplo do item 3.5. o titular de dados pode fazer tais solicitações diretamente frente aos controladores com os quais esteja diretamente vinculados.

3.7 - Segurança

(Princípios Fundamentais)

Utilização de 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?

Sim. No momento de confecção e fechamento da versão do presente PIA v.2.0, a SIMPLIFICACI enquanto operadora está em fase de implementação dos parâmetros de seguranças exigidos pelo artigo 50 da LGPD por meio do framework da ISO/IEC 27002, ISO/IEC 27001 e ISO/IEC 27701.

3.8 - Prevenção

(Princípios Fundamentais)

Existe adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais?

Sim. No momento de confecção e fechamento da versão do presente PIA v.2.0, a SIMPLIFICACI enquanto operadora está em fase de implementação dos parâmetros de seguranças exigidos pelo artigo 50 da LGPD por meio do framework da ISO/IEC 27002, ISO/IEC 27001 e ISO/IEC 27701.

3.9 - Não Discriminação

(Princípios Fundamentais)

A organização realiza tratamentos por meio dos dados pessoais objetos de input que possam gerar discriminação ou ato atentatório à dignidade da pessoa humana dos titulares de dados na forma do artigo 2º da LGPD?

Não há para o presente software qualquer realização do tratamento para fins discriminatórios ilícitos ou abusivos.

3.10 - Responsabilização e Prestação de Contas

(Princípios Fundamentais)

A SIMPLIFICACI enquanto agente de tratamento adota medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas em expresso atendimento à lei 13.709/2018.

3.11 - Atualização de Dados Pessoais e Fidedignidade

(Princípios Fundamentais)

No momento de confecção e fechamento da versão do presente PIA v.2.0 a base de dados da SIMPLIFICACI está zerada, sem inputs e atendendo ao referido princípio.

4 - Riscos

4.1 - Controles para proteger os direitos dos titulares dos dados

(Riscos)

- **Como é que os titulares dos dados são informados sobre o tratamento dos seus dados?**
  Por meio da política de privacidade, termos e condições de uso do software bem como direito à requisição feita pelos mesmos ao CONTROLADOR.

- **Como é obtido o consentimento dos titulares de dados?**
  Decisão cabível ao CONTROLADOR.

- **Como é garantido o acesso e portabilidade dos dados pessoais?**
  NMediante solicitação pelo titular dos dados junto ao CONTROLADOR que gerará relatório para respectiva entrega.

- **Como é garantida a atualização / retificação e apagamento dos dados pessoais pedido pelo titular dos mesmos?**
  Por meio de acesso mediante requisição pelo usuário junto ao encarregado de dados do CONTROLADOR e mediante acesso sistêmico permitindo a atualização dos dados.

- **Como é garantida a limitação do tratamento dos dados pessoais pedido pelo titular dos mesmos?**
  Atualmente a garantia quanto às operações de tratamento se dá pela SIMPLIFICACI enquanto operadora por meio da remodelação de seu contrato de outorga de licença de uso de software limitando suas obrigações enquanto operador.

- **As obrigações dos subcontratantes são claramente identificadas e regulados por contrato ou outro ato normativo?**
  Sim

- **No caso de transferência de dados, os dados são adequadamente protegidos?**
  Sim, a SIMPLIFICACI possui adequada estrutura de armazenamento em ambiente altamente tecnológico. No momento de construção do presente PIA a ANPD ainda está em fase de formatação e, portanto, sem maiores diretivas.

4.2 - Mapeamento de Riscos

(Riscos)

No momento de confecção e fechamento da versão do presente PIA (versão 1), a SIMPLIFICACI enquanto operadora está em fase de implementação dos parâmetros de seguranças exigidos pelo artigo 50 da LGPD por meio do framework da ISO/IEC 27002, ISO/IEC 27001 e ISO/IEC 27701 que permitirá não apenas o mapeamento dos riscos atrelados à solução MOBILE mas também a definição de políticas de segurança da informação, plano de respostas à incidentes com sua respectiva àrvore de acionamentos e tomadas de decisões frente à Autoridade Nacional de Proteção de Dados na forma do artigo 48 da Lei Geral de Proteção de Dados

4.3 - Plano de Ação

(Riscos)

A SIMPLIFICACI em seu processo de adequação e plano de conformidade frente à LGPD vislumbrará sempre eventuais recursos de otimização para atendimento pleno às diretivas e instruções legais bem como à futuras determinações da ANPD.

5 - Parecer DPO

Por tratar-se o presente PIA da Versão 1 delineada após o Risk Assessment, Inventário de Dados, Datamapping a SIMPLIFICACI conta com consultoria externa por especialista em programas de privacidade que, atuando conjuntamente ao time de privacidade da SIMPLIFICACI permite o engajamento e enforcement para cumprimento às determinações na forma da lei. O presente PIA em sua V1 atende e antecipa às exigências legais de uma legislação recentemente em vigor e cuja aplicabilidade ainda carece de maiores diretivas da própria Autoridade Nacional de Proteção de Dados demonstrando, desta forma, compromisso ético e zelo junto à sua frente de atuação, clientes, parceiros e programa de compliance implementado em seu core de negócios.