RELATÓRIO INICIAL DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPDP)

SUMÁRIO

1. INTRODUÇÃO E ESCLARECIMENTOS NECESSÁRIOS

Aqui estão elencados os processos, procedimentos, ações e demandas relacionadas à dados pessoais no âmbito da VAMOS PARCELAR e a demonstração detalhada de quais dados são coletados, por onde chegam esses dados, como eles são tratados e armazenados, o período de armazenamento dos dados, as formas e possibilidades de exclusão e de que forma os titulares desses dados pessoais podem exercer seus direitos frente à VAMOS PARCELAR.

Inicialmente, é necessário esclarecer alguns dos termos que serão utilizados neste documento, todos eles também utilizados no texto da Lei Geral de Proteção de Dados, sobretudo no artigo 5º.

i) Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

ii) Dado pessoal sensível: dado pessoal sobre 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, quando vinculado a uma pessoa natural;

iii) Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

iv) Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

v) Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

vi) Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

vii) Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

viii) Agentes de tratamento: o controlador e o operador;

ix) Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

x) Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um

dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

xi) Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

xii) Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

xiii) Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

xiv) Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

xv) Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

xvi) Relatório de impacto à proteção de dados pessoais (RIPDP): documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

2. TIPOLOGIA DOS DADOS MANEJADOS PELA VP

- Abaixo se observa a lista de dados pessoais utilizados na VAMOS PARCELAR.
  - I. Nome
  - II. Dados de identificação civil (RG e CPF)
  - III. Endereço eletrônico.
  - IV. Endereço de I.P.
  - V. Telefone.
  - VI. Dados bancários.

3. MÉTODOS DE COLETA DE DADOS

Os dados são coletados por intermédio das redes sociais, por meio da interação dos clientes com as mídias sociais, dos cookies utilizados no site, nas plataformas e nos cadastros realizados pelos clientes no marketplace.

Existem ainda os dados dos clientes que comparecem aos pontos de atendimento físico, nos quais os atendentes realizam o cadastro dos clientes na plataforma marketplace.

4. ARMAZENAMENTO DOS DADOS

Por motivos de segurança e governança, os dados coletados são armazenados no sistema marketplace pelo período de cinco anos, respeitando-se o prazo prescricional do Código Civil Brasileiro (art. 206, § 5).

A justificativa para o armazenamento temporário ocorre no sentido de evitar/mitigar riscos de demandas pautadas em responsabilidade civil, bem como, no aspecto processual, assegurar produção e apresentação de provas em possível demanda judicial, em atenção à possibilidade de inversão do ônus da prova nos termos do art. 6º VIII do Código de Defesa do Consumidor.

Quando solicitada pelo cliente, a VP procederá com o bloqueio dos dados de modo que não serão utilizados dados pessoais para fins comerciais ou de compartilhamentos.

5. FINALIDADE DO USO DOS DADOS PESSOAIS

Os dados pessoais coletados e tratados servirão para:

i) Realizar o serviço de parcelamento contratado pelo cliente.
ii) Identificação do cliente.
iii) Validação de dados para evitar fraudes.
iv) Identificação do perfil de consumo.

6. MAPEAMENTO DO FLUXO DE DADOS PESSOAIS NA VP

6.1. Do formulário sobre o fluxo e manejo de dados na VP

Foi confeccionado um formulário por meio do qual os setores deveriam responder a questionamentos sobre como os dados chegam até o setor, quem trata esses dados, para onde são enviados e como são armazenados, e diante dessas respostas foi criado o mapeamento de dados dentro da VP, documento que servirá de apoio para as futuras ação do setor de compliance no sentido de minimizar, acompanhar e metrificar os dados de forma a evitar exposições a riscos.

6.2. Das respostas ao formulário

A seguir tem-se a síntese das respostas encaminhadas ao setor jurídico e compliance pelos gestores dos demais setores da empresa.

Pergunta 1: Quais os dados pessoais/sensíveis que seu setor costuma movimentar de clientes e/ou colaboradores? (Ex: número de documentos, nome completo e de parentes, dados bancários, CPF, endereço e etc...)

Resumo das respostas: Os setores informaram que não tem acesso à dados sensíveis. Em geral se transaciona dados pessoais como RG e CPF, endereço, número de cartão, email e contatos telefônicos.

Pergunta 2: Por qual meio esses dados chegam ao seu setor?

Resumo das respostas: os dados dos clientes chegam na VP através dos sistemas de pagamento, redes sociais e atendimento direto aos clientes.

Os dados que chegam por meio dos sistemas de pagamento chegam primeiro ao antifraude, e os dados advindos das redes sociais e atendimento aos clientes chegam para os setores de atendimento e marketing (redes sociais).

Já os setores mais internos da empresa, como financeiro e operacional, tem acesso aos dados a partir do envio das demandas e pagamentos por outros setores.

O setor de Recursos Humanos e Departamento Pessoal tem acesso aos dados com o envio de currículos via Whatsapp, e-mail e sites de busca de emprego.

Pergunta 3: Como esses dados são armazenados dentro do seu setor?

Resumo das respostas: Os dados costumam ser salvos em nuvem (por meio de e-mails, drives e canais de chat, por exemplo, condensados em documentos, ordens de serviço e planilhas. Apenas o setor operacional possui *backoffice* e HD externo para armazenamento dos dados.

Pergunta 4: Existe alguém em especial para tratar desses dados, ou são tratados por todo o setor?

Resumo das respostas: Na maioria dos setores o contato com esses dados é observado por todos os componentes do setor. Apenas o setor de atendimento que concentra as informações nos casos de ressarcimento em uma única colaboradora, o marketing tem uma única colaboradora que tem acesso às redes sociais, e que, portanto, só ela tem acesso aos dados, e o setor jurídico subdivide as áreas, e consequentemente o acesso aos dados.

Pergunta 5: Depois de tratados, qual o destino dos dados pessoais/sensíveis, dentro do seu setor?

Resumo das respostas: Os dados dos clientes costumam ser armazenados pelo próprio setor, através de drives em nuvem, e-mails, planilhas online e etc...

Os currículos recebidos pelo setor RH/DP ficam arquivados pelo período de 6 meses, e depois são descartados, conforme termo de ciência alojado no site da VP, na aba trabalhe conosco.

Ademais, o setor de marketing captura e envia os dados dos clientes para o setor de atendimento, via trello.

Pergunta 6: Existe alguma preocupação do seu setor com a confidencialidade e/ou segurança dos dados pessoais? (Ex: fragilidade do sistema, tramitação de informações entre setores, funil de comunicação, etc.…)

Resumo das respostas: os setores têm especial preocupação com o livre acesso de dados pessoais dentro do setor.

Pergunta 7: Você tem alguma sugestão para melhorar o tratamento desses dados dentro da VP?

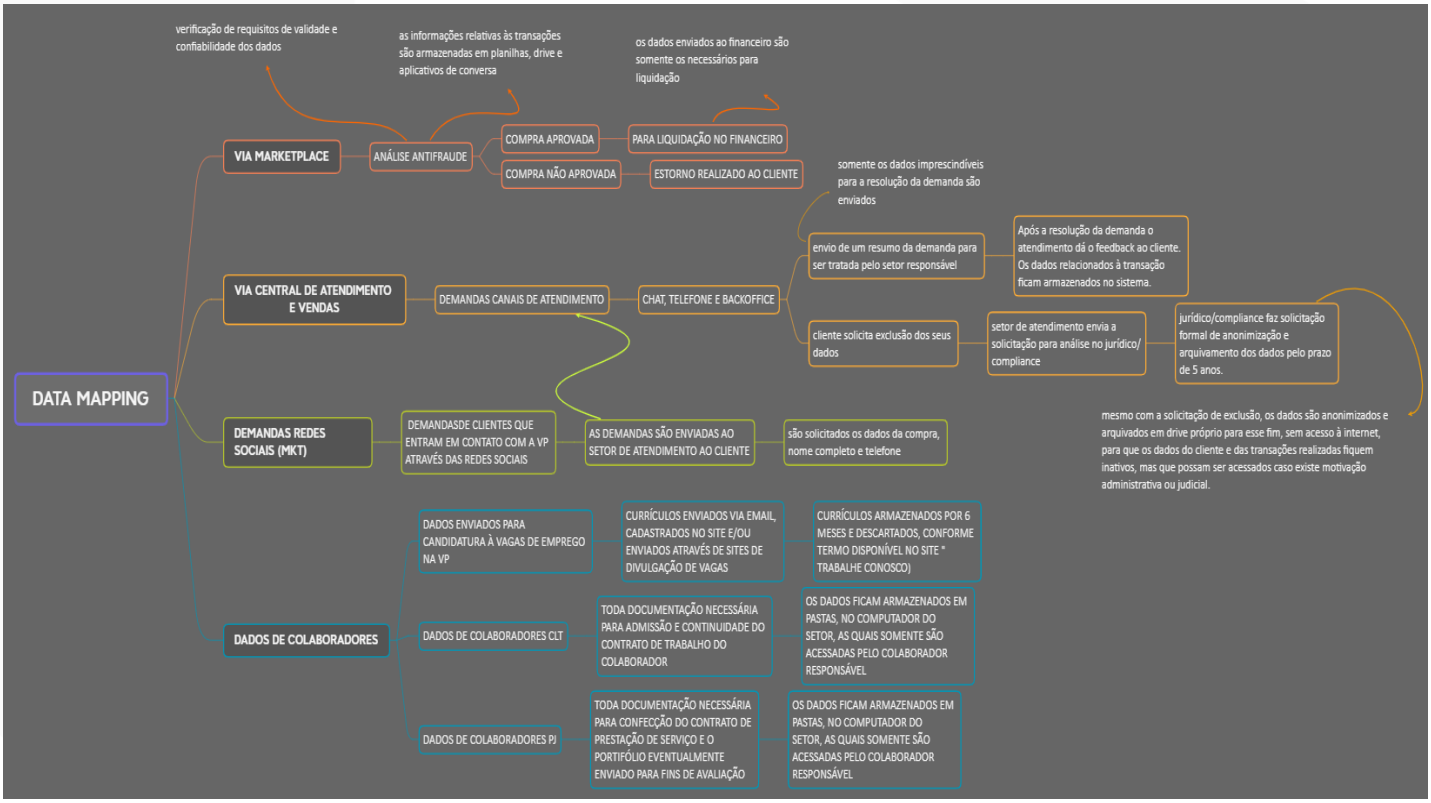
Resumo das respostas: sugeriu-se sistemas de antivírus, perfis com limitação de acesso à determinados dados e melhorias do meio de comunicação e transição de dados entre setores.

7. MAPEAMENTO DO FLUXO DE DADOS MANEJADOS

A partir das informações fornecidas pelo formulário foi possível realizar o mapa de trajetória dos dados dentro da VAMOS PARCELAR, podendo visualizar de forma mais clara e completa a jornada dos dados.

Diante da avaliação do mapa é possível identificar os pontos de maior vulnerabilidade dos dados, podendo colocar em prática os sistemas, fluxos e soluções para diminuir a exposição dos dados à riscos.

Abaixo, segue o mapa, que também ficará disponível para melhor visualização, anexo a este documento.



8. PLANEJAMENTO DA ELABORAÇÃO DE MATRIZ DE RISCOS NO PROCESSO DE TRATAMENTO

- Com base nas coletas de informações já efetuadas, no intuito de melhor compreender e monitorar os riscos para proteção de dados, mostrou-se necessário também catalogar e classificar os riscos, para então organizar uma política de proteção eficiente.

Observou-se até então a incidência de alguns riscos identificados, com base na observação do mapa do fluxo dos dados e das respostas observadas no formulário, quais sejam:

- RISCOS:
    1. Risco de vazamento por agentes externos.
    2. Risco de vazamento por agentes internos.
    3. Risco de vazamento acidental de dados.
    4. Risco de armazenamento inseguro de dados.
    5. Risco de ataque cibernético de vírus e/ou *malwares*.
    6. Risco de tratamento inadequado ou em desacordo com o previsto na legislação.
    7. Risco de alteração e/ou inexatidão dos dados.

Para realizar a matriz de riscos, será utilizada a metodologia de classificação de riscos do COSO (Commit-tee of Sponsoring Organizations of the Treadway Commission).

Os riscos identificados serão submetidos a uma matriz que os classificará de acordo com a probabilidade de ocorrência e o impacto causado, em seguida serão submetidos ao gráfico de calor, que indicará quais riscos merecem maior atenção e observação mais próxima e quais riscos podem ser observados e acompanhados com maior elasticidade.

As tabelas serão apresentadas em planilhas e serão periodicamente revisadas, assim como todo o programa.

CLASSIFICAÇÃO DA PROBABILIDADE POR EVENTO		
CLASSIFICAÇÃO	**DESCRIÇÃO**	**PESO**
1- REMOTO	MENOS DE UMA VEZ POR ANO	1
2 - IMPROVÁVEL	UMA VEZ POR ANO	2
3 - POSSÍVEL	UMA VEZ POR SEMESTRE	3
4 - PROVÁVEL	UMA VEZ POR MÊS	4
5 - QUASE CERTO	UMA VEZ POR SEMANA OU MAIS	5

CLASSIFICAÇÃO DO IMPACTO POR EVENTO		
CLASSIFICAÇÃO	**DESCRIÇÃO**	**PESO**
1 - INSIGNIFICANTE	Sem danos e prejuízos, perda financeira pequena ou indireta	1
2 - BAIXO	Compromete somente o processo em questão, com impacto referente à eficiência do processo sob a dimensão de custo e duração. Ex: retrabalho, parada de sistemas não críticos, ausência de ferramentas adequadas.	2
3 - MODERADO	Requer tratamento, indica significativa perda financeira. Impacto relacionado à perda e/ou comprometimento de ativos não críticos e/ou descumprimento de leis ou regulamentaçãos que não comprometem a imagem da empresa.	3
4 - ELEVADO	Grandes danos e prejuízos diretos, perda de capacidade de operação. Impacto relacionado à perda e/ou descumprimento	4
5 - CRÍTICO	Eventos relevantes que comprometem fortemente o resultado da empresa e sua estratégia. Eventos deste tipo podem afetar o resultado da empresa fortemente.	5

PROBABILIDADE						
	5 -QUASE CERTO					
	4- PROVÁVEL					
	3- POSSÍVEL					
	2 - IMPROVÁVEL					
	1 - REMOTO					
IMPACTO POR EVENTO		1 - INSIGNIFICANTE	2 - BAIXO	3 - MODERADO	4 - ELEVADO	5 - CRÍTICO

9. CONCLUSÃO E RESULTADOS

Referente à primeira etapa, foram realizadas diligências no sentido de se obter informações do atual cenário de manejo dos dados pessoais de clientes da VP.

Identificou-se a necessidade de realizar um mapa de riscos com base nas informações levantadas de modo a permitir a organização de um normativo efetivo acerca da política interna de proteção de dados pessoais.

Considera-se que a primeira fase cumpriu seus objetivos, pois apresentou a visão inicial do atual fluxo de dados pessoais da VP, bem como esclareceu sobre formas de detectar possíveis lacunas no tratamento dos dados.

Assim, verificou-se a possibilidade de prosseguir para a fase seguinte, elaboração da matriz de riscos, anexa a este documento.