POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

SEGURANÇA DA INFORMAÇÃO

ÍNDICE

1. OBJETIVO 3
2. APLICAÇÃO 3
3. REFERÊNCIAS 3
4. GLOSSÁRIO 3
5. RESPONSABILIDADES 5
5.1. Encarregado da Proteção dos Dados Pessoais (DPO) 5
5.2. Segurança da Informação 6
5.3. Tecnologia da Informação 6
5.4. Comitê de TI e SI 7
5.5. Compliance 7
5.6. Jurídico 7
5.7. Gerente de Recursos Humanos 7
5.8. Marketing 8
5.9. Gestores 8
5.10. Colaboradores 8
5.11. Terceiros e Prestadores de Serviços 9
6. DIRETRIZES 9
6.1. Princípios 9
6.2. Direitos dos Titulares 10
6.3. Proteção dos Dados Pessoais 11
6.3.1. Coleta dos Dados Pessoais 11
6.3.2. Uso dos Dados Pessoais 12
6.3.3. Armazenamento dos Dados Pessoais 12
6.3.4. Eliminação de Dados Pessoais 13
6.3.5. Compartilhamento de Dados Pessoais com Terceiros 14
6.3.6. Transferência Internacional de Dados Pessoais 14
6.4. Diretrizes de Resposta às Solicitações e Requisições 15
6.4.1. Resposta à Requisição do Titular dos Dados Pessoais 15
6.4.2. Resposta à Autoridade Fiscalizadora 15
6.4.3. Resposta à Autoridade Judicial 16
6.5. Inventário de Tratamento de Dados Pessoais 16

6.6. Resposta aos Incidentes de Violação de Dados Pessoais 17
6.7. Relatório de Impacto à Proteção de Dados Pessoais 17
7. VIOLAÇÃO À POLÍTICA 17
8. HISTÓRICO 18

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Definir os princípios e regras aplicáveis no tratamento de dados pessoais, em atenção às disposições da LGPD, bem como organizar os pontos de atenção necessários para a elaboração de um programa de privacidade que garanta à Galapagos Capital, a adequada conformidade com a referida Lei, considerando os dados nos formatos físico e digitais/eletrônicos.

Para efeito desta política, entende-se que o termo *Galapagos Capital* compreende todas as subsidiárias da Galapagos Holding S.A.

2. APLICAÇÃO

Esta política se aplica a todos os envolvidos, direta ou indiretamente, com os dados pessoais e dados pessoais sensíveis sob responsabilidade da Galapagos Capital, e que estejam autorizados a acessá-los para suas atividades diárias, abrangendo todos os sistemas, as soluções e os equipamentos em uso. Os envolvidos são: os colaboradores da empresa, as consultorias externas, os auditores internos e externos e os representantes dos órgãos reguladores sempre que requerido.

Para efeitos desta política, entende-se que os dados pessoais consideram, em geral, as duas classificações dispostas na LGPD: dados pessoais e dados pessoais sensíveis. Quando houver a necessidade de especificar quais dados estão sendo mencionados – pessoais ou pessoais sensíveis, a política irá indicar, em caso contrário, ambos serão considerados como foco das diretrizes apresentadas.

3. REFERÊNCIAS

- LGPD - Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)
- PO-SI-001 – Política de Segurança da Informação

4. GLOSSÁRIO

Anonimização: utilização de meios técnicos disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Considerando que dados anonimizados não são considerados dados pessoais para fins da LGPD, não se aplicam os princípios de tratamento de dados pessoais aos dados anonimizados, salvo quando o processo de anonimização ao qual os dados pessoais foram submetidos for revertido ou for reversível;

Ativo: é qualquer coisa que tenha valor material ou imaterial, sendo tangível ou intangível, para a Galapagos Capital e precisa ser adequadamente protegido;

Autenticidade: garantia de que a informação foi criada, editada ou emitida por quem se disse ter sido, sendo capaz de gerar evidências não repudiáveis em relação ao criador, editor ou emissor;

Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da LGPD;

Backup: salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de restauração ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada da Galapagos Capital;

Colaborador: empregado, estagiário, menor aprendiz, ou qualquer outro indivíduo ocupante de cargo ou emprego na Galapagos Capital.

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

Dado pessoal: Quaisquer informações relativas a uma pessoa física identificada ou identificável ou que possam ser identificadas, direta ou indiretamente, em particular, por referência a um identificador como nome, número de identificação, dados de localização ou a um ou mais fatores específicos para a identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, 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;

Encarregado de dados (DPO): ou Data Protection Officer, é a pessoa indicada pela Galapagos Capital para atuar como canal de comunicação entre o Controlador, os Titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD);

Incidente de segurança da informação: ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede que indica possível violação à Política de Segurança da Informação ou documentos complementares, falha de controles ou situação previamente desconhecida e que possa ser relevante à Segurança da Informação;

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

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;

Titular: pessoa natural a quem os dados pessoais se referem.

5. RESPONSABILIDADES

5.1. Encarregado da Proteção dos Dados Pessoais (DPO)

O encarregado da proteção dos dados pessoais (DPO) deve ser formalmente nomeado e ter seu contato publicado para acesso dos titulares dos dados pessoais da Galapagos Capital.

O DPO responde diretamente perante o nível mais elevado da administração da Galapagos Capital e tem as seguintes responsabilidades específicas:

- Gerenciar o programa de proteção de dados pessoais e reportar no Comitê de TI e SI as ações que necessitam de atuação das áreas;
- Desenvolver e promover políticas, normas e procedimentos de proteção de dados pessoais para os processos da Galapagos Capital;
- Monitorar a execução das políticas, normas e procedimentos relacionados à proteção dos dados pessoais e da privacidade dos titulares envolvidos;
- Acompanhamento a regulação aplicável ao tratamento de dados pessoais;
- Auxiliar os demais departamentos no cumprimento de suas metas relacionadas a tratamento de dados pessoais;
- Analisar contratos que envolvam tratamento de dados pessoais, seguindo o framework legal específico aplicável a cada situação em suas particularidades;
- Repassar responsabilidades de proteção de dados pessoais aos fornecedores e prestadores de serviços, incluindo a melhoria contínua dos níveis de conscientização dos mesmos em relação à proteção de dados pessoais;
- Organizar e/ou ministrar treinamentos em proteção de dados pessoais aos colaboradores e/ou prestadores de serviço que utilizam dados pessoais em suas atividades;
- Informar imediatamente aos gestores das informações quaisquer situações de violação desta política;
- Avaliar a necessidade, metodologia, salvaguardas e conformidade relativas à elaboração de Relatório de Impacto à Proteção de Dados, bem como proceder à sua elaboração;
- Conduzir procedimentos a fim de avaliar e preservar o nível de conformidade e transparência da Galapagos Capital, como por exemplo a avaliação de legítimo interesse, avaliação de impacto à privacidade, e outros que sejam definidos e requeridos pela ANPD;
- Atuar em conjunto com TI e SI nos casos de incidentes envolvendo dados pessoais, dados pessoais sensíveis e/ou dados de crianças/adolescentes;
- Atuar com a ANPD nos casos de incidentes verificados de acordo com as premissas indicadas por aquela instituição.

5.2. Segurança da Informação

- Assegurar a efetividade e a continuidade da aplicação desta política, disseminando as diretrizes indicadas;
- Prover recursos suficientes para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente os controles e procedimentos relacionados à proteção dos dados pessoais;
- Identificar e avaliar riscos relacionados à segurança da informação e proteção de dados pessoais e propor melhorias e recursos necessários;
- Gerenciar os controles e as ferramentas de segurança da informação, assim como tratar os incidentes, problemas, mudanças e quaisquer requisições e/ou reportes relacionados à privacidade dos dados;
- Garantir que os requerimentos de segurança indicados na LGPD estejam estabelecidos e efetivos;
- Comunicar tempestivamente ao DPO os incidentes de segurança cibernética envolvendo dados pessoais, dados pessoais sensíveis e/ou dados de crianças/adolescentes.

5.3. Tecnologia da Informação

- Desenvolver, revisar e coordenar atividades com a finalidade de garantir o atendimento aos requisitos da LGPD, de acordo com o processo de identificação, análise e tratamento dos riscos de relacionados à privacidade, incluindo os aspectos específicos relacionados aos controles de segurança dos dados pessoais no formato eletrônico/digital sob responsabilidade da Galapagos Capital;
- Avaliar a efetividade e a eficácia de controles de proteção e dos processos de negócios vigentes, e promover a melhoria contínua no âmbito da privacidade;
- Monitorar ativamente as violações comportamentais a esta política, observadas sua natureza e gravidade;
- Cumprir e observar os requisitos legais, regulatórios e estatutários pertinentes à proteção da privacidade;
- Definir procedimentos e controles voltados à prevenção e ao tratamento dos incidentes, a serem adotados por empresas prestadoras de serviços e terceiros que manuseiem dados pessoais, tanto pelas definições legais e regulatórias, quanto pelas diretrizes, políticas e normas próprias da Galapagos Capital, ou que sejam relevantes para a condução das atividades operacionais destas;
- Assegurar que todos os sistemas, serviços e equipamentos usados para armazenamento de dados pessoais atendam aos padrões de segurança determinados pela empresa e por regulamentações aplicáveis, incluindo as melhores práticas mundiais;

- Reportar ao DPO e à Segurança da Informação quaisquer eventos ou incidentes envolvendo dados pessoais, dados pessoais sensíveis e/ou dados de crianças/adolescentes, bem como as ações iniciais para atendimento àqueles.

5.4. Comitê de TI e SI

- Assegurar a efetividade e a continuidade da aplicação da Política de Proteção de Dados Pessoais considerando os dados pessoais nos formatos físico e eletrônicos/digitais;
- Aprovar com periodicidade mínima anual a revisão desta política e o plano de ação e de resposta a incidentes envolvendo dados pessoais;
- Ser envolvido na tomada de decisões a respeito de atividades de tratamento de dados pessoais que envolvem riscos avaliados como altos e/ou críticos;
- Garantir que os planos e objetivos de proteção da privacidade estejam estabelecidos.

5.5. Compliance

- Revisar as alterações e criação de políticas, normas ou procedimentos sugeridos pelo DPO;

5.6. Jurídico

- Prestar suporte ao DPO na análise da legislação de dados pessoais;
- Revisar as alterações e criação de políticas, normas e procedimentos sugeridos pelo DPO;
- Participar previamente dos processos de contratação e aquisição de produtos e serviços da Galapagos Capital, validando as minutas de contrato visando que atendam aos controles de proteção de dados pessoais aplicáveis;
- Apoiar o DPO quanto a possiblidades de tratamento de dados pessoais no exterior, auxiliando no entendimento de validação do nível de proteção de dados pessoais do país destino;
- Aprovar antecipadamente quaisquer declarações de proteção de dados anexadas em comunicações, como e-mails, relatórios, comunicados diversos e cartas.

5.7. Gerente de Recursos Humanos

- Garantir que os dados pessoais dos colaboradores são tratados e protegidos com base nos propósitos comerciais legítimos e de acordo com as necessidades da Galapagos Capital, considerando os mesmos nos formatos físico e eletrônicos/digitais;
- Promover, em conjunto com o DPO, a cultura de proteção de dados pessoais na Galapagos Capital, realizando campanhas de capacitação e divulgação da proteção dos dados pessoais;
- Assegurar a divulgação e a disponibilidade dos documentos que compõem esta política e outras políticas internas para proteção de dados pessoais na empresa;

- Reportar tempestivamente ao DPO quaisquer situações de uso indevido ou quebra de controle de proteção dos dados pessoais, dados pessoais sensíveis e/ou dados de crianças/adolescentes sob a responsabilidade da área.

5.8. Marketing

- Atuar com o Encarregado de Dados para garantir que as iniciativas de marketing cumpram os princípios de proteção de dados em todos os formatos;
- Elaborar, com o apoio do DPO, campanhas de conscientização e materiais de divulgação e alerta relacionados a proteção de dados pessoais, sempre que necessário;
- Responder, seguindo as orientações do DPO, eventuais questionamentos de veículos de imprensa;
- Submeter à análise do DPO textos e comunicados sobre privacidade e proteção de dados pessoais, antes de sua publicação.

5.9. Gestores

- Garantir que as políticas e as normas relacionadas com a segurança e a proteção dos dados pessoais, nos formatos físico e eletrônicos/digitais sejam seguidas em sua área e pelos seus colaboradores;
- Orientar seus colaboradores e prestadores de serviço sempre que necessário sobre as diretrizes de privacidade evitando que incidentes de segurança sejam cometidos;
- Zelar pela proteção dos dados pessoais e dos recursos relacionados à sua área, fornecendo parâmetros de classificação condizentes com a criticidade dos mesmos e controlando os privilégios de acesso dos colaboradores sob sua gestão de acordo com as atividades que desempenham;
- Realizar a gestão dos riscos relativos aos processos de negócio e ativos sob sua responsabilidade;
- Manter os inventários de dados pessoais de sua área estejam atualizados refletindo todos os processos que os utilizam;
- Reportar ao DPO quaisquer eventos de descumprimento desta política, de incidentes ou outros relacionados com a quebra de controle de proteção dos dados pessoais sob responsabilidade da Galapagos.

5.10. Colaboradores

- Conhecer e observar a aderência dos itens descritos nesta política e nos demais documentos de governança relacionados ao tema de privacidade e proteção de dados pessoais, e relatar qualquer situação que represente seu respectivo desvio ou violação da privacidade;
- Tratar os dados pessoais sob responsabilidade da Galapagos Capital somente para fins autorizados, de forma ética e legal, respeitando os direitos do titular dos dados pessoais e de acordo com as orientações desta política e da legislação aplicável;

- Colaborar com a disseminação das boas práticas de segurança e privacidade das informações que são utilizadas no dia a dia de suas funções;
- Zelar pela integridade, disponibilidade, confidencialidade, autenticidade e legalidade dos dados pessoais acessados ou manipulados, não utilizando, enviando, transmitindo ou compartilhando indevidamente estes dados pessoais, em qualquer local ou mídia, inclusive na Internet;
- Reportar formalmente ao seu Gestor ou ao DPO quaisquer eventos relativos à violação, suspeita de violação ou mau uso de dados pessoais de que tiver conhecimento.

5.11. Terceiros e Prestadores de Serviços

- Seguir os procedimentos e controles definidos pela Galapagos Capital para a prevenção e 0 tratamento dos dados pessoais, assim como a norma e procedimentos de prestação de serviços da mesma;
- Proteger os dados pessoais sob sua responsabilidade e relatar ao Gestor do contrato ou ao DPO, tempestivamente, qualquer situação que represente seu respectivo desvio ou violação de segurança e de proteção daqueles;
- Participar dos treinamentos e programas de capacitação definidos pela Galapagos Capital para os temas de segurança da informação e de proteção da privacidade;
- Estabelecer procedimentos e controles internos voltados ao tratamento seguro e à proteção dos dados pessoais e demais informações relacionadas, assim como à prevenção e ao tratamento dos incidentes que envolvam informações críticas ou que sejam relevantes para a condução das principais atividades operacionais contratadas pela Galapagos Capital, de acordo com suas determinações e legislação e regulamentações vigentes aplicáveis;
- Zelar pela integridade, disponibilidade, confidencialidade, autenticidade e legalidade dos dados pessoais da Galapagos Capital, acessados ou manipulados, não utilizando, enviando, transmitindo ou compartilhando indevidamente estes dados pessoais, em qualquer local ou mídia, inclusive na Internet;
- Reportar formalmente ao Gestor do contrato ou ao DPO quaisquer eventos relativos à violação, suspeita de violação ou mau uso de dados pessoais de que tiver conhecimento.

6. DIRETRIZES

6.1. Princípios

Todas as atividades de tratamento dos dados pessoais, dados pessoais sensíveis e dados de crianças/adolescentes, deverão ocorrer de forma a atender os princípios estipulados pela LGPD:

- Da boa-fé: as operações de tratamento serão pautadas em boas intenções, na moral e nos bons costumes aceitos pela sociedade;

- Da finalidade e adequação: o tratamento de dados pessoais se limitará aos propósitos legítimos, específicos, explícitos e informados ao titular, e somente deve ocorrer de formas e por meios compatíveis com estas finalidades;
- Da necessidade: a coleta e a utilização de dados pessoais serão limitadas ao mínimo necessário para o cumprimento das finalidades pretendidas e expostas ao titular. Tais informações serão armazenadas pelo menor tempo possível/necessário;
- Do livre acesso e qualidade dos dados: é garantida a consulta facilitada e gratuita quanto à forma e duração da atividade de tratamento e, mediante requisição, integralidade dos dados pessoais tratados, sendo assegurada a exatidão, clareza e relevância destas informações, bem como a atualização/correção, mediante solicitação e caso seja comprovada a desatualização ou inexatidão;
- Da transparência: serão garantidas informações claras, precisas e facilmente acessíveis sobre a atividade de tratamento e os respectivos agentes envolvidos, bem como demais fatores de relevância, observados aqueles que se classificam como segredos estratégicos da Galapagos Capital;
- Da segurança e prevenção: a segurança e a confidencialidade dos dados pessoais serão garantidas por meio de medidas técnicas e administrativas, a fim de prevenir a ocorrência de incidentes de segurança envolvendo dados pessoais sob responsabilidade da Galapagos Capital;
- Da não discriminação: as atividades de tratamento de dados pessoais não terão como objetivo finalidades discriminatórias, ilícitas ou abusivas;
- Da responsabilização: serão armazenados os registros das medidas implementadas para cumprimento da LGPD, comprovando sua eficácia e eficiência.

6.2. Direitos dos Titulares

A Galapagos Capital deve implementar funcionalidades que atendam aos requisitos da LGPD que define os seguintes direitos garantidos aos titulares de dados pessoais:

- A confirmação da existência do tratamento;
- O acesso aos dados pessoais tratados;
- A correção dos dados pessoais incompletos, inexatos ou desatualizados;
- A anonimização, o bloqueio ou a eliminação dos dados pessoais;
- A portabilidade dos dados pessoais;
- A informação sobre as entidades públicas e privadas com as quais foi realizada o compartilhamento de dados;
- A informação sobre as consequências da revogação do consentimento, caso seja requerido pelo titular;
- A informação sobre quais fatores relevantes definiram uma decisão automatizada.

O atendimento dos direitos dos titulares deve ser realizado por meio de um canal de comunicação específico que será publicado no site junto com a Política de Privacidade que ficará disponível para todos os que utilizarem os serviços e informações disponibilizados pela Galapagos Capital. Este canal terá atendimento pelo Encarregado da Proteção dos Dados Pessoais (DPO) definido pela empresa.

6.3. Proteção dos Dados Pessoais

6.3.1. Coleta dos Dados Pessoais

A Galapagos Capital deve garantir que a coleta dos dados pessoais é a mínima possível para o desempenho de suas funções, respeitando e implementando o princípio da necessidade, inclusive se os dados pessoais que forem coletados de terceiros.

A Galapagos Capital, em grande parte de suas operações, coleta dados pessoais para execução de contrato, cumprimento de uma obrigação legal ou regulatória, proteção ao crédito e garantia da prevenção à fraude e à segurança do titular. Contudo, podem existir situações que a Galapagos Capital se valha de outras bases legais como consentimento e o legítimo interesse.

Os dados pessoais podem ser tratados para as seguintes finalidades, atendendo aos padrões de segurança definidos para a proteção da privacidade:

- Fornecer serviços bancários e financeiros dentro do modelo de negócio da empresa, necessários para o desempenho de um contrato do qual o cliente é parte ou para tomar medidas a pedido do cliente antes de celebrar um contrato;
- Cumprir obrigações legais e regulatórias do Banco Central do Brasil e outras autoridades;
- Realizar tarefas de interesse público, especialmente para efeitos de prevenção a fraudes. Se necessário, a empresa processa dados pessoais para cumprir os requisitos decorrentes de tais regulamentos;
- Avaliação da capacidade de pagamento;
- Análise de risco de crédito;
- Realizar atendimento ao cliente;
- Verificação da identidade dos clientes e/ou seus representantes legais;
- Cumprimento das obrigações de monitoramento e de reporte decorrentes da legislação;
- Regulamentos de gestão de riscos;
- Prevenção de erros em relação aos clientes quando são oferecidos produtos que não são adequados às suas necessidades ou avaliação do conhecimento do investimento em instrumentos financeiros;
- Tratamento de dados de indivíduos agindo em nome dos clientes da empresa;
- Prevenção a fraudes;

- Pesquisa de satisfação do cliente;
- Marketing direto dos produtos e serviços oferecidos pela empresa, bem como outras entidades para as quais a empresa fornece serviços sob acordos separados ou para fins administrativos internos da empresa, tais como a análise da carteira de crédito ou para fins internos de estatística e relatórios dentro da Galapagos Capital;
- Outras atividades que se façam necessárias para atendimento e cumprimento do modelo de negócio da empresa, e aos interesses do próprio titular dos dados pessoais.

6.3.2. Uso dos Dados Pessoais

A Galapagos Capital deve manter a exatidão, a integridade, a confidencialidade e a relevância dos dados pessoais com base na finalidade do tratamento quando do uso dos dados pessoais:

- Mecanismos de segurança adequados devem ser definidos e implementados para a proteção dos dados pessoais, e devem ser utilizados para evitar que aqueles sejam roubados, mal utilizados, além de evitar incidentes e violações relacionadas àqueles.
- Somente pessoas e Agentes de Tratamento autorizados podem ter acesso aos dados pessoais (em observância à necessidade e relevância da concessão do acesso);
- Todo e qualquer compartilhamento de dados pessoais deve ocorrer por meio das ferramentas e recursos da empresa, e de acordo com as políticas e controles de segurança vigentes.
- Soluções e mecanismo de comunicação segura devem ser definidos e implementados para assegurar a confidencialidade, integridade e disponibilidade do dado pessoal, em todos os meios de armazenamento e transmissão dos dados pessoais;
- Medidas de segurança da informação devem ser adotadas e monitoradas para assegurar que os dados pessoais se mantenham íntegros (sem alterações indevidas), exatos, completos e atualizados;
- Os dados pessoais não são transferidos para os países que não possuem leis de proteção de dados adequadas ou sem conformidade com o que preconiza a LGPD do Brasil;
- Os dados pessoais devem estar acessíveis e utilizáveis pelas pessoas e entidades autorizadas sempre que sejam necessários;
- Registro de logs e trilhas de auditoria do ciclo de vida do dado pessoal devem ser implementados.

6.3.3. Armazenamento dos Dados Pessoais

Os dados pessoais, incluindo os dados sensíveis e os de menores de idade, quando aplicável, devem ser armazenados de forma segura e seu tratamento deve seguir todas as diretrizes da Política de Segurança da Informação (PSI) e, também, deste documento e de todos destes derivados.

Os documentos são sempre retidos em um local seguro, com pessoal autorizado sendo o único a ter acesso. Após o término do período de retenção, os documentos são revisados, arquivados ou destruídos confidencialmente, dependendo de sua finalidade, classificação e tipo de ação.

Estas regras descrevem como e onde os dados devem ser armazenados com segurança:

- Quando os dados são armazenados em papel, eles devem ser mantidos em um local seguro com acesso apenas a pessoal autorizado. Estas diretrizes também se aplicam a dados pessoais armazenados eletronicamente e que foram impressos por quaisquer motivos;
- Arquivos devem ser mantidos em uma gaveta trancada ou em um arquivo com acesso controlado;
- Os colaboradores devem certificar-se de que dados pessoais impressos não sejam deixados onde pessoas não autorizadas possam acessá-los;
- As impressões de dados pessoais devem ser trituradas e descartadas com segurança quando não forem mais necessárias.

Quando os dados são armazenados eletronicamente, eles devem ser protegidos contra o acesso não autorizado, exclusão acidental e ações maliciosas:

- Os dados pessoais devem ser protegidos por senhas fortes que são alteradas regularmente e nunca devem compartilhadas;
- Os dados pessoais só devem ser armazenados em unidades e servidores designados e devem ser enviados somente para serviços e provedores de computação em nuvem devidamente aprovados;
- Os dados pessoais devem ser submetidos a backup com frequência. Esses backups devem ser testados regularmente, de acordo com os procedimentos de backup definido pela empresa;
- Os dados pessoais nunca devem ser salvos diretamente em notebooks ou outros dispositivos móveis, como tablets ou smartphones sem mecanismos de segurança devidamente aprovados pela Galapagos Capital, e apenas quando estritamente necessário para a operação;
- Todos os servidores e computadores que contêm dados pessoais devem ser protegidos por processos e tecnologias de segurança da informação definidos pelas políticas da empresa;
- No caso de armazenamento fora do Brasil, a área responsável pelo processo de negócio relacionada ao tratamento dos dados pessoais deve estar atenta para o país em que o hardware se localiza e deve-se acionar o Jurídico e Compliance da empresa para verificar se há amparo legal e contratual para que os dados pessoais estejam armazenados nesse país.

6.3.4. Eliminação de Dados Pessoais

- Após cumprida a finalidade do tratamento e findo o prazo de armazenamento determinado pela Galapagos Capital ou por definição de um regulador, os dados devem ser eliminados de modo seguro, sejam eles registrados em meios físicos ou digitais;
- A eliminação dos dados pessoais poderá ser realizada também a pedido do titular do dado ou da ANPD;
- A manutenção dos dados pessoais após atingida sua finalidade é possível no caso de cumprimento de obrigação legal ou regulatória por parte da Galapagos Capital;

- A solicitação de eliminação também não poderá ser atendida no caso de cumprimento de obrigação legal quanto ao armazenamento destes dados para fins regulatórios, respeitada a tabela de temporalidade;
- O descarte de dados confidenciais e dados restritos deve ser evidenciado para fins de controle e auditoria.

6.3.5. Compartilhamento de Dados Pessoais com Terceiros

- Ao utilizar os serviços de um fornecedor ou parceiro de negócios terceiro para tratar dados pessoais em seu nome, a Galapagos Capital deve garantir que este operador forneça as medidas de segurança para proteger os dados pessoais apropriados aos riscos associados, incluindo, mas não se limitando a proteger sua divulgação não autorizada, o uso indevido de dados pessoais e/ou o acesso por pessoas não autorizadas;
- Deve ser exigido contratualmente que o fornecedor ou parceiro de negócio forneça o mesmo nível de proteção de dados aplicados dentro da Galapagos Capital. O fornecedor ou parceiro de negócio deve apenas tratar dados pessoais para cumprir suas obrigações contratuais com a empresa ou sob suas instruções, e não para quaisquer outros fins;
- O compartilhamento de dados pessoais ou de documentos/arquivos com dados pessoais pode ser feito para agentes de tratamento autorizados, com as medidas de segurança indicadas pelas áreas de Segurança e de Tecnologia da Informação e somente para as finalidades de uso ou tratamento prévia e devidamente informadas e legitimadas junto ao titular dos dados pessoais;
- O compartilhamento de dados pessoais com demais agentes de tratamento, excetuando-se o compartilhamento realizado para cumprimento de obrigações legais, somente poderá ocorrer caso estes tenham firmado contratos com cláusulas referentes à Proteção de Dados Pessoais, seguindo os padrões adotados pela Galapagos Capital;
- No caso de impossibilidade de celebração de contrato ou aditivo com a parte em questão, devem ser adotados controles mitigatórios em relação à segurança e proteção do tratamento dos dados pessoais;
- O compartilhamento de dados pessoais cujo tratamento tenha como hipótese legal o consentimento somente poderá ocorrer com o consentimento do titular dos dados pessoais que esteja ciente deste compartilhamento, sendo que aquele consentimento deve ser coletado anteriormente ao início do tratamento dos dados pessoais;
- Os dados pessoais anonimizados podem ser transferidos para terceiros, desde que respeitados os requisitos de tratamento disposto na legislação aplicável.

6.3.6. Transferência Internacional de Dados Pessoais

Caso os dados pessoais sejam transferidos para outro país, a possibilidade de compartilhamento com outro Controlador deverá ser submetida à análise do DPO, das áreas de Segurança e de Tecnologia da Informação

e pela área Jurídica, de modo que possam avaliar se o país de destino possui grau de proteção de dados que esteja adequado ao ordenamento jurídico brasileiro.

Se o Controlador Receptor oferecer e comprovar garantias de cumprimento dos direitos do titular, a transferência internacional de dados também poderá ser possível na forma de (i) cláusulas contratuais específicas para determinada transferência; (ii) cláusulas-padrão contratuais; (iii) normas corporativas globais; e (iv) selos, certificados e códigos de conduta emitidos pela ANPD.

A transferência internacional de dados pessoais também pode ocorrer a partir das finalidades elencadas abaixo:

- Quando a transferência for necessária para a proteção da vida do titular ou de terceiros;
- Quando a Autoridade Nacional autorizar a transferência;
- Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional
- Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente este evento de outras finalidades;
- Para cumprimento de obrigação legal ou regulatória pela Galapagos Capital;
- Quando necessária para execução de contrato e procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

6.4. Diretrizes de Resposta às Solicitações e Requisições

6.4.1. Resposta à Requisição do Titular dos Dados Pessoais

- Todos os colaboradores ou prestadores de serviço têm o dever de encaminhar ao DPO as requisições amparadas na LGPD que foram recebidas diretamente. Não devem enviar nenhuma resposta ao solicitante;
- Cabe ao DPO a avaliação do questionamento e o encaminhamento para as áreas necessárias para o atendimento ao solicitado;
- O DPO irá responder de forma mais adequada perante a legislação específica aplicável e às boas práticas estipuladas internamente;
- As respostas somente deverão ser encaminhadas por meio do canal de comunicação definido e publicado no site da Galapagos Capital.

6.4.2. Resposta à Autoridade Fiscalizadora

- Em determinadas circunstâncias, a LGPD permite que os dados pessoais sejam divulgados às agências de aplicação da lei sem o consentimento do titular dos dados. Nestas circunstâncias, a Galapagos Capital divulgará os dados solicitados;

- Nestes casos, os colaboradores ou prestadores de serviço têm o dever de notificar o DPO, o Jurídico e o Compliance da Galapagos Capital, sem demora injustificada e sem responder à Autoridade, sobre qualquer ordem ou requisição relativa à privacidade e proteção de dados pessoais por eles recebida.

6.4.3. Resposta à Autoridade Judicial

- Os colaboradores ou prestadores de serviço têm o dever de notificar imediatamente o DPO, o Jurídico e o Compliance da Galapagos Capital sobre qualquer ordem ou determinação de autoridade judicial relativa a dados pessoais que tome conhecimento, sem responder à Autoridade, salvo se assim orientado pelo DPO, Jurídico e Compliance da Galapagos Capital;
- Quando requisitado por meio de ordem judicial, caberá ao Jurídico fornecer quaisquer esclarecimentos e entregar as informações demandadas pela Autoridade, sem demora injustificada, podendo requisitar o apoio do DPO caso entenda como necessário;
- Caso se faça necessário o acesso a dados pessoais e informações com acesso restrito ou moderado, caberá ao Jurídico e Compliance acionar o DPO e as áreas responsáveis para que estas forneçam acesso temporário (seguindo as diretrizes estabelecidas pela área de Segurança da Informação), possibilitado assim o cumprimento de ordem judicial de forma tempestiva;
- Quando a Autoridade determinar a necessidade de prestação de esclarecimentos, caberá ao Jurídico e Compliance buscar junto DPO e aos colaboradores ou prestadores de serviço que tenham envolvimento no fluxo de dados pessoais, solicitando relatórios, fazendo entrevistas, e buscando compilar o máximo de informações pertinentes para estruturar uma resposta adequada e concisa.

6.5. Inventário de Tratamento de Dados Pessoais

A Galapagos Capital irá manter um inventário de dados pessoais, incluindo, no mínimo, as seguintes informações utilizadas em cada um dos processos que os tratam:

- Descrição do fluxo da informação em cada etapa de seu ciclo de vida;
- Base legal para tratamento;
- Finalidade para o qual o dado é tratado;
- Local lógico (nuvem, servidor, laptop etc.) e geográfico onde o dado é tratado;
- Período de retenção do dado;
- Área responsável pelo dado;
- Volume aproximado de registros existentes;
- Os propósitos das atividades de tratamento;
- As categorias de dados pessoais tratados;
- Os destinatários a quem os dados pessoais foram ou serão compartilhados, incluindo destinatários e respectivo países terceiros;

- Os prazos propostos para a eliminação das diferentes categorias de dados;
- Sempre que possível, uma descrição geral das medidas técnicas e organizacionais de segurança aplicadas.

6.6. Resposta aos Incidentes de Violação de Dados Pessoais

Quando houver uma suspeita ou violação real de dados pessoais, o Comitê de TI e SI deve designar um focal para realizar uma investigação interna e tomar as medidas corretivas apropriadas em tempo hábil, de acordo com o definido no Plano de Respostas a Incidentes da Galapagos Capital.

Quando houver qualquer risco para os direitos e liberdades dos titulares de dados, a Galapagos Capital deve notificar a ANPD tão logo seja possível.

6.7. Relatório de Impacto à Proteção de Dados Pessoais

Os relatórios de impacto à proteção de dados pessoais serão conduzidos pela Galapagos Capital sempre quando a operação de tratamento de dados pessoais for passível de gerar altos riscos ao titular de dados, levando em consideração os fatores: (i) volumetria; (ii) categoria de dados pessoais envolvidos; (iii) categoria de titulares envolvidos; e (iv) atividades mapeadas com a base legal do legítimo interesse onde o titular não possua expectativa da realização da atividade.

A obrigatoriedade primária de elaboração do documento é do Encarregado (DPO) pela proteção de dados pessoais juntamente ao gestor da área, que irá desempenhar o papel de avaliar o documento preparado e elaborar um parecer final sobre a atividade de tratamento.

Via de regra, tais documentos não deverão ser publicados ou disponibilizados. Contudo, poderão ser objeto de requisição da ANPD, a qualquer tempo.

7. VIOLAÇÃO À POLÍTICA

O descumprimento desta política acarretará a aplicação das penalidades disciplinares previamente definidas de acordo com os procedimentos internos da Galapagos Capital e com a legislação vigente, a todos os envolvidos.

Para os casos em que tenha envolvimento de pessoas externas, cabe à Galapagos Capital definir os procedimentos legais cabíveis de acordo com a legislação aplicável.

8. HISTÓRICO

Data	Responsável	Aprovação	Motivo
13/02/2023	Keysson Sabino (Gerente de Governança de TI)	Aprovado pelo Comitê de TI e SI em 14/04/2023	Elaboração do documento