POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Política de Privacidade e Proteção de Dados Pessoais

1. OBJETIVO

Esta Política estabelece as orientações gerais para a proteção de dados pessoais dentro do ambiente corporativo da Atvos Bioenergia S.A. e todas as suas Sociedades Controladas no Brasil e no exterior ("**Atvos Bio**" ou "**Companhia**"), uma vez que na execução de suas operações coleta, manuseia e armazena informações que podem estar relacionadas a pessoas físicas identificadas e/ou identificáveis ("**Dados Pessoais**"), com vistas a:

- Estar em conformidade com as leis e regulamentações aplicáveis de proteção de Dados Pessoais e seguir as melhores práticas;
- Proteger os direitos dos Integrantes, clientes, fornecedores e parceiros contra os riscos de violações de Dados Pessoais;
- Ser transparente com relação aos procedimentos da Companhia e das Sociedades Controladas no Tratamento de Dados Pessoais; e
- Promover a conscientização em toda a Companhia e nas Sociedades Controladas em relação à proteção de Dados Pessoais e questões de privacidade.

2. DEFINIÇÕES

Os termos utilizados nesta Política têm os significados definidos abaixo. Tais termos definidos serão utilizados, conforme apropriado e aplicável, na sua forma singular ou plural, no gênero masculino ou feminino, sem que, com isso, percam o significado que lhes é atribuído a seguir:

"**Agente de Proteção de Dados**": Os Agentes de Proteção de Dados atuarão como pontos focais do Encarregado, nos respectivos Polos Agroindustriais em que atuam, naquilo que concerne ao Tratamento de Dados Pessoais, e facilitadores de comunicação entre os Integrantes, gerindo, monitorando, planejando e implementando planos de ação que venham a ser determinados pelo Encarregado, com o objetivo de mitigar a materialização de eventuais riscos que tenham sido identificados, porém, com reduzido ou nenhum poder decisório.

"**Anonimização**": Processo e técnica por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Dado anonimizado não é considerado Dado Pessoal.

"**Atvos Bio**" ou "**Companhia**": Atvos Bioenergia S.A.

"**CA-Atvos**" ou "**Conselho**" ou "**Conselho de Administração**": Conselho de Administração da Atvos Bio.

"**Comitê de Conformidade**" ou "**CC**": Comitê de Conformidade, de assessoramento ao Conselho de Administração da Atvos Bio.

"**Compartilhamento**": toda comunicação, difusão, Transferência (inclusive 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.

"**Criança**": toda e qualquer pessoa natural com até 12 (doze) anos de idade incompletos.

"**Consentimento**": manifestação livre, informada e inequívoca pela qual o Titular de Dados concorda com o Tratamento de seus Dados Pessoais para uma finalidade determinada.

"**Controlador**": Pessoa jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais.

"**Dado(s) Pessoal(is)**": Qualquer informação relativa a uma pessoa singular identificada ou identificável. Considera-se identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial, por referência a um identificador, como - por exemplo - um nome, um número de identificação, dados de

localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.

"**Dado(s) Pessoal(is) Sensível(is)**": Todo Dado Pessoal que diga respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dado referente à saúde ou à vida sexual, dado genético ou biométrico.

"**Diretriz de Segurança da Informação**": Diretrizes corporativas globais da Atvos Bio sobre Segurança da Informação, quando em vigor e que podem ser alteradas periodicamente.

"**Documentação(ões) Orientadora(s)**": Documento(s) formal(is) da Atvos Bio que fornece(m) conteúdo sobre decisões, regras e orientações corporativas que são vitais para direcionar o trabalho da Atvos Bio com legitimidade, rastreabilidade e aplicabilidade e deve ser observado e praticado por um certo universo definido de Integrantes.

"**Encarregado**" ou "***Data Protection Officer ("DPO")***": A pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os Titulares de Dados e a Autoridade Nacional de Proteção de Dados (ANPD). Nos Escritórios da Organização Dinâmica da LN-Atvos, o Encarregado atuará também na condição de Agente de Proteção de Dados.

"**Incidente**": O acesso, aquisição, uso, Compartilhamento, eliminação ou qualquer outra forma de Tratamento de Dados Pessoais, proposital ou acidental, não autorizada ou ilícita, que violem a integridade, disponibilidade e confidencialidade das informações.

"**Integrante(s)**": Funcionários/empregados que trabalham na Atvos Bio e nas suas Sociedades Controladas em todos os níveis, incluindo executivos, conselheiros, diretores, estagiários e aprendizes.

"**Integrante Responsável pelo Projeto**": Integrante responsável pela elaboração de um novo Projeto que envolva o Tratamento de Dados Pessoais a ser realizado pela Atvos Bio e/ou pelas Sociedades Controladas.

"**Jurídico**": Área responsável pela gestão dos contratos celebrados entre a Companhia e Terceiros.

"**LGPD**": Legislação brasileira nº 13.709/2018, comumente conhecida como Lei Geral de Proteção de Dados Pessoais, que regula as atividades de Tratamento de Dados Pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

"**LIA**": O questionário de avaliação de legítimo interesse, com o objetivo de avaliar se o legítimo interesse pode fundamentar o Tratamento de Dados Pessoais no escopo do Projeto em concepção.

"**Líder(es)**": Os responsáveis por apoio ao empresariamento, o responsável pelo empresariamento das áreas de operações e engenharia, o responsável pela área de produção agrícola, e o responsável pelo empresariamento das áreas comercial, energia e logística, todos sob a liderança da LN Atvos.

"**LN Atvos**": Líder de Negócio da Atvos Bio.

"**Operador**": Pessoa natural ou jurídica, de direito público ou privado, que realiza o Tratamento de Dados Pessoais em nome do Controlador.

"**Pessoas e Organização**": Área responsável pela gestão dos Integrantes da Companhia e suas Sociedades Controladas.

"**Política**": essa Política de Privacidade e Proteção de Dados Pessoais da Atvos Bio.

"**Polo Agroindustrial**": um ou mais unidades agroindustriais, cuja gestão é delegada para um Superintendente (SU) na condição de parceiro do responsável pelo empresariamento das áreas de Operações e Engenharia.

"**Projeto**"**:** O desenvolvimento ou alterações significativas de quaisquer produtos, práticas de negócio, sistemas ou serviços da Atvos Bio e/ou de suas Sociedades Controladas.

"**Pseudonimização**": Processos e técnicas por meio dos quais um dado tem sua possibilidade de associação dificultada. O dado Pseudonimizado é considerado Dado Pessoal tendo em vista a possibilidade de associação desse dado a uma pessoa natural.

"**Relatório de Impacto à Proteção de Dados Pessoais**" ou "**RIPD**": A documentação do Controlador, conforme estabelecida pela LGPD, 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.

"**Relatório de Proteção de Dados Pessoais de Novos Projetos**": A documentação do Controlador referente a a cada novo Projeto a ser realizado pela Atvos Bio e/ou pelas Sociedades Controladas, a fim de se identificar a sua sensibilidade, utilizando-se dos parâmetros descritos na tabela do **Anexo 6.10**.

"**Riscos e Conformidade**" ou "**Área de Riscos e Conformidade**": Área responsável por Riscos e Conformidade da Companhia e de suas Sociedades Controladas.

"**R-Riscos e Conformidade**": Responsável pelo Programa de Ação de Riscos e Conformidade da Companhia sob a liderança do Comitê de Conformidade.

"**Tecnologia da Informação**" ou "**TI**": Área responsável por proteger a integridade, disponibilidade e confidencialidade dos sistemas de TI e deve implementar as medidas adequadas para alcançar este objetivo, sendo o apoio técnico do R-Riscos e Conformidade e responsável pelas questões relacionadas às medidas técnicas e administrativas.

"**Sociedade(s) Controlada(s)**": Sociedades nas quais a Atvos Bio, diretamente ou por meio de outras Sociedades Controladas, detêm direitos que lhe asseguram, de forma permanente, a prevalência nas deliberações societárias e o poder de eleger a maioria dos administradores ou conselheiros.

"**Terceiro(s)**" ou "**Parceiro(s)**": Qualquer pessoa, física ou jurídica, que atue em nome, no interesse ou para o benefício da Atvos Bio ou de suas Sociedades Controladas, preste serviços ou forneça outros bens, assim como Parceiros comerciais que prestem serviços à Atvos Bio e/ou às suas Sociedades Controladas, diretamente relacionados à obtenção, retenção ou facilitação de negócios, ou para a condução de assuntos da Atvos Bio e/ou de suas Sociedades Controladas, incluindo, sem limitação, quaisquer distribuidores, agentes, corretores, despachantes, intermediários, Parceiros de cadeia de suprimentos, consultores, revendedores, contratados e outros prestadores de serviços profissionais.

"**Titular(es) de Dados**": Pessoa natural singular identificada ou identificável a quem se refere um Dado Pessoal específico, integrante ou não da Atvos Bio ou de suas Controladas.

"**Tratamento de Dados Pessoais** " ou "**Tratamento**": Qualquer operação ou conjunto de operações efetuadas sobre Dados Pessoais ou sobre conjuntos de Dados Pessoais, por meios automatizados ou não automatizados, tais como a coleta, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

"**Transferência Internacional**": A operação de uso Compartilhado de Dados com Controladores ou Operadores que se encontram fora do território nacional, inclusive por meio da utilização de servidores localizados no exterior.

3. ABRANGÊNCIA

Esta Política é aplicável à Atvos Bio e a todas as suas Sociedades Controladas, tanto no Brasil quanto no exterior, e a todos os Integrantes que tenham acesso a quaisquer Dados Pessoais Tratados pela Atvos Bio, pelas suas Sociedades Controladas ou em seus nomes.

4. REFERÊNCIAS

- Código de Conduta da Atvos Bio;
- Lei Geral de Proteção de Dados Pessoais ("**LGPD**");
- Regulações vigentes relativas à proteção de dados pessoais.

5. ATRIBUIÇÕES E RESPONSABILIDADES

Conselho de Administração ("CA-Atvos" ou "Conselho")

- Aprovar esta Política e suas futuras alterações; e
- Responsabilizar-se pelo uso adequado de Dados Pessoais em suas atividades.

Comitê de Conformidade ("CC")

- Revisar e recomendar a aprovação desta Política e suas alterações ao CA-Atvos;
- Responsabilizar-se pelo uso adequado de Dados Pessoais em suas atividades;
- Revisar anualmente, ou em prazo menor quando necessário, as iniciativas de privacidade adotadas pela Companhia e pelas Sociedades Controladas;
- Promover o conhecimento adequado dos principais *stakeholders* em relação à importância da proteção de Dados Pessoais e das atividades internas inerentes as iniciativas de privacidade;
- Discutir e tomar decisões técnicas sobre novas atividades de Tratamento de Dados Pessoais, com base nos relatórios de impacto à proteção de Dados Pessoais, quando cabível;
- Decidir sobre as medidas técnicas a serem aplicadas para Tratamentos de Dados Pessoais de risco crítico, assim como as medidas disciplinares cabíveis, em caso de descumprimento das regras dispostas nesta Política;
- Reportar ao CA-Atvos os eventos relacionados a Incidentes de Segurança que envolvam Dados Pessoais e as suas decisões;
- Definir e aprovar a estrutura de governança para os assuntos de privacidade e proteção de dados;
- Fazer o monitoramento permanente e efetivo da implementação das iniciativas de privacidade, incluindo os eventos relacionados a Incidentes de Segurança envolvendo Dados Pessoais;
- Garantir que no orçamento da Área de Riscos e Conformidade, a ser aprovado anualmente pelo CA-Atvos, estejam previstos os recursos necessários para a implementação e gerenciamento das iniciativas de privacidade;
- Examinar, com imparcialidade, as ocorrências que lhes forem apresentadas;
- Emitir parecer para o CA-Atvos, periodicamente, sobre os resultados do programa de privacidade e proteção de dados da Atvos;
- Avaliar os Projetos relativos à gestão de mudanças (de processos, físicas ou sistêmicas), que envolvam o Tratamento de Dados Pessoais cujos riscos tenham sido mensurados como "crítico", recomendar medidas mitigadoras de riscos e decidir pela continuidade ou não destes Projetos; e
- Fazer o monitoramento permanente e efetivo da implementação das iniciativas de privacidade e proteção de Dados Pessoais da Atvos Bio, incluindo os eventos relacionados a vazamento de Dados Pessoais.

R-Riscos e Conformidade

- Propor ao CC a revisão e atualização desta Política;
- Responsabilizar-se pelo uso adequado de Dados Pessoais em suas atividades;
- Garantir que a Atvos Bio e suas Sociedades Controladas estejam em conformidade com as leis e regulamentos relacionados à privacidade e proteção de Dados Pessoais, bem como com suas políticas e procedimentos internos relacionados ao tema;
- Liderar, coordenar e supervisionar a estratégia de proteção de Dados Pessoais e orientar na implementação das medidas requeridas para estar em conformidade com os requisitos da legislação e da regulação aplicáveis de proteção de Dados Pessoais;

- Participar e orientar, sob a ótica de privacidade, os projetos corporativos que envolvam Tratamento de Dados Pessoais a fim de validar a aderência aos requisitos da legislação e da regulação aplicáveis, além de garantir privacidade como um padrão a ser adotado e a incorporação no desenho das medidas de segurança necessárias;
- Realizar treinamentos, programas de conscientização e comunicação do tema de privacidade e proteção de Dados Pessoais em toda a Companhia e nas Sociedades Controladas;
- Elaborar e manter atualizada a documentação orientadora relativa à privacidade que estejam na sua competência;
- Monitorar o cumprimento das regras internas de privacidade;
- Coordenar a execução de análise de impacto de privacidade de Dados Pessoais;
- Apoiar administrativamente o Encarregado e os Agentes de Proteção de Dados nos treinamentos, campanhas de conscientização, comunicação interna, etc.;
- Definir, revisar e atualizar os avisos de privacidade (meios utilizados para garantir a transparência aos Titulares de Dados);
- Conduzir periodicamente avaliações de maturidade da Companhia em relação às iniciativas de privacidade, identificando melhorias assim como a sua evolução;
- Acompanhar e apoiar a implementação dos planos de ação para correção de *gaps* das iniciativas de privacidade;
- Garantir a manutenção das evidências de execução e implementação das iniciativas de privacidade, atendendo ao princípio da responsabilização;
- Reportar ao CC as preocupações relacionadas à implementação das iniciativas de privacidade;
- Aprovar as Documentações Orientadoras de Proteção de Dados Pessoais que estejam na sua competência, alinhados com esta Política;
- Avaliar os Projetos relativos à gestão de mudanças (de processos, físicas ou sistêmicas), que envolvam o Tratamento de Dados Pessoais cujos riscos tenham sido mensurados como "alto", recomendar medidas mitigadoras de riscos e decidir pela continuidade ou não destes Projetos; e
- Reportar ao CC os eventos relacionados a vazamento de Dados Pessoais e as suas decisões.

Encarregado:

- Responsabilizar-se pelo uso adequado de Dados Pessoais em suas atividades;
- Cooperar e se relacionar com a Autoridade Nacional de Proteção de Dados Pessoais;
- Garantir a gestão eficiente do Consentimento, por meio de revisões periódicas do seu uso e registro, das Bases Legais que autorizam o Tratamento de Dados Pessoais e da implementação das medidas técnicas e organizacionais cabíveis;
- Endereçar as solicitações dos Titulares de Dados de acordo com a legislação e regulação vigente no Brasil e com a Documentação Orientadora da Companhia;
- Analisar situações em que os Dados Pessoais de Crianças poderão ser manuseados sem o Consentimento de um dos pais ou responsável legal;
- Manter registro atualizado das operações de Tratamento de Dados Pessoais, contemplando a respectiva base legal;
- Realizar o acompanhamento e monitoramento periódico das operações de Tratamento, tomando as medidas necessárias para mitigar eventuais riscos identificados;
- Aprovar todas as formatações ou *scritps*, cujo objetivo seja informar os Titulares de Dados acerca do Tratamento de seus Dados;
- Avaliar os Projetos relativos à gestão de mudanças (de processos, físicas ou sistêmicas), que envolvam o Tratamento de Dados Pessoais cujos riscos tenham sido mensurados como "intermediário", recomendar medidas mitigadoras de riscos e decidir pela continuidade ou não destes Projetos;
- Elaborar parecer a respeito do Relatório de Proteção de Dados Pessoais de Novos Projetos, quando cabível, e submeter os novos Projetos e/ou atualização de Projetos para aprovação do Comitê de Conformidade, nos casos de operações com níveis de sensibilidade alta ou crítica;
- Elaborar, com o apoio das demais áreas da Companhia, o RIPDs, quando necessário; e
- Aprovar a concepção de novos Projetos, quando considerados de sensibilidade intermediária, mediante parecer devidamente fundamentado no Relatório de Proteção de Dados Pessoais de Novos Projetos, e no LIA, quando aplicável.

Agente de Proteção de Dados

- Orientar o uso adequado de Dados Pessoais nos Polos Agroindustriais;
- Participar e orientar, sob a ótica de privacidade, os Projetos dos Polos Agroindustrais que envolvam Tratamento de Dados Pessoais a fim de validar a aderência aos requisitos da legislação e da regulamentação aplicáveis, além de garantir privacidade como um padrão e a incorporação no desenho das medidas de segurança necessárias;
- Auxiliar operacionalmente o monitoramento do cumprimento das regras internas e manutenção de KPIs (*Key Performance Indicator*) relacionados à proteção de dados e privacidade;
- Auxiliar na condução periódica de avaliações nos Polos Agroindustriais acerca da maturidade sobre as iniciativas de privacidade, identificando a evolução do programa e os *gaps* remanescentes e/ou novos;
- Apoiar no acompanhamento e na implementação dos planos de ação para correção de *gaps* das iniciativas de privacidade nos Polos Agroindustriais;
- Apoiar no preparo dos RIPDs e dos Relatórios de Proteção de Dados Pessoais de Novos Projetos no âmbito dos Polos Agroindustriais;
- Monitorar as requisições dos Titulares de Dados no âmbito dos Polos Agroindustriais, a fim de garantir que sejam respondidas dentro do prazo;
- Garantir a manutenção das evidências de execução e implementação das iniciativas de privacidade no âmbito dos Polos Agroindustriais (princípio da responsabilização);
- Coordenar as atividades e consultas com o Encarregado;
- Facilitar a comunicação entre os Integrantes da Companhia e suas Sociedades Controladas que atuam em seus Polos Agroindustriais e o Encarregado;
- Facilitar a coleta de evidências sobre a aplicação das regras internas de privacidade e proteção de Dados Pessoais; e
- Disseminar a cultura de privacidade e proteção de Dados Pessoais nos Polos Agroindustriais.

Tecnologia da Informação ("TI")

- Responsabilizar-se pelo uso adequado de Dados Pessoais em suas atividades;
- Analisar Incidentes de Segurança que envolvam Dados Pessoais, bem como efetuar a coleta de evidências técnicas;
- Monitorar e implementar medidas de segurança para garantir o cumprimento da legislação e da regulação aplicáveis;
- Publicar avisos de privacidade em *websites* e plataformas externas;
- Revisar e manter atualizada a Documentação Orientadora relativa à Tecnologia da Informação que estejam na sua competência;
- Definir procedimento e *templates* para a formalização de Incidentes de Dados Pessoais;
- Implementar mecanismos para garantir os direitos dos Titulares de Dados, quando solicitado pelo Encarregado e pelo R-Riscos e Conformidade;
- Prestar suporte técnico e analisar novas ferramentas e sistemas com foco na proteção de Dados Pessoais; e
- Garantir a aplicação das medidas de segurança proporcionais ao risco gerado pelo Tratamento de Dados Pessoais e em linha com a expectativa de proteção do Titular de Dados, garantindo a integridade, disponibilidade e confidencialidade destas informações.

Área Jurídica

- Responsabilizar-se pelo uso adequado de Dados Pessoais em suas atividades;
- Apoiar as demais áreas para que os contratos que contemplem o Compartilhamento ou o Tratamento de Dados Pessoais contenham cláusulas de privacidade adequadas à legislação e regulação aplicáveis;
- Prestar apoio jurídico, na ocorrência de Incidentes de Segurança que envolvam de Dados Pessoais;
- Prestar apoio jurídico na interpretação da legislação e regulação relativas à proteção de Dados Pessoais;

- Apoiar na renegociação de contratos/aditivos com fornecedores e clientes que realizam o Tratamento de Dados Pessoais; e
- Apoiar o Encarregado na interface com Autoridades Nacionais de Dados Pessoais.

Líderes

- Responsabilizar-se pelo uso adequado de Dados Pessoais nas atividades de suas respectivas áreas;
- Garantir, no âmbito de suas respectivas áreas, que os requisitos da legislação e regulação aplicáveis no local de atuação sejam atendidos, bem como que os seus liderados atuem de acordo com esta Política;
- Apoiar, no âmbito de suas respectivas áreas, no preparo dos RIPDs e dos Relatórios de Proteção de Dados Pessoais de Novos Projetos;
- Revisar e manter atualizado o mapeamento de Dados Pessoais realizado por suas respectivas áreas, pelo menos uma vez por ano (ou sempre em caso de mudanças substanciais), com o apoio da Área de Riscos e Conformidade; e
- Garantir, no âmbito de suas respectivas áreas, que, ao usar Consentimento para o Tratamento de Dados Pessoais, que este seja coletado e gerenciado de forma que a opção dada pelo Titular de Dados seja respeitada e que gere evidências necessárias para apresentação às autoridades ou ao próprio Titular de Dados, quando necessário.

Todos os Integrantes da Companhia, incluindo os Líderes

- Responsabilizar-se pelo uso adequado de Dados Pessoais em suas atividades;
- Cumprir a legislação e regulação aplicáveis, bem como Documentação Orientadora da Companhia relativos à proteção de Dados Pessoais e aplicação das medidas adequadas de segurança de TI;
- Relatar para o Encarregado a ocorrência de quaisquer Incidentes de Dados Pessoais ou segurança de dados, bem como as deficiências identificadas relacionadas ou possíveis riscos de privacidade;
- Elaborar um Relatório de Proteção de Dados Pessoais de Novos Projetos, quando cabível; e
- Participar das atividades de treinamento em proteção de dados, conforme orientado.

Auditoria Interna

- Responsabilizar-se pelo uso adequado de Dados Pessoais em suas atividades; e
- Incluir avaliação de aderência à Documentação Orientadora que versa sobre proteção de Dados Pessoais nos projetos de auditoria e reportar ao R-Riscos e Conformidade e ao CC o resultado dessas avaliações.

6. POLÍTICA

6.1. Princípios de Proteção de Dados Pessoais

Esta seção descreve os princípios que devem ser observados na coleta, manuseio, armazenamento, divulgação, Compartilhamento e quaisquer outras formas de Tratamento de Dados Pessoais pela Companhia e pelas Sociedades Controladas para atender aos padrões de proteção de dados no âmbito corporativo e estar em conformidade com a legislação e regulação aplicáveis no Brasil.

6.1.1. Boa-fé e Não Discriminação

A Companhia deve tratar os Dados Pessoais de forma justa, ética, transparente e em conformidade com legislação e regulação aplicáveis.

Além disso, os Dados Pessoais sob tutela da Atvos Bio e das suas Sociedades Controladas não devem ser tratados para finalidades que se prestem a discriminação de seus Titulares.

6.1.2. Limitação da Finalidade

O Tratamento de Dados Pessoais deve ser realizado de maneira compatível com a finalidade original para a qual os Dados Pessoais foram coletados, não podendo ser coletados com um propósito e utilizados para outro. Quaisquer outras finalidades devem ser compatíveis com a razão original para qual os Dados Pessoais foram coletados.

6.1.3. Necessidade e Adequação

A Companhia somente pode tratar Dados Pessoais na medida em que seja necessário para atingir um propósito específico, devendo estes Dados Pessoais serem proporcionais, adequados e não excessivos para tanto. O Compartilhamento de Dados Pessoais com outra área ou outra empresa deve considerar, em especial este princípio.

6.1.4. Livre Acesso e Transparência

A Companhia deve fornecer aos Titulares uma consulta facilitada e gratuita sobre as informações do Tratamento realizado com seus Dados Pessoais, garantindo uma relação transparente a respeito dos Dados Pessoais que são tratados, a forma e a duração do Tratamento.

6.1.5. Precisão e Qualidade dos Dados

A Companhia deve adotar medidas razoáveis para assegurar que quaisquer Dados Pessoais em sua posse sejam mantidos precisos e atualizados em relação às finalidades para as quais foram coletados, sendo certo que deve ser possibilitado ao Titular de Dados de requerer a correção de dados imprecisos ou desatualizados.

6.1.6. Prevenção e Segurança

A Companhia deve assegurar que medidas técnicas e administrativas apropriadas sejam aplicadas aos Dados Pessoais para protegê-los contra o Tratamento não autorizado ou ilegal, de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. O Tratamento de Dados Pessoais também deve garantir a devida confidencialidade. Dentre as medidas técnicas mais comuns, podem ser descritas:

- **Anonimização** significa que os Dados Pessoais são tornados anônimos de tal forma que os dados não mais se referem a uma pessoa direta ou indiretamente identificável. O anonimato tem que ser irreversível.

- **Pseudonimização** é um processo pelo qual os Dados Pessoais não mais se relacionam diretamente com uma pessoa identificável (por exemplo, mencionando seu nome), mas não é anônimo, porque ainda é possível, com informações adicionais, que são mantidas separadamente, identificar uma pessoa.

6.1.7. Responsabilização e prestação de contas

A Companhia é responsável e deve demonstrar o cumprimento desta Política, assegurando a geração de evidências e seu posterior armazenamento, relativas às obrigações dispostas neste documento, que incluem, mas não se limitam a:

- Garantia de que os Titulares de Dados possam exercer os seus direitos conforme descritos na Seção 6.7 desta Política;
- Registros de atividades de Tratamento de Dados Pessoais, com a descrição dos propósitos/finalidades desse Tratamento, os destinatários do Compartilhamento dos Dados Pessoais e os prazos pelos quais a Companhia deve retê-los;
- Registro de Incidentes de Dados Pessoais e violações de Dados Pessoais;
- Garantia de que os Terceiros que sejam Operadores de Dados Pessoais também estejam agindo de acordo com esta Política e com a legislação e regulamentação aplicáveis;
- Garantia de que a Companhia, quando requerida, registre as informações solicitadas junto à Autoridade de Proteção de Dados; e
- Garantia de que a Companhia esteja cumprindo com todas as exigências e solicitações da Autoridade de Proteção de Dados.

6.2. Padrões de Segurança

6.2.1. Importância da Proteção de Dados Pessoais

A Companhia está comprometida com a implementação dos padrões de Segurança da Informação e com a proteção de Dados Pessoais com vistas a garantir o direito fundamental do indivíduo à autodeterminação da informação e à privacidade.

6.2.2. Garantir a Segurança dos Dados Pessoais

A confidencialidade, integridade e disponibilidade, bem como autenticidade, responsabilidade e não-repúdio são objetivos a serem perseguidos para a segurança dos Dados Pessoais.

6.2.3. Obrigação de Sigilo e Confidencialidade

Todos os Integrantes com acesso a Dados Pessoais estão obrigados aos deveres de sigilo e confidencialidade dos Dados Pessoais, mediante a anuência ao Código de Conduta e aos Termos de Uso da Atvos Bio, quando do ingresso na Companhia ou nas Sociedades Controladas, e, periodicamente, quando necessário.

6.2.4. Privacidade e Proteção de Dados Pessoais por Concepção e por Padrão

Ao implementar novos processos, procedimentos ou sistemas que envolvam o Tratamento de Dados Pessoais, a Companhia deve adotar medidas para garantir que as regras de Segurança, Privacidade e Proteção de Dados sejam adotadas desde a fase de concepção até o lançamento/implantação destes Projetos.

6.3. Hipóteses Autorizadoras de Tratamento de Dados Pessoais

A Companhia somente tratará Dados Pessoais quando o propósito/finalidade do Tratamento tiver fundamento uma das hipóteses legais permitidas, abaixo elencadas, sendo certo que os Titulares de Dados devem ser informados sobre a razão e a forma pela qual seus Dados Pessoais estão sendo tratados anteriormente ou durante a coleta:

- **Cumprimento de Obrigação Legal ou Regulatória**: existência de lei, norma, decisão judicial ou regulação vigente, pela qual o Tratamento de Dados Pessoais se torna obrigatório para a Companhia e para as Sociedades Controladas;
- **Execução de Contrato ou Procedimentos preliminares:** necessidade para a execução de um contrato do qual o Titular de Dados é parte;
- **Exercício Regular de Direitos:** quando o Tratamento de Dados Pessoais for necessário para prover os direitos da Companhia e/ou das Sociedades Controladas em processo judicial, administrativo ou arbitral;
- **Tutela da Saúde:** para garantir a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, inclusive para garantia da segurança sanitária do ambiente de trabalho da Atvos Bio, suas Sociedades Controladas e seus Polos Agroindustriais, sendo vedado qualquer outro uso que desvirtue essa finalidade;
- **Proteção da Vida ou Incolumidade Física:** para garantir a proteção da vida ou incolumidade física do Titular de Dados ou de Terceiros, quando em iminente perigo;
- **Proteção ao Crédito:** para garantir a proteção ao crédito, em análises feitas ao perfil dos Titulares de Dados, observando-se a legislação vigente (como a Lei do Cadastro Positivo e o Código de Defesa do Consumidor).
- **Legítimo Interesse:** para garantir a continuidade da atividade econômica/operação da Companhia e/ou das Sociedades Controladas, desde que o Titular dos Dados tenha expectativa quanto à atividade de Tratamento de Dados Pessoais. Esta base legal não se aplica para Dados Pessoais Sensíveis; e
- **Consentimento:** a coleta de Consentimento do Titular de Dados pode ser utilizada para embasar qualquer atividade de Tratamento de Dados Pessoais, devendo-se a Companhia e as Sociedades Controladas assegurar que este seja obtido de forma livre, inequívoca e informada. A Companhia e as Sociedades Controladas devem coletar, armazenar e gerenciar todas as respostas de Consentimento de maneira organizada e acessível, para que a comprovação de Consentimento possa ser fornecida quando necessário.

Em algumas circunstâncias a Companhia também poderá tratar Dados Pessoais Sensíveis. Nesse caso, deverão ser observados padrões de segurança mais robustos do que os empregados no tratamento dos demais Dados Pessoais:

- Quando for necessário para o cumprimento de obrigação legal ou regulatória, pela qual o Tratamento se torna obrigatório (e não opcional), como, por exemplo, o cumprimento de obrigações em matéria de emprego, previdência social e proteção social;
- Para garantir a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, inclusive para garantia da segurança sanitária do ambiente de trabalho da Atvos Bio, suas Sociedades Controladas e seus Polos Agroindustriais, sendo vedado qualquer outro uso que desvirtue essa finalidade;
- Para proteção à vida ou à incolumidade física do Titular de Dados, incluindo Compartilhamento de dados médicos com fins preventivos e ocupacional; e
- Quando o Titular de Dados tiver dado o seu Consentimento livre, informado e inequívoco, de acordo com a legislação e regulamentação aplicáveis, como, por exemplo, para fins de promoção ou manutenção de igualdade de oportunidades entre pessoas de origem racial ou étnica diferente.

Ainda, Dados Pessoais Sensíveis poderão ser tratados nas seguintes hipóteses:

- Quando o tratamento se fizer necessário para a **Prevenção à Fraudes e à Segurança do Titular**, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos;
- Quando o tratamento se fizer indispensável para o **Exercício Regular de Direitos, inclusive em contratos**, como, por exemplo, para defesa ou proposição de ações judiciais ou administrativas ou arbitrais, em decorrência de um contrato, ainda que não esteja explicitamente previsto no respectivo instrumento contratual.

6.4. Tratamento de Dados Pessoais de Crianças

Em decorrência da vulnerabilidade de Crianças, o Tratamento de Dados Pessoais destes indivíduos deverá visar o seu melhor interesse, ou seja, com a finalidade de beneficiá-los, ainda que de forma indireta.

Adicionalmente, o Tratamento de Dados Pessoais de Crianças necessitará, em regra, da prévia coleta do Consentimento específico e destacado, de pelo menos um dos pais ou responsáveis legais.

6.5. Política de Transferência Internacional de Dados Pessoais

Quando os Dados Pessoais forem compartilhados com outros países, a Companhia deve garantir a existência e atualização de contratos de Transferência Internacional de Dados Pessoais.

Em caso de Transferência Internacional de Dados Pessoais, as regras dispostas no **Anexo 6.10** deverão ser observadas.

Quando Dados Pessoais coletados em outros países forem tratados no Brasil, a legislação e regulamentação aplicáveis ao tratamento de Dados Pessoais de cada país deve ser observada.

6.6. Retenção e limitação do Armazenamento de Dados Pessoais

A Companhia deve ter conhecimento de suas atividades de Tratamento e estabelecer períodos de retenção para os Dados Pessoais, não podendo mantê-los por prazo superior ao necessário para atender às finalidades pretendidas.

O armazenamento dos Dados Pessoais deve ser submetido à revisão periódica para verificar a observância dos prazos de retenção previamente estabelecidos.

6.7. Direitos dos Titulares de Dados Pessoais

Observadas as normas e procedimentos internos da Atvos Bio, a Companhia está comprometida com os direitos dos Titulares de Dados, os quais incluem:

- **Confirmação de Existência de Tratamento de Dados Pessoais:** direito de obter informação se os Dados Pessoais são tratados pela Atvos Bio e pelas Sociedades Controladas;
- **Acesso aos Dados Pessoais:** direito de obter cópia/acesso aos Dados Pessoais tratados pela Atvos Bio e pelas Sociedades Controladas;
- **Correção de Dados Pessoais**: direito do Titular de Dados de solicitar a correção dos seus Dados Pessoais, caso esses estejam imprecisos, incorretos ou incompletos;
- **Anonimização, Bloqueio ou Exclusão**: direito de o Titular de Dados solicitar a exclusão, bloqueio e/ou anonimização dos Dados Pessoais, caso estes estejam sendo tratados em desconformidade com a LGPD ou de forma excessiva e desnecessária;
- **Oposição ao Tratamento de Dados Pessoais:** direito de o Titular de Dados solicitar a restrição/interrupção do Tratamento de seus Dados Pessoais, em determinadas circunstâncias;
- **Possibilidade de não Fornecer o Consentimento**: direito de o Titular de Dados não fornecer o seu Consentimento para o Tratamento de Dados Pessoais, quando este for necessário para o Tratamento. Nesses casos, as consequências do não fornecimento de Consentimento deverão ser informadas ao Titular de Dados;
- **Revogação do Consentimento**: direito do Titular de Dados de solicitar a retirada/retirar o Consentimento a qualquer momento, se o Tratamento dos Dados Pessoais se basear no Consentimento do indivíduo;
- **Eliminação de Dados**: direito de solicitar a eliminação de Dados Pessoais que sejam tratados exclusivamente com base no Consentimento;
- **Portabilidade:** direito de o Titular de Dados solicitar a portabilidade dos Dados Pessoais a outro fornecedor de serviço ou produto semelhante, mediante sua requisição expressa;
- **Informações de Dados Compartilhados:** direito de o Titular de Dados obter informação das entidades públicas e privadas com as quais a Atvos Bio e as Sociedades Controladas realizaram o Compartilhamento de Dados Pessoais; e
- **Revisão de decisões automatizadas**: direito de revisão, pelo Titular de Dados, das decisões tomadas unicamente com base em Tratamento automatizado de Dados Pessoais, que afetem os seus interesses. São exemplos dessas decisões aquelas destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito. A Atvos Bio e suas Sociedades Controladas deverão fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para tais decisões automatizadas, observados os segredos comercial e industrial.

6.8. Relatório de Impacto a Proteção de Dados

O impacto à proteção de Dados Pessoais deve ser analisado de forma a identificar e mitigar riscos em iniciativas que envolvam o Tratamento de Dados Pessoais pela Atvos Bio e pelas Sociedades Controladas, sempre que necessário, a fim de garantir a privacidade dos Titulares de Dados e a garantia de proteção dos Dados Pessoais.

Nas iniciativas nas quais o Tratamento de Dados Pessoais provavelmente resultará em um alto risco de danos aos direitos e liberdades dos Titulares de Dados, como por exemplo, mas não limitado, aos casos de: (i) tomada de decisão automatizada; (ii) Tratamento de Dados Pessoais Sensíveis; e (iii) Tratamento de dados com base legal em Legítimo Interesse, será necessário elaborar um RIPD.

Um RIPD também deverá ser elaborado tempestivamente sempre que solicitado pela Autoridade Nacional de Proteção de Dados Pessoais, observados os segredos comerciais da Atvos Bio e das Sociedades Controladas.

6.9. Prestadores de Serviços Terceirizados

Os prestadores de serviços terceirizados que tratem Dados Pessoais sob as instruções da Atvos Bio e de suas Sociedades Controladas estão sujeitos às obrigações impostas aos Operadores de Dados Pessoais, de acordo com a legislação e regulamentação de proteção de Dados Pessoais aplicáveis. A Companhia deve assegurar que no contrato deprestação de serviço sejam contempladas as cláusulas de privacidade que exijam que o Operador de Dados terceirizado implemente medidas de segurança, bem como controles técnicos e administrativos apropriados para garantir a confidencialidade, segurança e proteção dos Dados Pessoais e especifiquem que o Operador está autorizado a tratar Dados Pessoais apenas quando seja formalmente solicitado pela Companhia.

6.10. Compartilhamento de Dados Pessoais

Toda atividade que envolva o Compartilhamento de Dados Pessoais com Terceiros deverá ser embasada em contrato ou aditivo contratual, conforme minutas padrão elaboradas pela Área Jurídica e regras estabelecidas no **Anexo 6.10** desta Política. Os contratos com Terceiros, quando pertinente, deverão conter cláusulas que resguardem os direitos dos Titulares de Dados relativos à privacidade e proteção de Dados Pessoais, bem como os interesses da Atvos Bio e suas Sociedades Controladas.

Caso não seja possível a formalização de um contrato ou aditivo contratual (como, por exemplo, em caso de requisições de órgãos fiscalizadores ou poder judiciário), o Compartilhamento de Dados Pessoais e o fundamento legal para tal Compartilhamento deverão, obrigatoriamente, ser analisados pelo Encarregado, com apoio da Área Jurídica e, caso estes verifiquem a ausência de fundamento legal, deverão levar ao conhecimento do R-Riscos e Conformidade, o qual deverá recomendar as providências a serem implementadas pela Companhia.

6.11. Avaliação de Novos Projetos

Todo Projeto da Atvos Bio e de suas Sociedades Controladas que envolver o Tratamento de Dados Pessoais deverá ser avaliado sob o aspecto da privacidade, incluindo a fase de concepção, desenvolvimento e execução, conforme procedimentos previstos no **Anexo 6.11(a)** desta Política, sendo certo que o Integrante Responsável pelo Projeto deverá encaminhar o Relatório de Proteção de Dados de Novos Projetos e, quando cabível, o LIA, ao Encarregado, conforme templates disponibilizados no **Anexo 6.11(b),** que deverá armazená-los como evidência do cumprimento da Política de Privacidade e Proteção de Dados Pessoais e instrumento de prestação de contas da Companhia.

6.12. Gerenciamento de Incidentes de Segurança

Todos os Incidentes e potenciais que envolvam Dados Pessoais devem ser reportadas ao Encarregado, tendo em vista que a resposta adequada será fundamental para a minimização dos danos causados aos Titulares de Dados, a Atvos Bio e as suas Sociedades Controladas, conforme procedimentos descritos no **Anexo 6.12** desta Política. Todos os Integrantes devem estar cientes de sua responsabilidade pessoal de encaminhar e escalonar possíveis problemas, bem como de denunciar Incidentes ou suspeitas de Incidentes de Dados Pessoais, assim que os identificarem. No momento em que um Incidente real for descoberto, é essencial que sejam informados e formalizados de forma tempestiva.

Um Incidente de Segurança que envolva Dados Pessoais significa uma quebra de confidencialidade, integridade ou disponibilidade dos Dados Pessoais tratados pela Atvos Bio e/ou pelas Sociedades Controladas independentemente de como, quem (Integrantes, fornecedores ou Parceiros) ou onde (dentro ou fora da propriedade da Companhia e de suas Sociedades Controladas) o Incidente ocorreu.

6.13. Auditorias de Proteção de Dados

A Companhia deve garantir que existam revisões periódicas a fim de confirmar que as iniciativas de Privacidade, seu sistema, medidas, processos, precauções e outras atividades incluindo o gerenciamento de proteção de Dados Pessoais são efetivamente implementados, mantidos e estão em conformidade com a legislação e regulamentação aplicáveis.

Adicionalmente e conforme previsto na regulamentação interna da Atvos Bio e suas Sociedades Controladas, o tema deve ser avaliado com a devida periodicidade e de acordo com os riscos existentes. Caso os riscos sejam relevantes, a Auditoria Interna deverá incluir revisão independente específica no plano anual de auditoria interna.

7. DISPOSIÇÕES GERAIS

Os Integrantes são responsáveis por conhecer e compreender todos os documentos orientadores que lhes forem aplicáveis. De forma similar, os Líderes são responsáveis por garantir que todos os Integrantes de sua equipe compreendam e sigam os Documentos Orientadores aplicáveis à Companhia.

Os Integrantes que tiverem perguntas ou dúvidas a respeito desta Política, incluindo seu escopo, termos ou

obrigações, devem procurar o Encarregado, seus respectivos Líderes e, se necessário a Área de Riscos e Conformidade da Atvos Bio.

Violações de qualquer Documentação Orientadora da Companhia podem resultar em consequências graves à Atvos Bio, às Sociedades Controladas e aos Integrantes envolvidos. Portanto, a falha em cumprir esta Política ou relatar o conhecimento de violação desta Política poderá resultar em ação disciplinar para qualquer Integrante envolvido.

Nenhuma regra prevista nas documentações orientadoras da Atvos Bio, incluindo esse Documento, proibirá que Integrantes ou Terceiros possam reportar preocupações ou atividades ilegais para as autoridades reguladoras correspondentes.

CA-Atvos

Anexo 6.10

Nível de Sensibilidade

O Compartilhamento de Dados Pessoais com Terceiros deverá ser classificado de acordo com o nível de sensibilidade da operação, observando-se os critérios dispostos na tabela abaixo.

Nível de sensibilidade	Operações de Compartilhamento
Muito Baixo	O Compartilhamento envolve Dados Pessoais Anonimizados ou Pseudonimizados que não possibilitam a identificação de um Titular de Dados.
Baixo	O Compartilhamento envolve quaisquer Dados Pessoais, salvo se o Compartilhamento tiver sido classificado como de sensibilidade alta ou crítica.
Intermediário	O Compartilhamento envolve Dados Pessoais classificados como: (i) Dados Pessoais Sensíveis; (ii) Dados Pessoais de Criança e adolescente; (iii) Dados Pessoais financeiros; (iv) Dados Pessoais de comportamento.
Alto	O Compartilhamento envolve Transferência Internacional de Dados Pessoais.

Regras de Compartilhamento de Dados Pessoais

Para o Compartilhamento de Dados Pessoais, deverão ser observadas as seguintes regras mínimas, de acordo com nível de sensibilidade da operação previsto no item acima, sem prejuízo de outras regras que venham a ser estabelecidas pela Atvos Bio:

a. **Muito Baixo**: deve-se garantir contratualmente que o Terceiro manterá a Pseudonimização ou Anonimização dos Dados Pessoais compartilhados, sendo vedado o cruzamento de qualquer base de dados que resulte em identificação dos Titulares de Dados.
b. **Baixo e Intermediário**: é de responsabilidade dos Líderes realizar, pelo menos, anualmente, o acompanhamento do Compartilhamento dos Dados Pessoais com Terceiros, para garantir que todas as obrigações contratuais relativas à privacidade e proteção de dados estão sendo observadas pelos Terceiros com quem os dados tenham sido compartilhados.
c. **Alto**: deverão ser observadas as regras especiais para Compartilhamentos de sensibilidade intermediária e, adicionalmente, o Agente de Proteção de Dados e/ou os Líderes também deverão se certificar que:
    - O grau de proteção de Dados Pessoais do país destinatário tenha sido reconhecido pela Autoridade Nacional de Proteção de Dados, como adequado ao previsto na legislação brasileira vigente;
    - O Terceiro destinatário garante o cumprimento dos princípios, dos direitos do Titular de Dados e do regime de proteção de dados adotado pela legislação brasileira vigente, na forma de:
        - Cláusulas-padrão contratuais, definidas pela Autoridade Nacional de Proteção de Dados;
        - Cláusulas contratuais específicas para determinada Transferência;
        - Normas corporativas globais; e/ou
        - Selos, certificados e códigos de conduta regularmente emitidos.

Limitações do Compartilhamento

Toda a atividade de Compartilhamento de Dados Pessoais deverá observar as seguintes limitações:

a. Compartilhamento de Dados Pessoais Sensíveis de saúde: Dados Pessoais que se referem à saúde do indivíduo não podem ser compartilhados com Terceiros com finalidade de se obter vantagem econômica.
b. Compartilhamento de Dados Pessoais de Crianças: Dados Pessoais de Crianças somente poderão ser compartilhados com Terceiros mediante consentimento de um dos pais ou responsável legal.
c. Desacordo com o Programa de Governança de Dados Pessoais: qualquer Compartilhamento em desacordo com as normativas internas da Atvos Bio e suas Sociedades Controladas não poderá ser realizado.

Anexo 6.11(a)

Identificação da sensibilidade do Projeto

Um Relatório de Proteção de Dados Pessoais de Novos Projetos deverá ser preenchido pelo Integrante Responsável pelo Projeto , a cada novo Projeto, a fim de se identificar a sua sensibilidade, utilizando-se dos parâmetros descritos na tabela abaixo.

Nível de sensibilidade	Operações de Tratamento
Baixo	O Projeto envolve Dados Pessoais Anonimizados ou Pseudonimizados que não possibilitam a identificação de um Titular de Dados.
Intermediário	O Projeto envolve quaisquer Dados Pessoais, salvo se classificado como de sensibilidade alta ou crítica.
Alto	O Projeto envolve: (i) Dados Pessoais Sensíveis; (ii) Dados Pessoais de Criança e/ou adolescente; (iii) Dados Pessoais financeiros; (iv) Dados Pessoais de comportamento; (v) decisões Automatizadas, exceto se classificadas como de sensibilidade crítica.
Crítico	O Projeto envolve Transferência Internacional de Dados Pessoais (p. ex.: envio, recebimento ou armazenamento de Dados fora do Brasil) / O Projeto envolve decisões Automatizadas que usam como *input* Dados Pessoais Sensíveis.

Caso o Projeto seja classificado como de sensibilidade "alta" ou "crítica" e o Tratamento de Dados Pessoais seja fundamentado na Base Legal do Legítimo Interesse, o Integrante Responsável pelo Projeto, deverá preencher o LIA e envia-lo ao Encarregado.

O LIA tem o objetivo de avaliar se o Legítimo Interesse pode fundamentar o Tratamento de Dados Pessoais no escopo do Projeto em concepção, sopesando, de um lado, os direitos e garantias fundamentais do Titular de Dados, e de outro, a necessidade e adequação do Tratamento para o alcance da finalidade pretendida pela Atvos.

Independentemente da sensibilidade, o Integrante Responsável pelo Projeto deverá encaminhar o relatório e, quando cabível, o LIA, ao Encarregado, que deverá armazená-los como evidência da Política de Privacidade e Proteção de Dados Pessoais e instrumento de prestação de contas.

Aprovação do Projeto

O responsável pela aprovação do Projeto será determinado de acordo com o nível de sensibilidade identificado pelo Integrante Responsável pelo Projeto, conforme disposto abaixo:

Nível de sensibilidade	Responsável pela aprovação do Projeto
Baixo	Não necessita de aprovação, somente do preenchimento do RPDP e reporte ao Encarregado
Intermediário	Encarregado
Alto	R-Riscos e Conformidade
Crítico	Comitê de Conformidade

Quando o Projeto tiver sido avaliado como de sensibilidade baixa, o Integrante Responsável pelo Projeto deverá preencher o Relatório de Proteção de Dados Pessoais de Novos Projetos e encaminhá-lo ao Encarregado, comunicando-o acerca da execução do Projeto.

No caso de Projetos de sensibilidade intermediária ou alta, o Integrante Responsável pelo Projeto submeterá o referido relatório ao R-Riscos e Conformidade, quem deverá decidir pela aprovação ou não do Projeto.

Os relatórios relativos à novos Projetos de sensibilidade crítica deverão ser submetidos para avaliação e aprovação do Comitê de Conformidade.

O Encarregado, ainda poderá, a qualquer momento, e independentemente da competência para a aprovação do Projeto:

a. Submetê-lo para aprovação do Comitê de Conformidade;
b. Solicitar informações adicionais sobre o Projeto e os Dados Pessoais envolvidos; e
c. Solicitar a elaboração, pelo Integrante Responsável pelo Projeto, do RIPD.

Acompanhamento de sensibilidades do Projeto

Caso haja alguma alteração da finalidade e/ou de Dados Pessoais utilizados no desenvolvimento e/ou atualização de um Projeto, o nível de sensibilidade deverá ser reavaliado pelo Integrante Responsável pelo Projeto.

Caso a alteração da sensibilidade implique em alteração da competência para a aprovação do Projeto, este deverá ser suspenso e submetido para nova aprovação.

Anexo 6.11(b)

Relatório de Proteção de Dados Pessoais de Novos Projetos

Nome do(a) Integrante Responsável pelo Projeto:	
Nome do Projeto/Processo:	
Dados envolvidos no Projeto	
Quais dados serão utilizados no Projeto?	
A iniciativa envolve Dados Pessoais?	[ ] SIM [ ] NÃO
A iniciativa envolve Dados Pessoais Sensíveis? (e.g. religião, raça, vida sexual) Se sim, quais?	[ ] SIM [ ] NÃO
A iniciativa envolve dados financeiros? Se sim, quais?	[ ] SIM [ ] NÃO
A iniciativa envolve dados que representam/revelem segredo de negócio ou cuja divulgação pode afetar o mercado?	[ ] SIM [ ] NÃO
A iniciativa envolve dados de menores de 12 anos de idade?	[ ] SIM [ ] NÃO
Serão tratados dados de, aproximadamente, quantos Titulares?	[ ] < 100 [ ] 101 a 1.000 [ ] 1.001 a 5.000 [ ] 5.001 a 10.000 [ ] 10.001 ou mais
Origem dos Dados Pessoais	
Quais as fontes (origens) dos dados tratados?	
Há aquisição de dados por meio de Terceiros (não adquiridos diretamente por meio do Titular)?	[ ] SIM [ ] NÃO
Os dados serão colhidos de quais bancos de dados a que temos acesso? (Nomear os Terceiros que fornecerão os bancos de dados)	[ ] Base Própria: [ ] Bases Públicas: [ ] Base Privada:
Compartilhamento (envio de Dados Pessoais)	
A iniciativa envolve o envio de dados para Terceiros? Se sim, de quais?	[ ] Sim [ ] Não
Para quem os dados serão enviados?	[ ] Outra empresa do grupo: [...] [ ] Terceiros
O Compartilhamento inclui agentes fora do território brasileiro? Se sim, para quais países?	[ ] SIM [ ] NÃO

Segurança	
Quais os controles/medidas de segurança aplicadas?	
Eventuais testes de segurança são feitos em ambiente amostral e controlado?	[ ] SIM [ ] NÃO
Há Anonimização de dados?	[ ] SIM [ ] NÃO
Há Pseudonimização de dados? Se sim, quem possui a chave?	[ ] SIM [ ] NÃO
Pretende-se deletar os dados após cumprimento da finalidade ou de um período determinado?	[ ] SIM [ ] NÃO Período (se aplicável):
Decisão automatizada	
A iniciativa se utiliza de procedimentos automatizados de decisão? Se sim, quais?	
Algum dos dados envolvidos é sensível?	[ ] SIM [ ] NÃO
Há previsão de revisão das decisões?	[ ] SIM [ ] NÃO
O sistema automatizado recebe *inputs* constantes para a sua atualização e aperfeiçoamento?	[ ] SIM [ ] NÃO
Nível de Sensibilidade	
[ ] BAIXO [ ] INTERMEDIÁRIO [ ] ALTO [ ] CRÍTICO	
Base Legal autorizadora do Tratamento dos Dados Pessoais envolvidos no Projeto	
	Necessário o preenchimento do LIA? [ ] SIM [ ] NÃO

Conclusão

Integrante Responsável pelo Projeto de Dados DATA

FORMULÁRIO PARA AVALIAÇÃO DE LEGÍTIMO INTERESSE

Nome do responsável pela aprovação do projeto:
Nome do Projeto/Processo:
PARTE 1 - Teste Objetivo **(Identifica se o Legítimo Interesse é a base legal de Tratamento adequada)**
1.1 Por que você deseja tratar os dados pessoais?
1.2 Que benefício você espera obter com o Tratamento?
1.3 Algum terceiro se beneficia do Tratamento?
1.4 Qual a importância desse tratamento?
1.5 Qual seria o impacto se você não pudesse prosseguir com esse tratamento?
1.6 Qual é o resultado pretendido para os titulares de dados pessoais?
1.7 Você está cumprindo alguma legislação ou regulamentação ao realizar esse tratamento?
1.8 Existem problemas éticos com o Tratamento?
1.9 O Tratamento tem a finalidade de prevenção de fraudes?
PARTE 2 - Teste de Necessidade **(Identifica se o procedimento é necessário)**
2.1 O tratamento realmente ajudará você a atingir seu objetivo?
2.2 O tratamento é proporcional a esse objetivo?
2.3 Você pode atingir seu objetivo sem tratar todos os dados ou tratando menos dados? Caso a atividade pretendida envolva o tratamento de dados pessoais sensíveis, esses dados são indispensáveis para o alcance da finalidade pretendida?

2.4 Você pode atingir seu objetivo tratando os dados de outra maneira menos intrusiva?
PARTE 3 - Teste de Balanceamento (Avalia os interesses do Titular)
3.1 São tratados dados sensíveis?
3.2 São tratados dados relativos ao histórico criminal do titular?
3.3. São tratados dados financeiros?
3.4 A atividade envolve o tratamento de dados de crianças?
3.5 São dados sobre pessoas em sua capacidade pessoal ou profissional?
3.6 Já há um relacionamento prévio da empresa com o titular? Se sim, qual é a natureza desse relacionamento?
3.7 Você coletou dados diretamente do titular?
3.8. Essa coleta foi comunicada diretamente titular?
3.9 Se os dados foram recebidos de terceiros, o que esses terceiros disseram aos titulares sobre o compartilhamento dos dados com terceiros para outros fins?
3.10 Há quanto tempo os Dados Pessoais foram coletados? Existe alguma mudança na tecnologia ou outro contexto desde aquela época que afetaria as expectativas atuais do titular?
3.11 Você pretende fazer algo novo ou inovador com esses Dados?

3.13 Você tem alguma evidência real sobre as expectativas do titular quanto ao tratamento, por exemplo, de pesquisa de mercado, grupos focais ou outras formas de consulta?
3.14 Existem outros fatores nas circunstâncias particulares que significam que eles esperariam ou não o tratamento?

Integrante Responsável pelo Projeto DATA

O LEGÍTIMO INTERESSE PODE FUNDAMENTAR O TRATAMENTO PRETENDIDO?

Encarregado DATA

Anexo 6.12

Detecção e Verificação do Incidente

Qualquer violação de Dados Pessoais ou suspeita de ciolação que comprometa a segurança das informações pessoais em poder da Atvos Bio deve ser comunicada imediatamente por meio do canal **privacidade@atvos.com**

A equipe de Tecnologia da Informação será responsável pela detecção e monitoramento dos canais de reporte de Incidentes, ou outros que, eventualmente, possam servir para o reporte e reportar ao R-Riscos e Conformidade sempre que constatado que o Incidente envolve Dados Pessoais.

Classificação e Notificação da Violação de Dados Pessoais

Constatada a ocorrência de uma violação de Dados Pessoais, o Agente de Proteção de Dados classificará a sua criticidade, considerando o risco de dano ao Titular de Dados, conforme classificação abaixo:

Natureza do dado / Pilar de Segurança violado	**Simples**	**Comportamentais**	**Financeiros**	**Sensíveis**
Confidencialidade	O acesso não autorizado se deu somente no interior da organização	Dados foram publicados para o exterior da organização por tempo limitado	Dados replicados na *web*, com contenção custosa	Dados replicados na *web*, com contenção praticamente impossível
Integridade	Uma alteração não autorizada nos dados ocorreu somente no interior da organização	Uma alteração não autorizada nos dados capaz de gerar frustração	Uma alteração não autorizada nos dados capaz de gerar estresse e constrangimento leve	Uma alteração não autorizada nos dados capaz de gerar danos difíceis de reverter ou irreversíveis
Disponibilidade	A impossibilidade de acesso aos Dados Pessoais se deu somente no interior da organização	A impossibilidade de acesso aos Dados Pessoais gerou frustração	A impossibilidade de acesso aos Dados Pessoais gerou estresse e constrangimento leve	A impossibilidade de acesso aos Dados Pessoais gerou danos difíceis de reverter ou irreversíveis

Insignificante **Pouco significante** **Significante** **Muito significante**

A tabela acima apresenta a escala de classificação de um Incidente de violação de Dados Pessoais, de acordo com os critérios definidos. Caso critérios de diferentes escalas incidam no mesmo Incidente, a escala de maior gravidade define a sua criticidade.

Classificado o evento, de acordo com os critérios apresentados acima, o R-Riscos e Conformidade providenciará a sua notificação, conforme critérios abaixo:

Classificação	Notificação Necessária
Muito significante	Sim
Significante	Sim
Pouco significante	Não
Insignificante	Não

Caso a criticidade do Incidente seja classificada em "muito significante" ou "significante", o R-Riscos e Conformidade deverá providenciar a comunicação do Incidente aos Titulares de Dados e à Autoridade Nacional de Proteção de Dados.

Quando os integrantes da Atvos Bio e/ou suas Sociedades Controladas tiverem seus Dados Pessoais envolvidos no Incidente, a área de Pessoas e Organização deverá auxiliar o R-Riscos e Conformidade na comunicação do Incidente.

A comunicação do Incidente deverá conter os critérios abaixo, sem prejuízo da inserção de outras informações:

a. Descrição da natureza dos dados afetados.
b. Informações sobre os Titulares de Dados impactados (se clientes/parceiros/colaboradores).
c. A indicação de medidas de segurança utilizadas para a proteção dos Dados Pessoais impactados, observados os segredos comercial e industrial.
d. Os motivos da demora do envio da notificação, caso a comunicação não tenha sido imediata ao conhecimento do Incidente.
e. As medidas técnicas adotadas para cessar o Incidente e reverter ou mitigar os efeitos do prejuízo.

A notificação deve ser enviada tão logo se tenha informações confiáveis sobre o Incidente, a menos que o R-Riscos e Conformidade tenha justificativa razoável para não o fazer, mediante aprovação do Comitê de Conformidade.

Medidas para mitigação de riscos

Quando o Incidente tiver sido comunicado para a Autoridade Nacional de Proteção de Dados e para os Titulares de Dados, o R-Riscos e Conformidade deverá monitorar a repercussão do Incidente, propondo as medidas cabíveis para mitigar eventuais riscos reputacionais e financeiros à Atvos Bio e suas Sociedades Controladas.

Nesse caso, deverá contar com o apoio da área Jurídica, especialmente para a adoção de medidas judiciais e extrajudiciais de compensação de danos junto aos Titulares de Dados, e com o apoio da área de Comunicação, para monitoramento do impacto do Incidente na mídia.

Medidas pós-Incidente

Encerrada a resposta ao Incidente, o Agente de Proteção de Dados elaborará um relatório, , com o apoio da área de Tecnologia da Informação, e enviará ao R-Riscos e Conformidade, que contenha, no mínimo:

a. A causa raiz do evento.
b. Medidas adotadas para resposta ao Incidente.
c. Eventuais melhorias a serem implementadas.
d. Tempo de reação entre a descoberta do evento e o início do seu gerenciamento.
e. Notificações e comunicações efetuadas sobre o Incidente.
f. Impacto financeiro, reputacional e operacional que o Incidente tenha causado.

O R-Riscos e Conformidade deverá manter o registro dos relatórios de Incidentes em repertório centralizado, especialmente para atendimento do princípio da responsabilização e prestação de contas.