Políticas e Normas.

Segurança da Informação

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Política de Privacidade e Proteção de Dados Pessoais.

1 Princípios da Proteção de Dados Pessoais

Os princípios abaixo elencados devem ser observados na coleta, manuseio, armazenamento, divulgação e tratamento de dados pessoais pela Instituição para atender aos padrões de proteção de dados no âmbito corporativo e estar em conformidade com a legislação e regulamentação aplicáveis nos respectivos países onde tiver operação ou atividade comercial.

a) Legalidade, Transparência e Não-Discriminação

A Instituição trata os dados pessoais de forma justa, transparente e em conformidade com a legislação e regulamentação aplicáveis.

Tratamento de Dados Pessoais

A Instituição somente trata dados pessoais quando a finalidade do tratamento se enquadra em uma das hipóteses legais previstas na LGPD, que se encontram abaixo elencadas, sendo certo que os titulares devem ser sempre informados sobre a razão e a forma pela qual seus dados pessoais estão sendo tratados. São hipóteses de tratamento:

• Necessidade para a execução de um contrato do qual o titular dos dados é parte;

EMBRASI

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

• Exigência decorrente de lei ou regulamento ao qual a Instituição está sujeita;

• Interesse legítimo no tratamento dos dados; e

• Necessidade de prover o exercício regular de direito em processo judicial, administrativo ou arbitral.

Quando o tratamento de dados pessoais não se enquadrar nas hipóteses legais acima, a Instituição deve obter o consentimento do titular para o tratamento de seus dados pessoais, e assegurar que este consentimento seja obtido de forma específica, livre, inequívoca e informada, nos termos do art. 7º, inciso I da LGPD.

A Instituição deve coletar, armazenar e gerenciar todas os formulários de consentimento de maneira organizada e acessível, para que a comprovação de consentimento possa ser provada quando necessário, nos termos do caput do art. 8º da LGPD.

Da mesma forma, o titular deve ter a possibilidade de retirar o seu consentimento a qualquer momento com a mesma facilidade pela qual foi fornecido, nos termos do art. 8º, §5º da LGPD.

Tratamento de Dados Pessoais Sensíveis

Em algumas circunstâncias a Instituição também pode ser obrigada a tratar dados pessoais considerados sensíveis, tais como os abaixo elencados:

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

• Dados relacionados à saúde do titular;

• Dados genéticos ou biométricos vinculados ao titular;

• Dados acerca da orientação sexual do titular;

• Dados sobre eventuais condenações criminais do titular;

• Dados que evidenciem a origem racial ou étnica, opiniões políticas, filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

O tratamento de dados pessoais sensíveis é vedado, exceto nas hipóteses específicas descritas abaixo, conforme definido pelo art. 11 da LGPD, casos em que serão observados padrões de segurança mais robustos do que os normalmente empregados aos demais dados pessoais. São hipóteses de tratamento de dados sensíveis:

• Necessidade para a execução de um contrato do qual o titular dos Dados é parte (art. 11, inciso II, alínea “b” da LGPD); ;

• Exigência decorrente de lei ou regulamento ao qual a Instituição está sujeita (art. 11, inciso II, alínea “a” da LGPD);

• Necessidade de prover o exercício regular de direito em processo judicial, administrativo ou arbitral (art. 11, inciso II, alínea “d” da LGPD).

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

• Proteção da vida ou da incolumidade física do titular (art. 11, inciso II, alínea "f" da LGPD);

Quando o tratamento de dados pessoais não se enquadrar nas hipóteses legais acima, a Instituição deve obter, de forma específica e destacada, o consentimento do titular para o tratamento de seus dados pessoais sensíveis, e assegurar que este consentimento seja obtido de forma específica, livre, inequívoca e informada, nos termos do art. 11, inciso I da LGPD.

Tratamento de Dados Pessoais de Criança ou Adolescente

Em outras circunstâncias, a Instituição pode ser obrigada a tratar dados pessoais de crianças e adolescentes, respeitando o disposto no Estatuto da Criança e do Adolescente e de acordo com os seus melhores interesses (art. 14, *caput* da LGPD). O tratamento de dados pessoais de crianças e adolescentes só será realizado mediante o consentimento específico e em destaque dado pelo seu responsável legal (art. 14, §1º da LGPD).

b) Limitação e Adequação 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 os dados serem coletados com um propósito e utilizados para outro. Quaisquer outras

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

finalidades devem ser compatíveis com a razão original para qual os dados pessoais foram coletados.

c) Necessidade e Minimização dos Dados

A Instituição seguirá o princípio da minimização dos Dados, isto é, somente poderá tratar os dados pessoais dos titulares na medida em que sejam necessários para atingir um propósito específico e determinado. O compartilhamento de dados pessoais com outra área ou outra empresa deve considerar sempre a observação deste princípio, só podendo haver o compartilhamento sob uma hipótese legal adequada.

d) Exatidão e Qualidade dos Dados

A Instituição 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, havendo inclusive a possibilidade de o titular de dados pessoais requerer a exclusão ou correção de dados imprecisos ou desatualizados.

e) Limitação da Retenção e do Armazenamento de Dados

A Instituição deve estabelecer períodos de retenção e processos de revisão periódica no tratamento de dados pessoais, não podendo manter os dados pessoais por prazo

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

superior ao necessário para atender as finalidades pretendidas, sempre fazendo atenção aos ditames estabelecidos pela sua Política de Retenção de Dados.

f) Integridade e Confidencialidade

A Instituição deve assegurar que medidas técnicas e administrativas apropriadas sejam aplicadas aos dados pessoais para protegê-los contra o tratamento não autorizado ou ilegal, bem como contra a perda acidental, destruição ou danos. O tratamento de dados pessoais também deve garantir a devida confidencialidade.

As medidas técnicas utilizadas pela Instituição para a garantia da integridade e confidencialidade dos dados pessoais estão previstas na Política de Segurança da Informação.

g) Responsabilização e Prestação de Contas

A Instituição deve demonstrar o cumprimento desta Política, assegurando a implementação de medidas que incluem:

- Garantias de que os titulares possam exercer os seus direitos previstos nesta política;
- Registro de dados pessoais, incluindo: (i) registros de atividades de tratamento de dados pessoais, com a descrição das finalidades desse tratamento, os destinatários do compartilhamento dos dados pessoais e os prazos pelos quais a

Instituição deve retê-los; (ii) registro de incidentes de dados pessoais; e (iii) registro de violações de dados pessoais.

- Garantias 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;
- Garantias de que a Instituição, quando requerida, registre junto à autoridade regulamentar um DPO; e
- Garantias de que a Instituição esteja cumprindo todas as exigências e solicitações de qualquer autoridade regulamentar à qual esteja sujeita.

2. Diretrizes e Padrões de Segurança

A Instituição deve seguir as boas práticas de segurança da informação, com o fim de proteger a privacidade e os dados pessoais dos indivíduos e garantir o direito fundamental à autodeterminação informacional dos titulares.

A confidencialidade, integridade e disponibilidade, bem como a autenticidade, a responsabilidade e o não-repúdio são considerados fundamentos da segurança da informação.

Todos os integrantes da Instituição com acesso a dados pessoais estão obrigados aos deveres de confidencialidade, mediante a assinatura de Acordo de Confidencialidade.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Ao implementar novos processos, procedimentos ou sistemas que envolvam o tratamento de dados pessoais, a Instituição deverá adotar medidas para garantir que as regras de Privacidade e Proteção de Dados sejam adotadas desde a fase de concepção até o lançamento ou implantação destes projetos, de acordo com a Política de Desenvolvimento de Novos Produtos e Negócios.

3. Gestão das Relações Controlador-Operador de Dados Pessoais

Cada parceiro ou fornecedor que tratar dados pessoais fornecidos pela Instituição será considerado, para todos os efeitos, um Operador de dados pessoais, sendo necessária a nomeação por este parceiro ou fornecedor de um DPO responsável por garantir que estes dados pessoais estejam sendo tratados de forma correta e de acordo com a legislação e regulamentação aplicáveis.

4. Transferência Internacional de Dados Pessoais

Se os dados pessoais forem tratados em países diferentes de onde foram coletados, a legislação e regulamentação aplicáveis à transferência internacional de dados de cada país devem ser observadas, nos termos da Política de Compartilhamento de Dados Pessoais.

A Instituição garante, de acordo com o disposto na Política de Compartilhamento de Dados Pessoais, que todos os seus contratos com fornecedores celebrados a partir da

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

publicação desta política estão em conformidade com a Lei 13.709/2018, nos termos do seu art. 33.

5. Direitos dos Titulares de Dados Pessoais

A Instituição deve agir para efetivar os direitos dos titulares de dados pessoais, mediante políticas, normas e procedimentos que forneçam:

- A informação sobre como seus dados pessoais serão tratados;
- A informação, a qualquer momento, sobre o tratamento de seus dados pessoais e o acesso aos dados pessoais que a Instituição detenha sobre eles;
- A possibilidade de correção de seus dados pessoais se estiverem imprecisos, incorretos ou incompletos;
- A possibilidade de exclusão, bloqueio ou anonimização dos seus dados pessoais em determinadas circunstâncias, nos termos de Política de Retenção de Dados da Instituição;
- A restrição do tratamento de seus dados pessoais em determinadas circunstâncias;
- A possibilidade de oposição ao tratamento, se o tratamento for baseado em legítimo interesse
- A possibilidade de retirada do consentimento a qualquer momento, se o tratamento dos dados pessoais se basear no consentimento do indivíduo para um propósito específico;

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

- A portabilidade dos dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa em determinadas circunstâncias;
- A possibilidade de revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais; e
- A possibilidade de apresentação de queixa à Instituição através do contato com o DPO responsável, ou através de comunicação à Autoridade de Proteção de Dados, se o titular dos dados pessoais tiver motivos para supor que qualquer um de seus direitos tenha sido violado.

6. Prestadores de Serviço Terceirizados

Os prestadores de serviços terceirizados que tratem dados pessoais sob as instruções da Instituição estão sujeitos às obrigações impostas aos Operadores de acordo com a legislação e regulamentação de proteção de dados pessoais aplicáveis, bem como às diretrizes estabelecidas nas Políticas de Compartilhamento e de Terceirização da Instituição.

A Instituição deve assegurar que no contrato de prestação de serviços terceirizados sejam contempladas as cláusulas de privacidade que exijam que a empresa terceirizada implemente medidas próprias de segurança e proteção de dados pessoais, devendo sempre estar em conformidade com a LGPD.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Nos casos em que o prestador de serviços estiver localizado fora do país em que os dados pessoais foram coletados, cláusulas contratuais padrão devem ser incluídas no contrato de proteção de dados pessoais em forma de um Anexo, para garantir que as devidas salvaguardas exigidas pela legislação e regulamentação aplicáveis sejam adequadamente implementadas.

7. Da Gestão de Incidentes de Segurança da Informação

Todos os incidentes de segurança da informação devem ser reportados ao DPO responsável, por meio das diretrizes e procedimentos previstos na Política e Plano de Resposta a Incidentes.

Todos os integrantes da Instituição devem estar cientes da sua responsabilidade pessoal perante a ocorrência de eventos e incidentes de segurança da informação, agindo para denunciar tais incidentes e eventos assim que os identificarem.

8. Auditorias de Proteção de Dados

A Instituição deve garantir que existam revisões periódicas a fim de confirmar que as iniciativas previstas nesta política, bem como seus sistemas, medidas, processos, precauções e outras salvaguardas estejam sendo efetivamente implementadas e mantidas em conformidade com a legislação e a regulamentação aplicáveis.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Adicionalmente, observando-se o previsto na Política de Auditoria Interna, 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.