POLÍTICA DE RETENÇÃO E DESCARTE DE DADOS

1. Introdução

Considerando que, a alta direção se compromete a seguir a Lei Geral de Proteção de Dados nº 13.709/18, visando tomar todas as precauções para mitigar possíveis ocorrências internas e externas, conforme o art. 5º e os incisos IV e XIV da referida Lei.

Considerando que, a presente política estabelece a conformidade com os incisos mencionados, que preveem (i) a definição de banco de dados, que é o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico e (ii) o conceito de eliminação de dados, fundado na exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Considerando que, seguir-se-á a presente política, que estabelece o descarte de documentos inativos, devendo e não se limitando a:

a) Garantir que todos os dados sensíveis e não sensíveis de pessoas físicas e jurídicas, sejam acessados somente pelos responsáveis em desempenhar o regular tratamento para seus devidos fins;

b) Agir de forma adequada para solucionar questões levantadas pelos trabalhadores, colaboradores, terceirizados e outras partes interessadas, bem como comunicar quanto às decisões tomadas e orientar quanto a política adotada, caso se aplique;

c) Realizar descarte de documentos do banco de dados tangível e intangível, como forma de não reter dados sensíveis e não sensíveis;

d) Assegurar a melhoria contínua de modo a atingir o pleno e incontestável cumprimento da Lei Geral de Proteção de Dados nº 13.709/18, realizando todas as manutenções necessárias pertinentes a esse devido fim;

e) Assegurar consonância com a Legislação Arquivística Brasileira, para a eliminação dos documentos destituídos de valor legal, comprobatório ou histórico.

2. Objetivo

Complementar a Política Interna de Proteção de Dados e Política de Segurança da Informação, definindo as diretrizes para o devido armazenamento, manuseio e descarte de informações.

3. Classificação de Registros

3.1. Registros de Negócios: informações registradas em qualquer meio, criadas ou capturadas que reflitam circunstâncias, eventos, atividades, transações ou resultados criados ou mantidos como parte da condução das atividades operacionais.

3.2. Registros de Marketing e Comunicação: informações pessoais obtidas pela organização em campanhas publicitárias, ações promocionais e pesquisas; redes sociais; e serviço de atendimento ao consumidor – SAC.

Os Registros utilizados para fins de marketing ou de pesquisa permanecerão armazenados na base apenas enquanto perdurar o interesse do titular em receber esses materiais, sendo possibilitado o *opt-out* a qualquer tempo, o qual permite a revogação do consentimento, caso esta seja a base legal que fundamente a respectiva modalidade de tratamento.

3.3. Registros de Recursos Humanos: Dados Pessoais coletados para (i) gestão do RH, como por exemplo, gerenciamento de tempo de trabalho, salários, benefícios, contribuições previdenciárias e impostos; férias, licenças, ausências; (ii) gestão de carreira, como treinamentos, avaliações, experiência profissional, mobilidade no grupo; (iii) administração do RH para comunicação corporativa, trabalho em rede social da empresa e uso de ferramentas de computador e telefonia; organogramas, serviços corporativos, planejamento e orçamentos, relatórios, pesquisa, reorganizações, aquisições e cisões; (iv) saúde ocupacional, como atestados médicos, prontuário médico, atestados de saúde ocupacional e todos os demais relacionados à saúde do empregado; (v) recrutamento e seleção, como nome, gênero, estado civil, idade, dados de contato, RG, CPF, comprovante de endereço, dados bancários, informações de função, habilidades, experiências, qualificações, referências, currículo, dados de entrevista e avaliação, notas e registros da entrevista e qualquer outra informação que o candidato disponibilize para a organização; e (vi) gestão de viagens de negócios, como informações para organização de viagens (preferências, local etc.); CNH e despesas. Alguns Dados Pessoais são retidos após o término do contrato de trabalho, estágio ou contrato de trabalho temporário para cumprir os períodos legais de armazenamento definidos pela legislação trabalhista ou tributária.

3.4. Registros de Segurança: informações coletadas para gerenciamento do acesso e permanência nas instalações como nome, RG, CPF, foto, biometria, controle de crachá, instalações por CFTV, login e senha para acesso aos sistemas de informação.

4. Definição de Termos

4.1. Anonimização: técnica que resulta do tratamento de dados pessoais a fim de lhes retirar elementos suficientes para que deixe de ser possível identificar o titular dos dados, de forma irreversível. Precisamente, os dados têm de ser tratados de forma a que já não possam ser utilizados para identificar uma pessoa singular utilizando o conjunto dos meios suscetíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por terceiros.

4.2. Dados Pessoais: qualquer informação relacionada a pessoa natural identificada ou identificável (titular dos dados), de qualquer natureza e independentemente do respectivo suporte. É considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social.

4.3. Dados Pessoais Sensíveis: dados sobre a origem racial ou étnica do seu titular, as suas opiniões políticas, as suas convicções religiosas ou filosóficas, informação genética, identificadores biométricos, vida sexual, orientação sexual ou sobre a sua saúde.

4.4. Definição de Perfis: qualquer forma de tratamento automatizado de dados pessoais consiste na utilização desses dados pessoais para, nomeadamente, incluir uma pessoa singular em determinada categoria, respeitante ao seu desempenho profissional, à sua situação econômica, saúde, preferências pessoais, interesses, comportamento, localização ou deslocações.

4.5. Encarregado da proteção de dados DPO (Data Protection Office): nomeado para ser responsável pela integridade dos dados pessoais e para atuar como canal de comunicação entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

4.6. Usuário de Dados: toda pessoa física que compartilhe um dado pessoal e/ou dado pessoal sensível.

5. Diretrizes para armazenamento, anonimização e descarte

A informação é um ativo muito importante, por isso, todos os colaboradores e prestadores de serviços devem adotar comportamento seguro ao armazenar, manusear e descartar qualquer tipo de informação, bem como devem assumir atitude proativa no que diz respeito à proteção das informações da organização. Todo o acesso à informação que não for explicitamente autorizado é proibido. Informações confidenciais não devem ser transportadas em qualquer tipo de mídia sem as devidas proteções e autorizações.

5.1. Classificação das Informações

As informações devem ser classificadas conforme a tabela abaixo:

Níveis de Classificação	**Características**
Pública	Informações que podem ou devem ser divulgadas publicamente. A divulgação deste tipo de informação não causa problemas à organização ou ao titular dos dados e parceiros, podendo ser compartilhada livremente com o público em geral, desde que seja mantida sua integridade. Será decisão da organização designar alguém ou um setor para divulgações públicas. A classificação dessa informação continua sendo uma responsabilidade do gestor.
Interna	Informações internas são aquelas divulgadas a todos os colaboradores e prestadores de serviços, seguindo os compromissos estabelecidos nas políticas de segurança da informação da organização com a confidencialidade das informações.
Reservada	Informações reservadas são aquelas restritas a um determinado grupo, área ou cargo, que necessitem conhecê-las para o desempenho de suas tarefas profissionais na organização. Exemplos: Projetos, relatórios, indicadores e outros.
Secreta / Confidencial	Informações Secretas/Confidenciais são aquelas que requerem um tratamento especial, pois cuja divulgação não autorizada ou acesso indevido pode gerar prejuízos financeiros, legais, normativos, contratuais ou na reputação, imagem ou estratégia da organização. Exemplos: informações

	privadas de pessoas, fornecedores e informações estratégicas.

5.2. Armazenamento

Todas as informações e dados de suporte físico categorizadas como confidenciais devem ser guardadas após o uso, no arquivo, serão armazenadas em caixas box lacradas e identificáveis em uma sala de acesso restrito, de forma a impedir o acesso de pessoas não autorizadas.

Todas as informações internas e confidenciais de suporte eletrônico deverão ser armazenadas em ambiente com acesso controlado e com senha, impedindo o acesso de pessoas não autorizadas, além de registro de acesso.

Todos os dados pessoais salvos na nossa base de dados devem ser fornecidos voluntariamente e conscientemente pelo usuário, deixando claro a sua utilização. Documentos, informações e dados pessoais de responsabilidade que forem armazenados em mídias móveis como Pen drive, HD, BD, DVD, CD e outros, deverão ser liberados pela área de TI e ter obrigatoriamente uma criptografia de alto nível e senha de alto nível.

Os servidores ou banco de dados que armazenam informações, dados e documentos devem possuir trilha de auditoria ativada para geração de log de acesso.

Todos os dados de autenticação devem ser armazenados para fazer recorrência. A única exceção à regra é o não armazenamento do Centro de Valorização da Vida (CVV). Somente devem ser armazenados os dados estritamente necessários, todo o resto deve ser descartado após a utilização.

5.3. Anonimização

A anonimização de dados é a prática de tratamento de dados que visa impossibilitar a identificação das pessoas relacionadas às informações. Os dados adequadamente anonimizados podem ser utilizados livremente, estando excluídos do escopo de aplicação de qualquer penalidade legal.

Neste sentido, quando a identificação do titular do dado não for essencial ou necessária para um determinado processo, tal como uma pesquisa interna ou externa, deverá ser feita a sua anonimização, a fim

de que seja impossível o seu reconhecimento, mantendo-se as informações que são necessárias para fins estatísticos, desde que não haja qualquer tipo de possibilidade de se reconhecer o titular do dado.

Poderá ser utilizado qualquer método de anonimização, desde que torne a recuperação de dados pessoais impossível.

5.4. Descarte

Mantém os dados pessoais de seus usuários armazenados em seu sistema de dados e arquivos por tempo indeterminado, exceção realizada a requisições de titulares dos dados.

Os dados pessoais deverão ser excluídos em um prazo de até 07 dias corridos, quando solicitado pelo titular do dado, desde que de acordo com as premissas de segurança e regulatórias.

Os itens de descarte deverão ser registrados sempre que possível para uma auditoria, seguindo os seguintes parâmetros:

5.4.1. Descarte via solicitação do Titular do Dado: deverá ser gerado um número de protocolo ou similar que será fornecido ao titular. Nos registros deverá conter o protocolo, data, quantidade de dados descartados e número do solicitante.

5.4.2. Troca ou Descarte do Desktop: deverá ser registrado o modelo e marca do equipamento, usuário antigo e destino do equipamento, além de registrar a data que foi executado o procedimento cabível de descarte de dados.

5.4.3. Destruição dos dados via terceiro: informar o tipo de equipamento ou documento, quantidade se aplicável, método de destruição e comprovante da destruição.

5.4.4. Descarte de dados armazenados em meios físicos: Os dados digitais e/ou documentos impressos, categorizados como confidenciais, deverão ser enviados para armazenamento no setor de arquivos, para posterior descarte.

Sempre que solicitado por um departamento e/ou pessoa o descarte de um documento, o setor de arquivo emite um checklist (Pedido de Descarte) de todo conteúdo armazenado, para que o solicitante sinalize quais conteúdos serão descartados.

Após o solicitante indicar no checklist quais documentos deverão ser descartados, este deve indicar a data e assinar o Pedido de Descarte. O responsável pelo setor de arquivos irá providenciar o descarte dos documentos e, somente após isso, irá: descrever o processo utilizado para descarte dos dados, indicar a data de descarte e assinar o Pedido de Descarte, arquivando este documento como evidência do processo de descarte.

O descarte de documentos arquivados poderá ser realizado pelo responsável do setor de arquivos, utilizando uma máquina fragmentadora de papel, destinando os resíduos posteriormente para reciclagem. Na hipótese de grande quantidade de documentos físicos a serem descartados, o processo de descarte poderá ser terceirizado, sendo destinado a empresa especializada em descarte de dados, que realiza o processo de fragmentação e posterior reciclagem, seguindo critérios ambientais para destinação final.

5.4.5. Descarte de dados armazenados em meios digitais: dispositivos que possuam informações classificadas como nível de confidencialidade elevado devem ser destruídos fisicamente ou as informações devem ser destruídas, utilizando técnicas que tornem a recuperação de dados impossível.

Documentos de baixa relevância podem utilizar processos de descarte mais simples. Documentos, informações e dados pessoais pertencentes à organização. Armazenado em mídia móvel como Pen drive, HD, BD, CD, DVD e outros, quando forem descartados, deverão ser destruídos (caso os dados não sejam de domínio público). Caso sejam dados categorizados como confidenciais, deverão preferencialmente fazer o descarte físico através dos meios citados no item 6.4.1 “Descarte de dados armazenados em meios físicos”

6. Retenção e descarte de dados pessoais

Para cada um desses cenários apresentados na seção 3, é definido a seguir o período máximo de retenção de Dados Pessoais, por categoria de Registro, descrição, bem como o formato de descarte.

6.1. Registro de Negócios

- Contato Comercial (nome; cargo; RG, CPF, endereço; país de origem, profissão, telefone; e-mail):

  Período para descarte: 10 anos

  Quando aplicável, esse período é considerado após contato inicial sem resposta, ou prontamente, no caso de revogação do consentimento ou da manifestação de desinteresse em ser contatado.

- Contratos Gerais (nome; cargo; RG, CPF, endereço; país de origem, profissão, telefone; e-mail; conta bancária; dados de cobrança):

Período para descarte: 10 anos

Período considerado após o término do contrato, quando aplicável.

- Documentos Tributários:

Período para descarte: 10 anos

Período a contar da data de emissão do documento, quando aplicável.

- Proteção do Crédito (nome; cargo; RG, CPF, endereço; país de origem, profissão, telefone; e-mail):

Período para descarte: 5 anos

Período a contar além da durante da relação comercial, quando aplicável.

6.2. Marketing e Comunicação

- Campanhas Publicitárias, Ações Promocionais, Pesquisas e redes sociais (nome, RG, CPF, endereço, país de origem, e-mail, telefone, respostas a pesquisas, dados online capturados):

Período para descarte: 20 anos

Período a contar após a última atividade ou prontamente após revogação do consentimento, quando aplicável.

- Serviços de Atendimentos (nome, telefone, e-mail, endereço e CPF):

Período para descarte: 20 anos

Quando se aplica, período considerado após o último atendimento.

- Recursos Humanos e Gestão de RH:

Período para descarte: 10 anos

Período a contar após o término do contrato de trabalho, exceto FGTS (30 anos) e Folha de Pagamento (10 anos).

- Gestão de Carreira:

Período para descarte: 15 anos

Período a contar após o término do contrato de trabalho.

- Saúde Ocupacional:

Período para descarte: 25 anos

Período a contar após o término do contrato de trabalho.

- Recrutamento e Seleção:

Período para descarte: 10 anos.

Aprovação do candidato: Durante o Contrato de Trabalho e mais 5 anos após o término.

6.3. Segurança

- Acesso às instalações físicas da organização (dados biométricos, nome, foto, RG, CPF):

Período para descarte: 30 dias.

Período a contar após o último acesso, quando aplicável.

- Acesso aos sistemas de informação da organização (login e senha)

Período para descarte: 30 dias.

Período a contar após o último acesso, quando aplicável.

7. Sanções e Punições

O descumprimento desta política e das políticas de segurança da informação poderá acarretar sanções e punições aos envolvidos.

8. Contate-nos

Poderá ser contatado o Encarregado de Proteção de Dados DPO, para prestar mais informações sobre o tratamento dos seus dados pessoais, bem como quaisquer questões relacionadas com o exercício dos direitos que lhe são atribuídos pela legislação aplicável e, em especial, os referidos na presente Política de Privacidade.

ANEXO I

PEDIDO DE DESCARTE DE DADOS PELO TITULAR

Nome do Documento	Data de arquivamento	Descartar (Sim / Não)

Motivo do pedido:
Nome do solicitante: Setor do solicitante: Data de solicitação:
_____ Assinatura do Solicitante

Descrever o processo utilizado no descarte:
Nome do responsável: Data do descarte:
_____ Assinatura do Responsável


INTUIX
SMART CERTIFICATIONS