ecovita
INCORPORADORA E CONSTRUTORA

POLÍTICA DE PROTEÇÃO DE DADOS E PRIVACIDADE

Sumário

1. GERAL

1.1. Contexto

Como parte do nosso trabalho diário, inevitavelmente nos deparamos com dados pessoais (doravante referidos como “dados”) de colaboradores internos e externos, fornecedores, clientes e terceiros. Geralmente, esses dados pessoais devem ser armazenados para cumprir nossas tarefas, analisados ou transferidos para terceiros. Esse manuseio de dados pessoais está sujeito a Lei Geral de Proteção de Dados Pessoais Brasileira nº. 13.709/2018 (LGPD) que deve ser observada no tratamento de dados pessoais de toda pessoa física identificada ou identificável.

1.2. Objetivos

O objetivo desta Política de Proteção de Dados é fornecer a todos os colaboradores internos e externos, as informações necessárias para garantir o tratamento legítimo e adequado dos dados pessoais, e garantir que todos saibam com quem entrar em contrato em caso de dúvidas, incertezas ou solicitação de outras informações.

1.3. Escopo

A Política de Proteção de Dados se aplica a todos os sócios e funcionários da **ECOVITA INCORPORADORA E CONSTRUTORA LTDA. ("ECOVITA")**.

1.4. Sanções

As violações às normas previstas na Lei Geral de Proteção de Dados Pessoais Brasileira (LGPD), são passíveis de punição com multas de até 50 milhões de Reais ou 2% (dois por cento) do faturamento bruto do último exercício do **ECOVITA**. Além disso, as autoridades podem advertir a **ECOVITA** e exigir a implementação de medidas para remediar qualquer violação, indicando prazo para a adoção de medidas corretivas. Podem ainda ser aplicadas outras sanções, tais como *(i) multa diária até o limite de 50 milhões de Reais, (ii) publicização da infração após devidamente apurada e confirmada a sua ocorrência, (iii) bloqueio dos dados pessoais a que se refere a infração até a sua regularização e (iv) eliminação dos dados pessoais a que se refere a infração.*

No caso de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito de dados pessoais, como vazamento de dados, uso indevido ou ataques cibernéticos, poderá haver a necessidade de tornar público a ocorrência deste vazamento de dados e notificar as autoridades reguladoras e os titulares dos respectivos dados. Deve-se ressaltar que qualquer violação de privacidade pode, a princípio, ser divulgada ao público, causando perdas significativas à reputação da **ECOVITA**.

A **ECOVITA** se reserva o direito de instaurar procedimentos cíveis ou criminais contra os colaboradores internos e externos ou outras pessoas responsáveis em caso de violação desta Política de Proteção de Dados Pessoais ou da LGPD e impor sanções de acordo com tais comportamentos.

1.5. Definições

- ***Titular*:**

Qualquer pessoa natural cujos dados pessoais estão sendo tratados. Isso inclui, por exemplo, fornecedores, clientes ou pessoas de outras empresas. Também são considerados titulares os funcionários, abrangendo também os candidatos às vagas na ECOVITA, aposentados, funcionários temporários, estagiários, etc.

- ***Dados Pessoais:***

Todas as informações individuais sobre uma pessoa natural identificada ou identificável ("titular dos dados pessoais"). Dados pessoais de indivíduos identificados são aquelas informações que imediatamente podem identificar uma pessoa, tais como: nome, sobrenome, documentos pessoais (CPF, RG, CNH, Carteira de Trabalho, passaporte e título de eleitor), endereço, telefone, e-mail, etc. Uma pessoa é identificável se a conexão de dados puder levar a uma dedução de quem é essa pessoa e, assim, torná-la identificável, como por exemplo, predileções, interesses e hábitos de consumo, dados de endereço IP e geolocalização. Os dados pessoais podem estar relacionados a circunstâncias pessoais (por exemplo, nome, endereço, estado civil, filhos, hobbies, certificados, status profissional) ou a circunstâncias materiais (por exemplo, renda, bens, propriedades, seguro, e-mails, número da conta bancária).

- ***Dados Pessoais Sensíveis:***

Todos os dados pessoais, incluindo informações sobre saúde (como diagnósticos ou observações médicas), vida sexual e orientação sexual, origem racial e origem étnica (como nacionalidade ou cor da pele), filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados biométricos (como impressões digitais), dados genéticos, quando vinculado a uma pessoa física.

- ***Tratamento:***

Toda operação realizada com dados pessoais, com ou sem o auxílio de procedimentos automatizados, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. No processamento diário de dados, é necessário levar em consideração que, para cada um dos assuntos ora mencionados, deve ser verificado separadamente se o respectivo tratamento é permitido.

- ***Controlador:***

A pessoa física ou jurídica, de direito público ou privado, a quem compete, sozinha ou em conexão com outras pessoas, as decisões sobre os objetivos e meios de tratamento de dados pessoais.

- ***Operador:***

Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O Operador realiza o tratamento de dados pessoais conforme as instruções do Controlador, que permanece como proprietário dos dados.

- ***Agentes de tratamento:***

O Controlador e o Operador.

- ***Anonimização:***

Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

2. PRINCÍPIOS BÁSICOS DA LEI DE PROTEÇÃO DE DADOS

2.1 Finalidade

Realização do tratamento de dados pessoais para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Os dados pessoais podem ser processados apenas para os fins para os quais foram coletados. Os fins devem ser especificados e documentados no momento da coleta dos dados.

As alterações posteriores de finalidade dos dados coletados são permitidas apenas dentro de um limite mínimo, por exemplo, se houverem interesses legítimos da ECOVITA, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular dos dados pessoais, assim como os fundamentos e os princípios estabelecidos neste instrumento.

2.1. Adequação:

Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

2.2. Necessidade

Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Portanto, é necessário garantir que, a cada coleta de dados, apenas os dados realmente necessários para as finalidades informadas serão coletados. Se o objetivo do tratamento for cumprido, os dados serão excluídos, a menos que incorra em uma das hipóteses legais.

2.3. Livre Acesso

Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

2.4. Qualidade dos Dados

Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

2.5. Transparência

Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

2.6. Segurança

Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

2.7. Prevenção

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

2.8. Não discriminação

Impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos.

2.9. Responsabilização e prestação de contas

Demonstração, pelo agente de tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

3. BASES LEGAIS PARA O TRATAMENTO DE DADOS

O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses, previstas na LGPD:

(a) Mediante o fornecimento de consentimento pelo titular para um propósito determinado;

(b) Para o cumprimento de obrigação legal ou regulatória pelo Controlador;

(c) Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

(d) Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

(e) Quando necessário para a execução de um contrato do qual o titular dos dados é parte ou para execução de qualquer ação pré-contratual tomada a pedido do titular dos dados;

(f) Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

(g) Para a proteção da vida ou da incolumidade física do titular ou de terceiros;

(h) Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

(i) Quando necessário para atender aos interesses legítimos do Controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

(j) Para proteção do crédito;

Deve-se garantir que uma das justificativas acima esteja presente durante todo o tratamento. Se este não for mais o caso porque, por exemplo, um consentimento foi revogado, o tratamento posterior desses dados será considerado ilegal e, portanto, deve ser evitado.

4. ADMISSIBILIDADE DO TRATAMENTO DE DADOS

A **LGPD** sempre deve ser observada quando dados pessoais ou dados pessoais sensíveis são tratados. Isso se aplica independentemente desses dados serem tratados de forma física ou eletrônica, sejam eles confidenciais ou de conhecimento geral, divulgados a terceiros ou não.

A **ECOVITA** trata principalmente dados pessoais de seus funcionários, fornecedores, clientes e terceiros. O tratamento de dados pessoais – na medida do necessário e permitido para o cumprimento dos respectivos fins – deve ser realizado exclusivamente por funcionários competentes da **ECOVITA**, treinados para atender aos requisitos necessários e que estejam comprometidos com o sigilo dos dados.

4.1. Requisitos: Consentimento ou permissão legal

Os dados só podem ser tratados se a pessoa em questão consentir ou nas demais hipóteses legais permissivas descritas na Parte 3 acima. Os fundamentos legais para o

processamento podem ser, além do consentimento da pessoa envolvida (por exemplo, no envio de um informativo/ newsletter), requisitos contratuais (por exemplo, cumprimento de um contrato com o cliente), obrigações legais (por exemplo, armazenamento de dados pessoais para fins de seguridade social) ou mesmo interesses legítimos (por exemplo, execução de dívidas pendentes).

4.2. Tratamento de dados pessoais para fins trabalhistas

A **LGPD** se aplica ao tratamento de dados pessoais, por exemplo, de candidatos, empregados ou aposentados ("empregados"). Em particular, os seguintes pontos devem ser observados:

Os dados pessoais de um funcionário podem ser tratados pela **ECOVITA**, se isso for necessário, para as diferentes fases da relação de emprego, ou seja, para estabelecer, conduzir ou rescindir um contrato de trabalho. Os tratamentos de dados pessoais começam com a inscrição de um candidato junto à **ECOVITA** e termina em 3 anos após a extinção do contrato de trabalho.

Desta forma, os dados que a **ECOVITA** coleta no desenvolvimento de suas atividades e no exercício de seus direitos, são necessários para o desempenho da relação de emprego. Assim, por exemplo, o empregador pode armazenar e usar não apenas os dados básicos de seus funcionários (nome, idade, profissão, etc.), mas também sua qualificação, treinamento e capacidade operacional.

A necessidade de tratar dados pessoais na relação de empego pode resultar do próprio contrato de trabalho e do seu cumprimento (por exemplo, transferência de dados para o banco com o objetivo de pagamento salarial), mas também de um interesse legítimo do empregador (por exemplo, solicitando registros de saúde relacionados à relação de emprego).

Os dados pessoais sensíveis podem ser armazenados, por exemplo, para fins específicos da relação de emprego, previdência e seguridade social.

Os dados que não forem mais necessários ou que não tenham nenhum fundamento jurídico para serem armazenados devem ser excluídos.

4.2.1. Consentimento dos funcionários

Se o tratamento de dados pessoais não estiver nas bases legais previstas na LGPD, deverá ser requerido o consentimento do funcionário. A validade do consentimento pressupõe que ele seja de forma voluntária. O funcionário não deve consentir, por exemplo, por estar com medo de consequências negativas na relação de emprego, ele deve ser livre em sua escolha. Ao determinar a natureza voluntária, os seguintes critérios devem ser considerados:

- Vantagem legal ou econômica para o funcionário;

- Igualdade de interesses entre empregador e empregado.

Exemplos:

- Introdução à gestão da saúde ocupacional no local de trabalho;
- Uso privado de comunicações da empresa.

Em regra, o consentimento deve ser evitado e o tratamento de dados pessoais deve se dar dentro das hipóteses previstas em lei

4.3. Tratamento de dados do cliente, fornecedor ou terceiro

Os dados pessoais dos clientes, fornecedores e terceiros, incluindo usuários visitantes das páginas da web, podem ser utilizados para fins de consulta ou para a execução de contrato com o cliente ou usuário, ou seja, devem ser tratados e usados como parte do fornecimento de serviços. Isso inclui o tratamento para fins contábeis, prestação de serviços, armazenamento em um sistema eletrônico de controle processual.

4.4. Requisitos para o consentimento

Se o processamento de dados pessoais for baseado no consentimento, os seguintes requisitos deverão ser observados. Se esses requisitos não forem observados, não há validade no consentimento e o tratamento de dados deverá ser evitado.

REQUISITOS	EXPLICAÇÃO
Voluntário	O consentimento não será voluntário se: • O tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço e o titular não for informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos. • Existir incompatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. • Não é dado opções distintas (granulares) separadas para obter consentimentos para diferentes propósitos e tipos de processamento. • Os dados coletados não são necessários para a realização das suas finalidades.
	O consentimento deve se aplicar apenas para finalidades determinadas, as quais devem ser integralmente descritas e informadas ao titular dos dados pessoais. Deve-se

Específico/para uma finalidade determinada	especificar os motivos pelos quais os dados são coletados e o que será feito com eles. Finalidades diferentes devem ser separadas e, se necessário, deverá haver diferentes declarações de consentimento para cada questão (opções granulares de consentimento), ou seja, apenas um consentimento geral para todas as finalidades não é permitido.
Revogável	O titular dos dados pode revogar seu consentimento a qualquer momento. A revogação deve ser tão simples quanto à concessão do consentimento. O titular dos dados deverá ser informado de seu direito de revogação. Uma referência clara a esse direito deve ocorrer antes do consentimento. Após o recebimento da revogação, os dados pessoais não poderão mais ser utilizados, podendo, no entanto, ser mantido armazenado, com segurança e anonimizado, exclusivamente para exercício de direito em processo judicial, administrativo ou arbitral.
	A pessoa em questão deve saber com o que exatamente está consentindo. É, portanto, antes da declaração de consentimento, que o titular dos dados deve ser informado sobre isto. Essas informações também definem

Informação	os limites do processamento: todas as operações que não foram informadas ao titular não estão englobadas no consentimento.
Inequivocamente	Para o consentimento é necessário ter uma "atitude claramente confirmatória". A LGPD prevê, por exemplo, que um campo seja preenchido com a opção "aceitar" (opt-in). Esse requisito não é atendido, por exemplo, se houver silêncio, utilização de caixas pré-selecionadas, ou houver inatividade do titular dos dados (opt-out).
Detectável	A empresa deve ter provas do consentimento, mantendo registro das operações de tratamento de dados pessoais que realizar. Deverá possuir uma declaração de consentimento assinada ou usar um procedimento de aceitação dupla "*Double-Opt-In*". Para a documentação necessária.
Escrito	No caso de funcionários, o consentimento sempre deverá ser obtido por escrito, a fim de atender os requisitos da Lei Geral de Proteção de Dados.

4.5. Documentação e prova de consentimento

- O consentimento de forma eletrônica deve ser registrado, ou seja, a data e a hora do consentimento devem ser salvas. O registro de data e hora é armazenado juntamente com os dados da pessoa em questão no sistema. Para uma identificação segura da parte que consentiu, deve ser utilizado o procedimento de dupla aceitação "*Double-Opt-In"*. O consentimento deve estar disponível para o titular dos dados, a qualquer momento, para recuperação.

- O consentimento por escrito deve ser arquivado fisicamente ou digitalizado.

- A revogação do consentimento deve ser igualmente documentada da mesma forma que a declaração de consentimento do titular dos dados. Deverá ser garantido que, após o recebimento da revogação, os dados dos titulares serão processados e mantidos apenas na extensão permitida, tal como para o exercício de direito em processo judicial, administrativo ou arbitral.

5. TRANSFERÊNCIA E USO COMPARTILHADO DE DADOS

A transferência ou o uso compartilhado de dados com terceiros só é permitida se houver uma previsão legal para tal operação ou se houver o consentimento da pessoa titular dos dados.

5.1. Transferência de dados

5.1.1. Transferência para terceiros

A transferência é a mudança de dados para terceiro (= outro controlador). Neste caso, a mera disponibilização de dados para coleta por outro controlador já é suficiente.

Se um fundamento legal realmente permite a transferência de dados isto deverá ser analisado caso a caso. Em regra, esse apenas será o caso se a transferência for realmente necessária para cumprir um contrato com o cliente, fornecedor ou usuário. Alternativamente, pode haver interesse legítimo da ECOVITA que superam os do cliente, fornecedor ou usuário.

5.1.2. Tratamento Interno

Se os setores internos da ECOVITA tiverem acesso aos dados, deverá ser garantido que apenas pessoas autorizadas terão acesso. Isso é feito por meio de uma autorização apropriada que especifique:

- Quem;
- Formato (leitura, escrita, exclusão);
- Para quais fins (por exemplo, cobrança, avaliações) o acesso aos dados é concedido.

Conforme se verificou em todo processo de implementação, especialmente pelas diretrizes emanadas pelo Encarregado de Dados do Operador (Juris Factum) ao Controlador (ECOVITA) as perguntas “por que?” e “para que?” deverão ser respondidas satisfatoriamente para o tratamento de quaisquer dados.

5.2. Transmissão de dados para operadores

Se um terceiro (= contratado/operador) da ECOVITA (= CLIENTE) realizar o armazenamento de dados pessoais, este terceiro deverá seguir a instruções da ECOVITA, que usualmente é um trabalho de processamento no mesmo sentido da LGPD.

Neste caso, o cliente permanece responsável pelas atividades do contratado/operador - também através dos titulares dos dados e da autoridade de supervisão de proteção de dados – mesmo que o contratado tenha certa responsabilidade. O contratado ficará sob o controle como se fosse um “armazém” do cliente. Neste caso, a transferência de dados não será, portanto, considerada uma transferência no sentido da lei.

Neste caso, mesmo que a transferência não precise ser legitimada por um fundamento legal ou por consentimento, as partes deverão realizar um contrato de tratamento de dados. O contrato de tratamento de dados requer, necessariamente, a forma escrita e deve conter determinados conteúdos, expressamente padronizados na LGPD.

Em um contrato de tratamento de dados, em termos de conteúdo, as partes contratantes devem definir os seguintes pontos:

- O objeto e a duração do contrato;
- O escopo, natureza e os fins da coleta, processamento ou do uso pretendido dos dados, a natureza dos dados e seus titulares.
- As medidas técnicas e organizacionais que serão tomadas;
- A correção, exclusão e bloqueio de dados;
- Os deveres do contratado (por exemplo, obrigação de confidencialidade, apoiar a avaliação de impacto e a implementação dos titulares dos dados) que existem de acordo com o artigo 46 da LGPD, e também os controles que eles devem ser realizados.
- Quaisquer direitos de subcontratação;
- Os direitos de controle do cliente e a cooperação do contratado;
- Infrações cometidas pelo contratado ou pelas pessoas por ele contratadas para a proteção de dados pessoais ou contra provisões estabelecidas para tal tarefa;
- A extensão da autoridade que o cliente reserva ao contratado e quem documenta as instruções;

- A devolução de qualquer mídia contendo dados que foi fornecida e a exclusão dos dados armazenados pelo contratado após o término do contrato.

O cliente é obrigado a inspecionar o contratado antes e depois das atividades para garantir a conformidade com determinadas especificações acordadas, como o cumprimento com as medidas técnicas e organizacionais. Normalmente, as inspeções são realizadas no local. Às vezes, é suficiente para o contratado provar que implementou os requisitos acordados mediante a emissão de um certificado por um terceiro imparcial.

Se houver uma relação de pedidos sem um contrato de tratamento de dados ou se você não tiver certeza se existe um tratamento de dados para o presente caso, entre em contato com o encarregado de dados mencionado na Parte 9 deste Manual. Ele tem modelos para os contratos em questão.

As cópias destes contratos devem sempre ser enviadas para o Encarregado pela proteção de dados. Alterações nos contratos já existentes de processamento de pedidos sempre devem ser acordadas com o Encarregado pela proteção de dados.

5.3. Transmissão para um país terceiro sem segurança

A transferência de dados para os chamados “países sem segurança” exige uma legitimidade especial. “Países terceiros sem segurança” são países que não possuem um nível adequado de proteção de dados. Como existe um risco específico relacionado a

essa transferência e a ECOVITA normalmente não tem o direito de transferir dados para países sem segurança devido aos contratos firmados com as partes envolvidas, antes de enviar dados para um país sem segurança, o encarregado de dados listado no item 9 desta Política de Proteção de Dados deverá ser informado.

6. RETENÇÃO/BLOQUEIO/EXCLUSÃO/RETORNO DE DADOS

6.1. Padrões de Segurança

O armazenamento, bloqueio e exclusão dos dados devem estar de acordo com os padrões de segurança da ECOVITA.

6.2. Bloqueio, exclusão, destruição e devolução de dados

Basicamente, os dados podem ser armazenados apenas enquanto forem necessários ou enquanto uma disposição legal permitir seu armazenamento. Por exemplo, pode ser necessário reter dados dos clientes da ECOVITA por até 10 (dez) anos devido a regras fiscais, comerciais ou pelos respectivos prazos prescricionais ou decadenciais para exercício regular de direito, na forma da legislação vigente, mesmo que não haja mais nenhum contato com o cliente e seus dados devam realmente ser excluídos. No entanto, por exemplo, os dados arquivados podem ser usados apenas para fins fiscais, logo, devem ser bloqueados (anonimizados) para outros fins.

Se você tiver alguma dúvida ou incerteza quanto à classificação dos dados de acordo com sua sensibilidade, bem como os requisitos de armazenamento e exclusão, o Encarregado deverá ser imediatamente contatado (ver Parte 9 deste Manual de Proteção de Dados).

Também é necessário garantir que os dados pessoais sejam sempre destruídos ou excluídos de acordo com a LGPD (por exemplo, triturados ou mediante emissão de certificado por um triturador de dados certificado para tal).

7. PROTEÇÃO DE DADOS ORGANIZACIONAIS

7.1. Obrigação do funcionário em termos de confidencialidade

Todos os colaboradores internos e externos da ECOVITA devem estar sujeitos à confidencialidade e prestação de contas relacionadas a isto, mediante assinatura de uma declaração de confidencialidade. Você está proibido de coletar, processar ou usar dados pessoais sem autorização. A obrigação de confidencialidade continua mesmo após o término de suas funções.

7.2. Comunicação de incidentes relacionados à proteção de dados

7.2.1. Contexto legal

Todo funcionário é obrigado a informar imediatamente o seu supervisor se violar a LGPD, no decorrer de seu trabalho.

No caso de uma violação de dados pessoais, a **ECOVITA**, conforme o artigo 48 da LGPD, tem a obrigação de informar a Autoridade Nacional de Proteção de Dados em prazo razoável (até 72 (setenta e duas) horas). Além disso, a **ECOVITA** pode ser obrigada, nos termos do artigo 48 da LGPD, a adotar providências, tais como ampla divulgação do fato em meios de comunicação.

7.2.2. Pré-requisitos para ocorrência de violação na proteção de dados

Uma violação de privacidade ocorre sempre que uma violação da segurança de dados resulta na destruição, perda, alteração, divulgação ou acesso não autorizado a dados pessoais que foram transmitidos, armazenados ou processados. Existe uma divulgação ilegal, por exemplo, se as pessoas envolvidas (= funcionários, clientes, etc.) não tiverem consentido e a divulgação não for permitida por lei (por exemplo, pela LGPD) ou por qualquer outra disposição legal (por exemplo, um contrato da empresa). Basta que haja apenas uma suposição, com certa probabilidade, para que exista uma falha na proteção de dados.

7.2.3. Código de conduta para uma política de proteção de dados

Para poder reagir de forma adequada a uma falha na proteção de dados, por favor siga as instruções abaixo e reporte nos canais especificados:

7.2.3.1. Mensagem

Assim que você determinar ou acreditar que ocorreu uma violação de privacidade notifique imediatamente seu superior. Juntos, vocês enviarão uma notificação do incidente ao encarregado de dados que consta ao final desta Política de Proteção de Dados e também para o seguinte endereço de e-mail:

dpo@ecovitaconstrutora.com.br

Obs.: Não hesite em relatar situações nas quais você não tem certeza se elas atendem as condições de uma falha proteção de dados. Considerando que a análise pode ser difícil, funcionários e especialistas treinados, como o Encarregado pela proteção de dados, determinarão e decidirão finalmente se realmente existe um caso de falha.

7.2.3.2. Informações a serem relatadas

No caso de uma violação de privacidade, verifique se todas as informações necessárias foram coletadas. Cada etapa da quebra de proteção de dados deve ser documentada com precisão e remetido imediatamente ao encarregado de dados pelo e-mail dpo@ecovitaconstrutora.com.br

7.2.3.3. Notificação de obrigações em caso de incidentes no processamento de pedidos

Se a ECOVITA atua como operador, os deveres de fornecer informações decorrem do processamento do pedido. O cliente deve ser informado imediatamente que houve uma violação da proteção de seus dados pessoais pela ECOVITA ou pelos funcionários da ECOVITA incorreram em uma falha na proteção de dados.

Esta obrigação de relatar é válida para cada violação de proteção de dados se os dados pessoais processados são/foram afetados.

7.2.3.4. Procedimento para uma mensagem

Os seguintes passos deverão ser seguidos:

1. A pessoa responsável internamente deverá informar imediatamente a gerencia, o Encarregado pela proteção de dados e o responsável do RH/TI sobre a notificação.

2. O Encarregado pela proteção de dados examinará o assunto juntamente com o responsável do RH/TI e fornecerá à gerência uma avaliação e recomendações.

3. O responsável pela proteção de dados também irá, juntamente com o responsável do RH/TI e com a participação da pessoa relatora, preencher ou finalizar o registro de falha na Proteção de Dados e disponibiliza-lo à diretoria.

4. A decisão sobre se e o que fazer no caso concreto será tomada pela diretoria após consulta com o Encarregado pela proteção de dados e do RH/TI.

7.2.3.5. O que mais deve ser considerado?

Se você tomar conhecimento de alguma violação de privacidade, observe as seguintes regras:

- Não comunique a falha de proteção de dados para terceiros ou para seus colegas;
- Não tenha medo de divulgar erros de seus colegas. Lembre-se que uma violação da LGPD pode resultar em multas substanciais e a empresa pode sofrer danos severos em sua reputação! Portanto, é tarefa da gerência decidir como proceder no caso concreto e se e como o incidente será comunicado externamente.
- A sensibilidade do tópico requer um processo de relatório interno.
- Registre os eventos da maneira mais concreta possível ao encarregado de dados.

7.3. Verificação pelas autoridades

Será permitido aos funcionários da Administração Pública e do Judiciário, que precisarem acessar os dados, em especial dados pessoais, no exercício de suas funções. Todas as medidas necessárias serão coordenadas e supervisionadas pelo Encarregado de Dados.

Se isto acontecer, a pessoa responsável internamente deve ser informada imediatamente. A notificação da pessoa responsável, bem como o recebimento desta notificação deverá ser documentada.

7.4. Controle pelas autoridades de supervisão de proteção de dados

Se uma inspeção for realizada por uma autoridade supervisora de proteção de dados, a pessoa responsável internamente e o responsável pela proteção de dados deverão ser informados imediatamente.

De acordo com a **LGPD**, a Autoridade Nacional de Proteção de Dados é obrigada a monitorar e supervisionar a execução da **LGPD** e outros regulamentos de proteção de dados. Nesse caso, a autoridade supervisora de proteção de dados tem o direito de entrar, sob supervisão, durante o horário comercial nas instalações da empresa, a fim de realizar inspeções e, assim, visualizar documentos comerciais, dados pessoais armazenados e os programas de processamento de dados da empresa. Não é necessário um anúncio por parte da autoridade competente sobre a inspeção no local.

A **ECOVITA** deve tolerar essas medidas pela Autoridade Nacional de Proteção de Dados e garantir que as instalações nas quais ocorra o processamento de dados (como escritórios de funcionários, salas de computadores, arquivos) sejam disponibilizadas aos representantes da autoridade supervisora de proteção de dados, bem como haja a disponibilização das senhas necessárias e dos documentos relevantes. Além disso, mediante requerimento, a autoridade de supervisão também deve receber todas as informações necessárias para desempenhar suas funções.

7.5. Treinamento

A **ECOVITA** treina os funcionários em relação às disposições relevantes sobre proteção de dados. O treinamento dos funcionários será documentado, indicando o conteúdo, a data e o treinador.

Consigna-se que com a efetiva implementação da LGPD na ECOVITA, todos seus colaboradores serão capacitados no mínimo com o seguinte curso gravado em vídeo aulas, contemplando os seguintes tópicos abaixo:

1 – Introdução LGPD, GDPR e CCPA;

2 – Princípios da LGPD;

3 – Hipóteses legais de Tratamento;

4 – Dados Pessoais e Dados Sensíveis. Anonimização. Ciclo de Vida de Dados;

5 – Direitos dos Titulares. Agentes de Tratamento. Encarregado de Dados (DPO);

6 – Responsabilidade Civil;

7 – ANPD Sanções;

8 – Boas Práticas de Governança e Conscientização. Capacitação e efetiva adequação;

9 – Incidentes de Segurança. Vazamento de Dados;

10 – ISOs 27001, 27002 e 27701. Documentação pertinente. Política de Privacidade, Manual de Tratamento de Dados e Relatórios de Impacto de Risco.

Referido curso foi idealizado pelo Operador responsável pela Implementação (Juris Factum), ministrado por professores capacitados na área de Direito Digital e Segurança da Informação (Certificação DPO Exin segundo os padrões da GDPR – Europa - https://www.exin.com/career-path/exin-certified-data-protection-officer?language_content_entity=en).

7.6. Registro de atividades de tratamento de dados

7.6.1. Geral

A Lei Geral de Proteção de Dados Pessoais exige que a ECOVITA compile e mantenha uma lista de atividades de tratamento. Isso deve ser feito, por um lado pelos controladores e, por outro pelos operadores.

O registro de atividades de tratamento de dados geralmente é fornecido às autoridades de supervisão de proteção de dados durante a inspeção para proporcionar uma visão geral do processamento atual de dados.

Portanto, verifique se elas estão sempre atualizadas.

7.6.2. Criação ou modificação do Registro de atividades de tratamento de dados

Os departamentos técnicos criam o Registro de atividades de tratamento de dados para todas as atividades de processamento que eles usam no local de trabalho e para as quais os dados pessoais são armazenados, processados e utilizados. No caso de novos procedimentos, a preparação deve ser realizada antes da sua introdução e entregue à pessoa responsável internamente.

O Registro de atividades de tratamento de dados é complementada por referência às análises de proteção de dados relacionadas à admissibilidade do processamento de dados, à necessidade de realizar uma avaliação de impacto e à respectiva declaração do responsável pela proteção de dados.

7.7. Avaliação de impacto na privacidade

Em certos casos, a ECOVITA deve realizar um Relatório de Impacto à Privacidade dos Dados, por exemplo, se o processamento puder representar altos riscos para os titulares dos dados. Podem surgir altos riscos quando são realizadas vigilância por vídeo ou

desempenho automatizado de funções dos funcionários e quando são realizados testes comportamentais.

A necessidade de realizar ou não uma avaliação de impacto será determinada pela diretoria e pelo Encarregado pela proteção de dados. Em casos específicos, eles também determinam quem será envolvido no processo ou quem irá implementar a avaliação de impacto.

Para efetiva implementação da LGPD, a ECOVITA encomendou junto ao Operador responsável seu primeiro RIPD.

7.8. Cumprimento das medidas técnico-organizacionais/segurança dos dados

Para garantir a segurança dos dados pessoais armazenados na ECOVITA, foram implementadas medidas técnicas e organizacionais apropriadas que também garantem a proteção dos dados contra acesso, processamento ou divulgação não autorizados, bem como perda acidental, alteração ou destruição. Em particular, a ECOVITA tomou medidas para garantir um nível de proteção adequado ao risco de processamento em termos de confidencialidade, integridade, disponibilidade e resiliência dos sistemas de TI, banco de dados, etc. A proteção da confidencialidade é implementada através do controle de acesso e desconexão. A integridade é implementada através do controle de transferência, controle de entrada e controle de pedidos. A disponibilidade e a resiliência são garantidas por meio de medidas de disponibilidade e monitoramento regular.

Essas medidas técnicas e organizacionais estão descritas no Sistema de Gerenciamento de Segurança da Informação da ECOVITA. Elas são adaptadas continuamente para refletirem desenvolvimentos técnicos e mudanças organizacionais.

8. DIREITOS DOS TITULARES

Por lei, o titular dos dados tem vários direitos em relação ao processamento de seus dados pessoais. A ECOVITA estabeleceu um ponto de contato central, sendo a única responsável por responder questões relativas a relacionamento externo.

No entanto, entre em contato com o responsável pela proteção de dados ou com o responsável interno se tiver alguma dúvida ou se um titular de dados entrar em contato diretamente com você.

Existem os seguintes direitos das pessoas em questão:

8.1. Direito à informação

O titular dos dados pode exigir, a qualquer momento, informações gratuitas sobre quais dados a ECOVITA processa sobre ele, os objetivos do processamento, a duração do armazenamento ou os critérios para determinar a duração do armazenamento e os destinatários dos dados. O titular também deve ser informado de seus direitos à retificação, exclusão, limitação de processamento ou de seus direitos de objeção.

Além disso, existe o direito de receber uma cópia dos dados.

Isso significa que todo titular de dados tem o direito de entrar em contato com o departamento responsável a qualquer momento para realizar perguntas ou reclamações. As informações devem ser fornecidas prontamente e de maneira apropriada e oportuna para as os titulares dos dados. Geralmente ocorre por escrito ou de forma eletrônica.

Em relação aos pedidos de informações deve-se garantir que as informações sejam enviadas apenas às pessoas autorizadas. Portanto, é sempre necessário identificar de forma clara o solicitante (por exemplo, por endereço de e-mail, número de transação, etc.) antes de divulgar informações pessoais.

8.2. Direito de corrigir, excluir e reestruturar o processamento

Além disso, os titulares dos dados têm direitos de correção em relação aos dados pessoais armazenados pela ECOVITA, assim titular de dados tem, por exemplo, o direito de corrigir dados pessoais incorretos ou incompletos armazenados pela ECOVITA.

Ademais, a ECOVITA deve excluir as informações pessoais armazenadas se o fundamento legal para seu processamento for revogado. Se houver o direito de excluir os dados pessoais, mas a exclusão não for possível ou for imotivada os dados pessoais deverão ser bloqueados para usos inadmissíveis.

O titular dos dados poderá solicitar uma limitação do processamento se considerar que seus dados estão incorretos; em princípio os dados deverão ser excluídos, porém, os dados ainda serão necessários pela ECOVITA para processar ações judiciais ou pela pessoa em causa contra o processamento de dados da ECOVITA, devido a interesses legítimos que eles negam devido à sua situação específica.

Se a ECOVITA divulgou os dados, os destinatários devem ser informados sobre a correção, exclusão ou restrição – a menos que isso seja impossível ou exija um esforço desproporcional.

8.3. Direito à portabilidade de dados

Se o titular dos dados fornecer à ECOVITA seus dados com base em seu consentimento ou em razão de uma relação contratual com a ECOVITA, a ECOVITA é obrigada a fornecer esses dados em um formato padrão mediante solicitação do titular, ou se for possível, a um terceiro por ele designado.

8.4. Direito de objeção

Se a ECOVITA processa dados com base em um interesse legal, o titular dos dados pode se opor a esse processamento por razões que decorrem de situação específica. O direito de objeção não existe se a ECOVITA reter os dados para, por exemplo, o exercício de reivindicações legais ou se os interesses da ECOVITA impedirem o término do processamento.

8.5. Direito de retirada

Se a pessoa em questão tiver dado o seu consentimento em relação ao tratamento de seus dados pessoais, poderá, a princípio, revoga-lo em qualquer momento com efeitos a partir de uma data específica. Por exemplo, o titular dos dados pode se opor ao processamento de seus dados pessoais para fins de publicidade a qualquer momento. Se os dados forem necessários em outros contextos (por exemplo, obrigações de arquivamento), eles poderão ser utilizados apenas para esse fim específico e, caso contrário, deverão ser bloqueados.

8.6. Direito de reclamação

A pessoa em questão tem o direito de entrar em contato com o responsável pela proteção de dados a qualquer momento. Ela também tem o direito de registrar uma reclamação junto à Autoridade de Proteção de Dados responsável, ou seja, na Autoridade Estadual responsável pela proteção de dados da Federação, na qual a pessoa responsável estiver situada.

9. CONTATO COM O ENCARREGADO DE DADOS

A **ECOVITA** nomeou um responsável interno para a proteção de dados:

Nome: Roberta de Angelis

E-mail: roberta.deangelis@ecovitaconstrutora.com.br

E-mail para reportar questões sobre privacidade de dados e afins:
dpo@ecovitaconstrutora.com.br