GUIA DE BOAS PRÁTICAS DA EMPRESA PARAIBANA DE COMUNICAÇÃO S.A. - EPC

EMPRESA PARAIBANA DE COMUNICAÇÃO

EMPRESA PARAIBANA DE COMUNICAÇÃO S.A. (EPC)

Naná Garcez de Castro Dória
Diretora Presidente

William Costa
Diretor de Mídia Impressa

Rui Leitão
Diretor de Rádio e TV

Amanda Lacerda
Diretora Administrativa, Financeira e de Pessoas

Elaboração
Adriana Borba de Medeiros (Encarregada pelo tratamento de dados pessoais - DPO)

Revisão
Clara de Freitas (Revisora)

Diagramação
Naudimilson Ricarte (Designer Gráfico)

GUIA DE BOAS PRÁTICAS DA EMPRESA PARAIBANA DE COMUNICAÇÃO S.A. - EPC

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
10/05/2024	1.0	Primeira versão do Guia de boas práticas	Encarregada pelo Tratamento de Dados (DPO): Adriana Borba

SUMÁRIO

1 INTRODUÇÃO

O Guia de boas práticas tem sua base no Decreto Estadual n° 41.238, de 7 de maio de 2021, seguindo as orientações das disposições de Segurança da Informação e de Proteção de Dados Pessoais, dispostas na Lei Federal de n° 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados, assim como demais regulamentações relacionadas.

O objetivo principal de um Guia de boas práticas é fornecer orientações claras e úteis para ajudar indivíduos ou organizações a alcançarem resultados eficazes e de alta qualidade em suas atividades, trazendo também orientações quanto a sua aplicabilidade no âmbito da empresa pública.

A Lei Geral de Proteção de Dados (LGPD) veio desempenhar um papel fundamental na proteção dos direitos individuais, na promoção da confiança nas instituições e no estímulo ao desenvolvimento econômico sustentável, tudo isso em um contexto de crescente importância dos dados na sociedade contemporânea.

A conformidade com a LGPD pode resultar em benefícios econômicos para as organizações, pois promove a eficiência operacional, reduz o risco de penalidades por violações e melhora a reputação da empresa.

O Guia de boas práticas da LGPD oferece diretrizes específicas sobre como as organizações podem se adequar à lei, garantindo que estejam em conformidade com suas disposições. Ele pode incluir recomendações sobre políticas de privacidade, segurança da informação, consentimento do titular dos dados, comunicação de incidentes de segurança, entre outros aspectos relacionados à proteção de dados pessoais.

Além disso, o Guia de boas práticas pode ajudar as organizações a adotarem uma abordagem proativa em relação à proteção de dados, promovendo uma cultura de conformidade e de conscientização dentro da empresa. Isso não apenas ajuda a evitar violações da lei, mas também contribui para a construção da confiança dos clientes e do público em geral em relação ao tratamento de seus dados pessoais da Empresa Paraibana de Comunicação S.A. (EPC), de acordo com o art.50 da Lei Geral de Proteção de Dados.

2 NOÇÕES GERAIS DA LEI GERAL DE PROTEÇÃO DE DADOS

2.1 Dados Pessoais e Dados Sensíveis

Para facilitar a compreensão, o dado pessoal fundamentado na LGPD, em seu art. 5°, define que qualquer informação que permita identificar, direta ou indiretamente, uma pessoa natural, tais como nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, cartão bancário, renda, histórico

de pagamentos, hábitos de consumo, preferências de lazer, endereço de IP (Protocolo da Internet) e cookies, é um dado pessoal. Dados pessoais são apenas os relacionados a uma pessoa natural.

Os dados pessoais sensíveis são os que exigem um maior cuidado em seu tratamento, sendo dados que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa.

2.2 Agentes de Tratamento: Controlador e Operador

A Lei Geral de Proteção de Dados traz os agentes de tratamento que desempenham papéis específicos no contexto do tratamento de dados pessoais e têm responsabilidades distintas de acordo com suas funções na operação. O cumprimento das obrigações estabelecidas pela LGPD é compartilhado entre esses agentes, com o objetivo de garantir a proteção adequada dos direitos e a privacidade dos titulares dos dados.

A Lei Geral de Proteção de Dados traz duas figuras importantes para esse cenário de tratamento de dados pessoais, os agentes de tratamento conhecidos como o controlador e o operador. Esses agentes são definidos a partir de seu caráter institucional e podem ser pessoais naturais ou jurídicas, de direito público ou privado. A classificação desses agentes é importante para que a responsabilidade seja definida.

O controlador é o agente responsável por definir a finalidade do tratamento de dados e por tomar as principais decisões em relação a ele, incluindo instruções fornecidas aos operadores contratados para aquele determinado tratamento. E suas obrigações serão demonstradas na tabela a seguir:

OBRIGAÇÕES DO CONTROLADOR LEI GERAL DE PROTEÇÃO DE DADOS:

Elaborar Relatório de Impacto à Proteção de Dados Pessoais − Art. 38
Comprovar que o consentimento obtido do titular atende às exigências legais − Art. 8,§ 2°
Comunicar à ANPD a ocorrência de Incidentes de Segurança − Art. 48
Responsabilidade de reparar danos decorrentes de violação à legislação de proteção de dados pessoais − Art. 42 a 45
Garantir os Direitos dos Titulares, como fornecer informações relativas ao tratamento, assegurar a correção e a eliminação de dados pessoais, receber requerimento de oposição a tratamento − Art.18
Indicar o Encarregado pelo Tratamento de Dados − Art. 41

O operador é o responsável por realizar o tratamento dos dados em nome do controlador e seguindo a finalidade delimitada por ele, podendo definir elementos não essenciais do tratamento, como medidas técnicas. Demonstrando a grande diferença entre os dois agentes, o poder de decisão. Assim, as obrigações do operador são:

OBRIGAÇÕES DO OPERADOR DA LEI GERAL DE PROTEÇÃO DE DADOS:

Seguir as instruções do operador − Art. 39 Manter registro de operações de tratamento − Art. 37 Responder solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador − Art. 42, § 1º, I

O agente de tratamento é definido para cada operação de tratamento de dados pessoais, podendo uma mesma empresa ser tanto operador como controlador, de acordo com a sua atuação. Sendo controladores quando atuarem com seus próprios interesses e sendo operadores quando atuarem de acordo com os interesses do controlador.

Nesse diapasão, a EPC é uma empresa pública de direito privado, podemos citar alguns cenários para melhor visualização do seu papel como controlador ou operador:

Exemplo 1: EPC como controladora.

→ Internamente: EPC toma as decisões de como tratar os dados pessoais e seus setores executam aquele serviço de acordo com o demandado. Ou seja, o poder de decisão está na EPC, tornando-a controladora, e os setores serão operadores;

→ Externamente: quando a EPC tem poder de decisão sob os dados pessoais e quer terceirizar um serviço de consultoria, ela será a controladora dos dados por decidir como eles serão tratados e a finalidade daquele tratamento, e a empresa que presta o serviço de consultoria será o operador por seguir as orientações da EPC.

2.3 Encarregado de Proteção de Dados − Data Protection Officer (DPO)

É a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), quando estabelecida. O encarregado tem a função de orientar e aconselhar o controlador e os operadores sobre as práticas de tratamento de dados, bem como monitorar o cumprimento da LGPD dentro da empresa.

As principais funções do encarregado, de acordo com o artigo 41, §2º da LGPD, incluem:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares

No caso de um funcionário interno ser indicado para a função de encarregado, a empresa também deverá capacitar esse profissional para que consiga exercer suas atividades com uma boa qualidade.

Também podemos encontrar na Classificação Brasileira de Ocupações - CBO, no código1421-35, que reconhece o encarregado como profissão perante o Ministério do Trabalho em 2022, e estabelecendo que o Oficial de Proteção de Dados Pessoais (DPO) deve:

Planejar processos administrativos, financeiros, de compliance, de riscos e de proteção de dados pessoais e privacidade
Gerenciar pessoas, rotinas administrativas e financeiras
Administrar riscos, recursos materiais, serviços terceirizados e canal de denúncia
Participar da implementação do programa de compliance e/ou governança em privacidade
Monitorar e avaliar o cumprimento das políticas do programa, normativas, código de ética, procedimentos internos e parceiros de negócios
Participar da identificação de situações de riscos e propor ações para mitigação deles
Prestar atendimento ao cliente e/ou cooperado e/ou titular de dados pessoais

O contato do encarregado pelo tratamento de dados deve ser publicados e de fácil acesso, nos termos no § 1º do art. 41 da LGPD, para que os titulares possam entrarem contato, assim como a Autoridade Nacional de Proteção de Dados. Exemplo: encarregada.lgpd@epc.pb.gov.br, Adriana Borba.

2.4 Autoridade Nacional de Proteção de Dados (ANPD)

A Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel central na implementação e fiscalização da LGPD, garantindo a proteção dos direitos dos titulares dos dados e promovendo uma cultura de respeito à privacidade e segurança das informações pessoais no Brasil. As suas principais competências estabelecidas

no art. 55-J da LGPD incluem a de aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação.

3 O CICLO DE VIDA DO TRATAMENTO DE DADOS PESSOAIS

3.1 O tratamento dos dados pessoais

O tratamento de dados na LGPD abrange todas as atividades realizadas com dados pessoais, desde a sua coleta até a sua eliminação, incluindo qualquer operação que envolva manipulação, uso, compartilhamento, armazenamento, entre outras. Isso engloba não apenas dados armazenados em sistemas digitais, mas também informações em formato físico, como documentos em papel.

A LGPD estabelece que o tratamento de dados pessoais deve ser realizado de acordo com os princípios e diretrizes previstos na legislação, garantindo sempre a proteção da privacidade e dos direitos dos titulares dos dados. Isso inclui a necessidade de obter consentimento dos titulares dos dados quando necessário, proteger os dados contra acessos não autorizados, adotar medidas de segurança adequadas e respeitar os direitos dos titulares, como o direito de acesso, retificação e exclusão de seus dados pessoais.

A definição de tratamento de dados pessoais está no art. 5°, X, da LGPD, no qual diz que é “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

O art. 4° da LGPD determina as hipóteses em que a Lei não será aplicada:

- Dados Pessoais tratados por pessoas naturais para fins não econômicos: podemos citar o exemplo de uma pessoa que posta uma foto de uma terceira pessoa na sua conta do Instagram;
- Dados Pessoais tratados para fins jornalísticos ou artísticos: essa hipótese garante a liberdade de imprensa, um exemplo é um caso de um jornalista que publica em um site o nome e foto de um suspeito de cometer um crime;
- Dados Pessoais tratados para fins acadêmicos: se os dados forem utilizados para pesquisas sem fins diretamente comerciais, valendo ressaltar que, sempre que possível, esses dados devem ser anonimizados. Um exemplo é o de um pesquisador de universidade federal que utiliza dados pessoais anonimizados para fundamentar sua pesquisa em relação ao COVID;

- Dados Pessoais provenientes de fora do território nacional sem comunicação ou compartilhamento com empresas brasileiras, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei: como, por exemplo, podemos citar uma empresa brasileira que é contratada por uma empresa europeia para tratamento de dados pessoais dos cidadãos europeus, e os dados são devolvidos para a empresa após o término do tratamento, dessa forma, se aplica a legislação europeia (GDPR).

3.2 Fases do ciclo de vida do tratamento de dados pessoais

Todo dado pessoal deve possuir um ciclo de vida, não podendo ficar armazenado de forma indeterminada pelo controlador ou pelo operador. O dado pessoal é coletado para atender a uma finalidade específica e pode, por exemplo, ser eliminado a pedido do titular dos dados ou ao término de seu tratamento, quando finalizar a relação contratual. Dessa forma, percebemos a configuração de um ciclo que se inicia com a coleta e que determina a "vida" (existência) do dado pessoal durante um período de tempo, de acordo com certos critérios de eliminação e legislações específicas.

O ciclo de vida do tratamento de dados pessoais é como cada operação de dado pessoal, como se inicia, como é finalizada e a forma como seus ativos organizacionais estão em cada etapa. Começando com a coleta do dado pessoal e encerrando-se com a eliminação ou descarte. Suas fases são:

- Coleta: essa fase inclui coleta, produção e recepção de dados pessoais, podendo ser por meio de documento em papel, de formulário eletrônico, sistema de informação, de banco de dados, etc;
- Retenção: trata-se do armazenamento dos dados ou arquivamento, independente de ser por meio eletrônico (banco de dados), documento salvo no computador, documento em papel, guardado em uma pasta ou em armário, etc;
- Processamento: são as operações relacionadas à classificação, à utilização, à reprodução, ao processamento, à avaliação ou ao controle da informação, à extração e à modificação de dados pessoais retidos pelo controlador. Em suma, é o que você faz com aquele dado pessoal, se acessa ele para autorização de pagamento, se utiliza para preenchimento de cadastro, para realização de treinamentos, etc;
- Compartilhamento: envolve qualquer operação de transmissão, distribuição, comunicação, transferência, difusão e uso compartilhado de dados pessoais. Por exemplo, quando compartilha dados pessoais para o banco para determinada finalidade;
- Eliminação: é a operação que exclui/elimina dados pessoais.

Essas etapas representam o ciclo de vida típico dos dados em uma organização e servem como um guia para garantir que os dados sejam gerenciados de forma eficiente, segura e em conformidade com as regulamentações de proteção de dados.

Em cada etapa do ciclo, existem tipos de ativos organizacionais, principalmente base de dados, documentos, equipamentos, locais físicos, pessoas, sistemas e unidades organizacionais:

- Base de dados: uma coleção de dados logicamente relacionados.
- Documento: unidade de registro de informações, qualquer que seja o suporte e formato (Arquivo Nacional, 2005);
- Equipamento: objeto ou conjunto de objetos necessário para o exercício de uma atividade ou de uma função;
- Local físico: determinação do lugar no qual pode residir, de forma definitiva ou temporária, uma informação de identificação pessoal;
- Pessoa: qualquer indivíduo que executa ou participa de alguma operação realizada com dados pessoais;
- Sistema: qualquer aplicação, software ou solução de TI que esteja envolvida com as fases do ciclo de vida do tratamento dos dados pessoais;
- Unidade organizacional: órgãos e entidades da Administração Pública.

4 COMO REALIZAR O TRATAMENTO DE DADOS

4.1 Hipóteses de tratamento de dados pessoais

A LGPD autoriza, em seu art. 23, os órgãos e entidades da administração pública a realizar o tratamento de dados pessoais unicamente para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que as hipóteses de tratamento sejam informadas ao titular.

Hipóteses de tratamento de dados pessoais

HIPÓTESE DE TRATAMENTO	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS
Hipótese 1: mediante consentimento do titular	LGPD, art. 7º, I	LGPD, art. 11, I
Hipótese 2: para o cumprimento de obrigação legal ou regulatória	LGPD, art. 7º, II	LGPD, art. 11, II, “a”
Hipótese 3: para a execução de políticas públicas	LGPD, art. 7º, inciso III	LGPD, art. 11, II, “b”

Hipótese 4: Para a realização de estudos e pesquisas	LGPD, art. 7º, inciso IV	LGPD, art. 11, II, “c”
Hipótese 5: para a execução ou preparação de contrato	LGPD, art. 7º, inciso V	Não se aplica
Hipótese 6: para o exercício de direitos em processo judicial, administrativo ou arbitral	LGPD, art. 7º, inciso VI	LGPD, art. 11, II, “d”
Hipótese 7: para a proteção da vida ou da incolumidade física do titular ou de terceiro	LGPD, art. 7º, inciso VII	LGPD, art. 11, II, “e”
Hipótese 8: para a tutela da saúde do titular	LGPD, art. 7º, inciso VIII	LGPD, art. 11, II, “f”
Hipótese 9: para atender interesses legítimos do controlador ou de terceiro	LGPD, art. 7º, inciso IX	Não se aplica
Hipótese 10: para proteção do crédito	LGPD, art. 7º, inciso X	Não se aplica
Hipótese 11: para a garantia da prevenção à fraude e da segurança do titular	Não se aplica	LGPD, art. 11, II, “g”

4.2 Dez princípios fundamentais específicos da LGPD

Para o tratamento de dados, devem ser observados os princípios, preconizados no art. 6º, são eles:

- Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- 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;
- 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;

- 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;
- 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;
- 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;
- Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- Responsabilização e prestação de contas: demonstração, pelo agente, 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.

Não basta, portanto, o enquadramento em uma das hipóteses legais autorizativas para iniciar o tratamento de dados pessoais. É fundamental garantir que os princípios listados acima sejam respeitados.

5 DIREITOS DO TITULAR DE DADOS

A LGPD estabeleceu uma estrutura legal que empodera os titulares de dados pessoais, fornecendo-lhes direitos a serem exercidos perante os controladores de dados. Esses direitos devem ser garantidos durante toda a existência do tratamento dos dados pessoais do titular realizado pelo órgão ou entidade.

I - Confirmação da Existência de Tratamento: o titular tem o direito de confirmar se uma empresa trata ou não seus dados pessoais;

II - Acesso aos Dados: o titular pode pedir à empresa uma cópia dos seus dados pessoais que ela possui, mediante solicitação;

III - Correção de Dados Incompletos, Inexatos ou Desatualizados: o titular tem o direito de solicitar a correção de dados pessoais incompletos, inexatos ou desatualizados que estejam sob tratamento do controlador;

IV - Anonimização, Bloqueio ou Eliminação de Dados: o titular tem o direito de solicitar a anonimização, o bloqueio ou a eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;

V - Portabilidade de Dados: o titular tem o direito de solicitar a portabilidade de seus dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

VI - Eliminação dos Dados com Consentimento: o titular tem o direito de solicitar a eliminação de dados pessoais tratados com seu consentimento, exceto nos casos previstos em lei;

VII - Informação sobre o Compartilhamento de Dados: o titular tem o direito de saber sobre o compartilhamento de seus dados com terceiros;

VIII - Informação da consequência do não consentimento: se a empresa não obtiver o consentimento do titular dos dados para tratar suas informações pessoais para determinada finalidade, ela não poderá realizar esse tratamento, a menos que exista outra base legal para fazê-lo. A LGPD estabelece diversas bases legais que permitem o tratamento de dados pessoais sem o consentimento do titular, como o cumprimento de obrigação legal ou regulatória pelo controlador, a execução de contrato, a proteção da vida ou da incolumidade física do titular, o exercício regular de direitos em processo judicial, entre outras;

IX - Revogação do consentimento: Após a revogação do consentimento, a organização responsável pelo tratamento dos dados deve cessar o tratamento desses dados para a finalidade especificada, exceto se houver outra base legal para o tratamento. Por exemplo, se os dados ainda forem necessários para cumprir obrigações legais da empresa, o tratamento pode continuar mesmo após a revogação do consentimento.

Esses direitos visam garantir a proteção dos dados pessoais dos indivíduos, conferindo-lhes controle sobre suas informações e promovendo a transparência no tratamento desses dados por parte das organizações.

6 LAI E LGPD

A LAI, no Brasil, é uma lei federal que estabelece o direito de acesso às informações públicas. Seu objetivo é promover a transparência governamental e garantir o direito dos cidadãos de solicitar e receber informações detidas pelos órgãos públicos.

Tendo como base o princípio da transparência governamental e o direito de acesso às informações públicas, enquanto a LGPD visa proteger a privacidade e os direitos dos indivíduos no tratamento de dados pessoais.

A LAI busca promover a transparência e o acesso às informações públicas detidas pelos órgãos governamentais, enquanto a LGPD tem como objetivo proteger a privacidade e os direitos dos indivíduos no tratamento de seus dados pessoais pelas empresas e organizações. Ambas as leis têm a finalidade de estabelecer direitos e garantias.

A LAI aplica-se aos órgãos públicos, enquanto a LGPD abrange empresas e organizações públicas e privadas que lidam com dados pessoais.

7 BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

7.1 Privacidade desde a concepção e por padrão (privacy by design and by default)

7.1.1 Privacidade desde a concepção

A privacidade desde a concepção e por padrão é um dos fundamentos da Lei Geral de Proteção de Dados (LGPD) e refere-se à necessidade de considerar a proteção da privacidade e dos dados pessoais desde o momento da concepção de um sistema ou processo, bem como a adoção de medidas de privacidade como padrão ao longo de todo o ciclo de vida dos dados. Vou explicar melhor esses conceitos:

Privacidade desde a concepção (privacy by design):

- Fundamentos: a privacidade desde a concepção (privacy by design) é um conceito que preconiza que a privacidade e a proteção de dados devem ser incorporadas desde o início do desenvolvimento de um sistema, produto ou serviço. Isso significa que as considerações de privacidade devem ser levadas em conta desde a fase de design, visando garantir a proteção dos dados pessoais ao longo de todo o processo;

- Aplicação: para aplicar a privacidade desde a concepção, é necessário considerar aspectos como minimização dos dados coletados, finalidade específica da coleta, segurança dos dados, transparência nas práticas de tratamento e obtenção de consentimento adequado. É essencial que a proteção da privacidade seja considerada desde o início, a fim de evitar problemas futuros e promover a conformidade com a legislação de proteção de dados.

7.1.2 Privacidade por Padrão

Já a **Privacidade por Padrão** (do inglês privacy by default) está diretamente relacionada ao princípio da necessidade, expresso pelo art. 6º, inciso III:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

III - 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.

Privacidade por padrão (privacy by default):

- Fundamentos: a privacidade por padrão (privacy by default) refere-se à configuração pré-definida de sistemas e serviços de forma a garantir a privacidade dos usuários e a minimização dos dados pessoais coletados. Significa que, por padrão, as configurações devem ser as mais restritivas possíveis em termos de privacidade, garantindo que apenas os dados necessários para o funcionamento adequado sejam coletados e processados;

- Aplicação: a privacidade por padrão envolve a implementação de medidas técnicas e organizacionais para garantir que, por padrão, a privacidade dos usuários seja respeitada. Isso inclui, por exemplo, o uso de criptografia, restrição de acesso aos dados, definição de períodos de retenção adequados e configurações de privacidade que sejam favoráveis à proteção dos dados pessoais.

7.2 Segurança digital

Além das boas práticas explicadas anteriormente, o ambiente digital requer um cuidado ainda maior, pois possui uma natureza dinâmica e é alvo constante de crimes cibernéticos. Dessa forma, é importante seguir as recomendações realizadas por especialistas em segurança da informação, conforme a seguir:

- Troque suas senhas e faça disso um hábito (trocas regulares);
- Crie senhas fortes, alternando entre letras maiúsculas e minúsculas, números e usando caracteres especiais;
- Ative a autenticação de duas etapas em todas as plataformas que você usa que tenham essa função;
- Jamais forneça dados pessoais para quem liga, manda e-mail ou SMS, solicitando-os;
- Desconfie de ligações, mesmo que o interlocutor tenha seu CPF, data de nascimento e outros dados pessoais e afirme falar em nome de uma empresa da qual você é cliente;
- Fique atento às transações que acontecem no seu cartão de crédito ou envolvendo o seu saldo bancário;

- Não abra e-mails duvidosos, desconfie de promoções enganosas, ofertas e brindes;
- Bloqueie câmeras e microfones se eles não estiverem em uso;
- Mantenha um antivírus atualizado e não faça downloads de fontes desconhecidas;
- Tome cuidado com o que postar nas redes sociais e não adicione qualquer um como amigo;
- Na eliminação de documentos que contenham dados pessoais, usar o triturador de papéis.

7.2.1 Boas práticas ao usar os computadores

As boas práticas no uso dos computadores são essenciais para garantir uma experiência segura, eficiente e produtiva ao utilizar a tecnologia, além de proteger os dados pessoais e confidenciais contra ameaças cibernéticas e garantir a durabilidade e o desempenho do equipamento.

- Ao se ausentar da sua mesa, lembre-se de sempre bloquear sua estação de trabalho. Desta forma você evitará que pessoas não autorizadas visualizem informações restritas, sigilosas ou confidências na tela de seu computador;
- Evite tirar prints, fotos ou gravar vídeos da tela do computador que contenha algum dado pessoal à mostra e encaminhá-los por meio de canais de comunicação não oficiais. Esses dados pessoais são de sua responsabilidade;
- Evite ao máximo baixar arquivos pessoais dentro do computador, para que não venham acompanhados de malwares e para que seus dados não fiquem expostos. Caso seja extremamente necessário baixar, lembre-se de excluí-los logo em seguida;
- Evite clicar em links em e-mails, mensagens instantâneas ou em sites não confiáveis. Isso pode ajudar a evitar a infecção por malware ou phishing.

7.2.2 O bom uso das impressoras da EPC

O uso eficiente, econômico e sustentável das impressoras no ambiente de trabalho, reduzindo custos, minimizando impactos ambientais e prolongando a vida útil do equipamento e o mais importante a segurança dos dados pessoais, contidos em documentos.

Portanto, é recomendável que:

- No momento em que o servidor imprimir documentos que contenham dados pessoais, deve lembrar-se de retirá-los da impressora logo em seguida;
- No caso da necessidade de descartar tais documentos, recomenda-se procurar técnicas para que os dados não sejam identificados, por exemplo, triturar o documento ou até mesmo riscar os dados pessoais de forma que se torne ilegível;
- Os documentos impressos que tiverem dados pessoais devem ser guardados em locais seguros, por exemplo, em um armário com chave;
- Quando deixar tais documentos em sua mesa, é preferível que vire o anverso das folhas para baixo, para que os dados pessoais não sejam vistos porqualquer pessoa.

7.2.3 O uso de ferramentas oficiais da EPC

A EPC utiliza a plataforma de e-mail corporativo chamada Zimbra, por isso, é preciso que a troca de e-mails contendo dados pessoais ocorra apenas por meio desse canal de comunicação, evitando que seja realizado por e-mails pessoais dos colaboradores.

7.2.4 O uso seguro das senhas

O uso seguro das senhas é essencial para proteger informações pessoais e confidenciais contra acessos não autorizados, garantindo assim a privacidade, segurança e integridade dos dados. É importante criar senhas fortes, exclusivas e protegidas, além de não compartilhá-las com outras pessoas para manter a segurança online, por isso, recomenda-se:

- Nunca compartilhe suas senhas com outras pessoas. A princípio, você é o responsável por tudo que ocorre com o uso de sua senha;
- Se você não consegue memorizar sua senha e precisar anotá-la, não a deixe em locais visíveis, expostas em cadernos ou marcadores em sua mesa de trabalho.

7.2.5 Boas práticas para tratar dados pessoais no PBdoc

O PBdoc é uma Plataforma oficial do Estado da Paraíba para criação e tramitação de documentos eletrônicos. Foi constituído pelo Decreto Estadual Nº 40.546, de 17 de setembro de 2020, como plataforma oficial do Estado da Paraíba.

A validação dos documentos é garantida pela plataforma, que é mantida por empregados públicos da Companhia de Processamento de Dados da Paraíba (CODATA), logo, dotados de fé de ofício.

Porém, quando documentos/processos forem elaborados no sistema, é importante que se colete ou insira somente os dados pessoais realmente necessários para atender a determinada finalidade, seguindo o princípio da necessidade da LGPD.

Quando se tratar de documentos públicos, assim como portarias, designações e outros, uma boa forma de proteger os dados pessoais é com o uso de tarjas e/ou descaracterização destes, a não ser que exista previsão legal quanto à publicidade/exposição de tais dados. Por exemplo:

CPF: 000.000.000-00 x
CPF: ***.000.000-** ✓
Matrícula: 000000000 x
Matrícula: ******000 ✓

Em qualquer caso, é importante que o servidor promova o equilíbrio entre a transparência e a proteção dos dados pessoais, analisando cada caso separadamente, se por ventura houver a necessidade de disponibilizar os processos ou documentos a usuários externos.

Na abertura de processos ou documentos, é importante vincular o nível de acesso, podendo ser público, restrito ou sigiloso.

O art. 31, da Lei n° 12.527/2011, a LAI, aduz que no tratamento de dados ou informações pessoais, o nível de acesso deve ser restrito sob a hipótese legal de “Informação Pessoal”.

Portanto, o usuário que criar um documento/processo no PBdoc, deve determinar os critérios de acesso, conforme item 2.2 do Manual de utilização do PBdoc. Dessa forma, recomenda-se, para documentos que possuam dados pessoais, a utilização dos seguintes níveis de acesso, conforme o caso:

→ Limitado de pessoa para divisão: somente o subscritor e a lotação destinatária podem visualizar e tramitar o documento;

→ Limitado de divisão para pessoa: Somente a lotação do subscritor e a pessoa destinatária podem visualizar o documento;

→ Limitado entre lotações: somente as lotações do subscritor e do destinatário podem visualizar o documento;

→ Limitado entre pessoas: somente o subscritor e destinatário podem visualizar o documento. Assim, por exemplo, o usuário ao enviar um atestado médico para o Setor de Recursos Humanos, deve utilizar o nível “Limitado de pessoa para divisão”, de modo que seu dado pessoal sensível fique restrito para

o próprio usuário e a divisão de recursos humanos. Conforme item 6.2 do Manual de Utilização do PBdoc, é possível a redefinição desse nível de acesso, o que pode gerar duas situações:

- Ao receber um processo/documento em que se verifique que o nível de acesso está incorreto, deve-se fazer a imediata redefinição;
- Ao se incluir dados pessoais em um processo que não constava, deve-se alterar o nível de acesso para um mais restrito, conforme o caso. Em qualquer caso, é importante que o servidor promova o equilíbrio entre a transparência e a proteção dos dados pessoais, analisando cada caso separadamente. Caso haja necessidade de disponibilizar os processos ou documentos a usuários externos, deve-se verificar ainda a necessidade de anonimização de dados pessoais.

7.2.6 **Dê preferência às Ferramentas Oficiais**

O Governo do Estado da Paraíba, por intermédio do Zimbra, disponibiliza ferramentas como e-mail que devem ser utilizados para realizar as atividades de rotina no trabalho.

Dúvidas
Contato: Adriana Borba
Canal: encarregada.lgpd@epc.pb.gov.br

EMPRESA
PARAIBANA DE
COMUNICAÇÃO