

## Sumário

1.	OBJETIVO.....	1
2.	ÂMBITO DE APLICAÇÃO .....	1
3.	DEFINIÇÕES.....	1
4.	DEFINIÇÕES.....	1
4.	DOCUMENTOS DE REFERÊNCIA .....	2
5.	RESPONSABILIDADES.....	3
7.	CONTROLE DE REGISTROS .....	5
8.	ANEXOS.....	5
9.	REGISTRO DE ALTERAÇÕES.....	5
10.	BASE LEGAL .....	Erro! Indicador não definido.
11.	DUVIDAS.....	Erro! Indicador não definido.
12.	HISTÓRICO DE ALTERAÇÕES .....	Erro! Indicador não definido.

## 1. OBJETIVO

Gerenciar riscos de proteção de dados e privacidade em processos, produtos, serviços e contratações do Grupo CPFL Energia, garantindo que o tratamento de dados pessoais de pessoa natural seja realizado observando as leis e regulamentações que regem a proteção de dados pessoais

## 2. ÂMBITO DE APLICAÇÃO

### 2.1. Grupo CPFL – a quem se aplica

Todas as empresas controladas e com governança orientada pelo Grupo CPFL Energia.

### 2.2. Departamentos


Todos os departamentos da Organização que (i) realizam ou pretendem realizar qualquer operação de tratamento de dados pessoais de pessoa natural em processos, produtos ou serviços de forma direta ou através de prestadores de serviços, parceiros ou fornecedores.

## 3. DEFINIÇÕES

Os principais termos contidos nesta norma envolvem as seguintes definições:

## 4. DEFINIÇÕES

**Agentes de tratamento:** controlador e operador;

 <i>Uso Interno</i>	Tipo de Documento: Procedimento
	Área de Aplicação: Proteção de Dados
	Título do Documento: Norma de Privacy by Design

**Autoridade Nacional de Proteção de Dados – ANPD:** órgão da administração pública responsável por zelar, implementar e fiscalizar as atividades de proteção de dados pessoais e cumprimento à LGPD em todo o território nacional;

**Banco de dados:** conjunto de dados pessoais, estabelecido em um ou vários locais físico ou eletrônico;

**Consulente:** pessoa física que realiza a consulta à Gerencia de Proteção de Dados

**Controlador:** pessoa física ou jurídica que toma decisões relacionadas ao tratamento de dados pessoais por meios próprios;

**Controlador independente:** pessoa física ou jurídica que toma decisões relacionadas ao tratamento de dados pessoais independentemente;

**Controlador conjunto:** duas ou mais pessoas físicas ou jurídicas que possuem uma intenção comum sobre as finalidades e meios de tratamento e tomam decisões em conjunto;

**Dado pessoal:** informação relacionada a uma pessoa física identificada ou identificável;

**Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

**Encarregado de dados:** pessoa indicada pelo controlador ou pelo operador para atuar como canal de comunicação entre o controlador, titular dos dados e a ANPD.

**Operador:** pessoa física ou jurídica que realiza o tratamento de dados pessoais em nome do controlador;

**Sub-operador/subcontratado:** pessoa física ou jurídica a quem é terceirizado, pelo operador, a realização do tratamento de dados pessoais;

**Titular dos dados:** pessoa física a quem se refere os dados pessoais que são objeto de tratamento;

**Tratamento:** toda operação realizada com os 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.

## 4. DOCUMENTOS DE REFERÊNCIA

### 4.1 Legislação

- Lei Geral de Proteção de Dados (Lei 13.709/2018)
- Código Civil Brasileiro
- Código de Processo Civil Brasileiro
- CLT

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18835	Procedimento Instrução	1.0	Jorge Alberto Bounassar	30/06/2021	2 de 13

- Marco Civil da Internet e Decreto Regulamentador
- Código de Defesa do Consumidor
- Procedimento para coleta de Termo de Consentimento n. 18.831
- Documento 0 – Documentos Normativos ("Norma Zero")

## 5. RESPONSABILIDADES

### Gerencias solicitantes

- Preencher a minuta padrão denominada Avaliação de Privacy By Design (Anexos I);
- Enviar a minuta padrão preenchida, via e-mail à Gerência de Proteção de Dados;
- Esclarecer dúvidas e fornecer informações e documentação adicional, mediante solicitação;
- Avaliar mitigadores orientados pela Gerencia de Proteção de Dados;
- Documentar planos de ação ajustados com a Gerencia de Proteção de Dados;
- Seguir orientações de compliance com as leis e regulamentações que regem a proteção de dados pessoais e a privacidade.

### Gerencia de Proteção de Dados

- Estabelecer os procedimentos para avaliação dos processos produtos e serviços que envolverem o tratamento de dados pessoais;
- Esclarecer dúvidas e orientar as áreas com relação as leis e regulamentações que regem a proteção de dados pessoais;
- Realizar a avaliação de riscos a privacidade e a proteção de dados orientando aplicação de mitigadores quando necessário;
- Dar orientação sobre segurança e prevenção a privacidade de titulares de dados pessoais;
- Recepcionar, tratar e responder as demandas das áreas por e-mail;
- Orientar a alteração do mapeamento de processos de tratamento de dados da gerencia solicitante, quando necessário;
- Gerar e monitorar os indicadores dos atendimentos realizados, para garantir que as requisições estão sendo respondidas de acordo com os procedimentos estabelecidos
- Melhoria contínua dos procedimentos internos e das análises relacionadas a proteção de dados pessoais.

## 5. Regras Básicas

### 5.1 Pontos a serem considerando antes do tratamento dos dados pessoais

Antes de realizar o tratamento dos dados pessoais orienta-se que a área que realizará o tratamento de dados reflita sobre o que segue:

1. Finalidade, adequação e necessidade. Para tratar um dado pessoal é necessário que exista um propósito legítimo e específico e que a categoria e os tipos de dados pessoais sejam compatíveis. Vale o seguinte exercício:
  - a) Para que eu preciso dos dados pessoais?
  - b) Para qual finalidade eu os utilizarei?
  - c) Qual o ganho para a Organização e para o titular?

- d) Considerando o meu propósito, quais são os dados que realmente eu devo utilizar para atingir a finalidade (a máxima é “menos é mais”).
- e) Utilizando o bom-senso, eu tenho segurança para falar publicamente que eu utilizo os dados pessoais definidos para atingir a finalidade?
- f) Os dados que eu vou utilizar foram gerados direto pela CPFL ou pelo Titular? Se foi pelo titular, o tratamento que eu vou fazer tem correlação com o propósito inicial que ele me forneceu a informação?
- g) Para atingir a finalidade que você definiu é realmente preciso trabalhar com dados pessoais de pessoa natural de forma que a identifique?

## 5.2 Reflexão sobre a hipótese autorizadora do tratamento dos dados pessoais

Embora caiba à Gerencia de Proteção de Dados realizar a definição da hipótese de tratamento de dados pessoais mais adequadas para atingir a finalidade estabelecida pelo consulente, vale uma reflexão inicial no momento da constituição ou na alteração de processos, produtos e serviços do Grupo CPFL Energia. Isto irá te ajudar a estruturar melhor o seu projeto e até mesmo refletir sobre os dados que irá coletar.

Portanto, sugerimos que a área consulente verifique a Tabela de Bases Legais (Anexo II) anexa e exercite seus conhecimentos em proteção de dados. Desta forma a Gerencia de Proteção de Dados ao avaliar sua solicitação poderá reforçar o uso das bases legais e te apoiar no novo modelo de tratamento de dados exigidos pela LGPD.

Atenção: o uso do consentimento como base legal autorizadora do tratamento de dados pessoais requer um maior cuidado em sua estruturação e também exige um processo de gestão, pois o titular de dados pessoais poderá retirar a sua autorização a qualquer tempo (vide Procedimento para coleta de Termo de Consentimento - GED n.18.831).

## 5.3 Formulário para avaliação de impacto a privacidade

Preencher o documento padrão (Anexo I) com informações detalhadas sobre as operações de tratamento de dados pessoais possibilitando que a área de proteção de dados possa identificar.

O documento deve ser enviado por e-mail em versão editável para que possamos fazer eventuais ajustes em eventuais entendimentos sobre as operações de tratamento de dados.

Este documento fará parte da análise de proteção de dados e portanto, será armazenado em nosso banco de dados juntamente com o parecer da Gerência de Proteção de Dados como documentação oficial do Grupo CPFL

## 5.4 Avaliação de Riscos a Privacidade

Através do documento padrão, a Gerência de Proteção de Dados realizará a avaliação de impacto a privacidade do processo, produto ou serviço e enviará o seu parecer à área solicitante.

Havendo orientação para implementação de ações mitigatórias de riscos identificados a área consultante deverá entrar em contato com a Gerência de Proteção de Dados para operacionalizar o Plano de Ação sugerido.

O Plano de Ação, além das ações necessárias conterá prazo para implementação e será ajustado pelo Gestor Direto da área solicitante.

A hipótese das Partes não chegarem a um acordo com relação ao plano de ação necessário para mitigação de riscos do processo, produto ou serviços avaliado a Gerência de Proteção de Dados agendará reunião de alinhamento com a Diretoria a qual reporta juntamente com a Diretoria do departamento consultante para melhor discussão e ponderação sobre o tema.

Não havendo alinhamento na reunião acima citada, para que haja o tratamento de dados pessoais sem a implementação dos mitigadores orientados pela Gerência de Proteção de Dados as áreas seguirão os procedimentos internos já estabelecido para tomada de riscos pelo Grupo CPFL Energia.

## 7. CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Anexo I	Pasta do Sharepoint da Gerência de Proteção de Dados	Restrição de Acesso	Por área	Permanente	Arquivo Inativo
Anexo II	Pasta do Sharepoint da Gerência de Proteção de Dados	Restrição de Acesso	Por área	Permanente	Arquivo Inativo

## 8. ANEXO

Anexo I – Avaliação de Privacy By Design/By Default

Anexo II – Tabela de Bases Autorizadoras

## 9. REGISTRO DE ALTERAÇÕES

### 9.1 Colaboradores

Empresa	Área	Nome
CPFL Renováveis	PAP	Denise Ramos de Lima
CPFL Renováveis	PAP	Nadine Emile Prado Marostegan



Uso Interno

Tipo de Documento: Procedimento  
Área de Aplicação: Proteção de Dados  
Título do Documento: Norma de Privacy by Design

CPFL Brasil	PAP	Thiago Bento dos Santos
CPFL Jaguari	PAP	Sara Cristina Coraini de Souza

## 9.2 Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
Não aplicável	Não aplicável	Documento em versão inicial.



Uso Interno

Tipo de Documento: Procedimento  
Área de Aplicação: Proteção de Dados  
Título do Documento: Norma de Privacy by Design



## ANEXO I

### Avaliação de Privacy By Design – Processo, Produtos e Serviços

I – EMPRESA DO GRUPO CPFL ENERGIA	[Empresa do grupo que decide sobre o que, como, onde, porquê e para qual propósito realizará ações de tratamento de dados pessoais]
II - Área da CPFL responsável pelo Processo	[informações do departamento indicado no Data Mapping - Sigla e Nome do Departamento]
III – Colaborador consultente	Nome: E-mail:
IV – Superior Hierárquico	[nome Gestor imediato]
V – Responsável pela avaliação	Nome: [colaborador da área de proteção de dados] E-mail: [e-mail colaborador da área de proteção de dados] Comunicador oficial: Teams
VI – Data da consulta	[dia/mês/ano]
VIII – Nome do Projeto	[nome que o projeto é conhecido na Organização]
IX – Documentos complementares	[juntar documentos que possam aclarar o propósito do projeto, identificar a jornada de coleta de dados pessoais, dentre outros]

<b>1. Descrição do Propósito do Tratamento dos dados</b> [indicar o objetivo do projeto ou do processo]	
<b>2. Identificação da categoria do titular dos dados pessoais</b> ( ) Clientes e consumidores em geral ( ) Participantes de eventos ( ) Participantes de projetos educacionais e pesquisa; ( ) Visitantes ( ) Candidatos, colaboradores e ex colaboradores ( ) Familiares de empregados ( ) Representantes legais e sócios de fornecedores e prestadores de serviços ( ) Empregados de fornecedores e prestadores de serviços ( ) Investidores	
<b>3. Informar todo os dados pessoais de pessoa natural tratados neste projeto/processo (utilizar a relação de dados pessoais anexa como base) e respectiva necessidade da coleta para o propósito informado[relacionar, de forma granular - um por linha -, todos os dados utilizado observando o disposto na lista exemplificativa anexa]</b>	
<b>Relação de dados pessoais</b> [informar o dado pessoal de acordo com a lista exemplificativa]	<b>Finalidade de Uso</b> [indicar o porquê a informação é essencial para atingir o propósito informado]
<b>4 Os dados pessoais fornecidos pelo titular dos dados?</b> ( ) Sim ( ) Não	
<b>5 Se a resposta for negativa descrever de onde os dados são coletados</b>	

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18835	Procedimento Instrução	1.0	Jorge Alberto Bounassar	30/06/2021	7 de 13



Uso Interno

Tipo de Documento: Procedimento  
Área de Aplicação: Proteção de Dados  
Título do Documento: Norma de Privacy by Design

<b>[identificar a fonte da informação – terceiro, CPFL, etc)</b>
<b>6. Indicar o local de onde os dados são extraídos</b>
<b>[Indicar nome do sistema, diretório, sharepoint, etc)</b>
<b>7. Se os dados pessoais são compartilhados com terceiros informar, a, identificar:</b>
<b>a) Razão/Denominação Social do Parceiro/PrestServiços/Fornecedor:</b>
<b>a) para qual finalidade:</b>
<b>b) relação de dados pessoais enviados:</b>
<b>c) canal de compartilhamento (e-mail, SFTP, Connect direct, Web...)</b>
<b>d) se possui contrato adequado a LGPD ( ) Sim ( ) Não</b>
<b>8. Comentário</b>
<b>[Fornecer outras informações que entende relevante para avaliação]</b>



## Anexo II – Tabela de Hipóteses Autorizativas

Hipóteses Legais	Dados Pessoais (Art. 7º)	Dados Pessoais Sensíveis (Art. 11)	Obs
Consentimento	X	X	Autorização livre, informada, inequívoca e para finalidade específica. Pode ser suspensa/cancelada pelo titular do dado a qualquer momento. Se dados sensíveis: específica e destacada
Cumprimento de obrigação legal ou regulatória	X	X	Necessário informar a lei e/ou regulamentação que determina que o tratamento de dados pessoais deve ser realizado.
Execução do contrato ou de procedimentos contratuais preliminares	X	X	Quando o controlador realiza o tratamento de dados pessoais com o propósito de realizar, posteriormente, um contrato ou qualquer outro instrumento que possa reger a relação jurídica entre o Grupo CPFL Energia e o Titular, ou ainda, para executar atividades decorrentes do contrato ou do instrumento jurídico celebrado entre as parte já citadas.
Exercício regular do direito em processo judicial, administrativo ou arbitral	X	X	Para defesa do Grupo CPFL Energia e/ou de terceiros
Pela administração pública, para o tratamento e uso compartilhado de dados necessários a execução de políticas públicas previstas em leis e regulamentos	X	X	Para dados pessoais comuns o respaldo poderá se dar em contratos, convênios ou instrumentos congêneres.
Para a realização de estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.	X	X	



Uso Interno

Tipo de Documento: Procedimento  
Área de Aplicação: Proteção de Dados  
Título do Documento: Norma de Privacy by Design

Proteção da vida ou da incolumidade física do titular ou de terceiro	X	X	
Tutela da saúde, em procedimento realizado por profissionais da área da saúde, serviços de saúde ou por entidades sanitárias.	X	X	
Garantia de prevenção a fraude e à identificação do titular nos processos de identificação e autenticação de cadastros em sistemas eletrônicos	Não há	X	
Proteção ao crédito	X	Não há	
Interesse legítimo do controlador ou de terceiros	X	Não há	Necessário equilibrar a balança = Legítima expectativa do titular, finalidade legítima do controlador, garantia dos direitos fundamentais do titular (como por ex. saída mediante requerimento)



Uso Interno

Tipo de Documento: Procedimento  
Área de Aplicação: Proteção de Dados  
Título do Documento: Norma de Privacy by Design

## Anexo II – Lista Exemplificativa de Dados Pessoais

**Esta cor indica Dado Sensível**

Associação sindical
Certidão de nascimento
Certidão de óbito
Cidadania
Código de verificação do cartão de crédito ou de cartão de débito (CVV, CVC)
Conjunto de habilidades/histórico de educação/histórico profissional
CPF
Crenças religiosas ou filosóficas
Dados salariais e/ou de remuneração
Data de contratação
Data de expiração do cartão de crédito ou cartão de débito
Data de nascimento (com ou sem indicação do ano específico)
Detalhamento da conta de energia
Detalhes da conta de membro de companhia aérea
Detalhes da conta de membro de rede de Hotel
E-mail comercial
E-mail pessoal
Endereço comercial
Endereço de IP
Endereço de residência
Endereço IP comercial
Especificar países para os quais a conta tem acesso, informações pessoais (PI) ou dados pessoais (PD)
Estado civil / certidão de casamento
Fotos de rosto completo e imagens de comparação
Gênero (masculino/feminino)
Histórico de consumo
Histórico de transações da conta
Idade
Identificadores de dispositivo do cliente que está sendo capturado tal como o endereço IP, o número de série do dispositivo, etc.
IDs de usuário comercial
Informação biométrica/genética
Informações coletadas através de "cookies"
Informações confidenciais do cliente
Informações confidenciais do governo

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18835	Procedimento Instrução	1.0	Jorge Alberto Bounassar	30/06/2021	11 de 13

Informações de imposto de renda
Informações de manutenção hipotecária: ESCRITURA
Informações de saldo da conta
Informações dos dependentes
Informações fornecidas para obter um empréstimo/outro produto/serviço financeiro, como devolução de imposto, extratos bancários, comprovante de renda, etc.
Informações pessoais de saúde
Informações sobre empréstimos: CONTRATO
Informações sobre empréstimos: HIPOTECA
Informações sobre empréstimos: LIBERAÇÃO
Informações/dados pessoais coletados pela conta pertencem aos funcionários ou prospects da empresa
Informações/dados pessoais recolhidos pela conta pertencem aos clientes finais do cliente
Informações/dados pessoais recolhidos pela conta pertencem aos fornecedores, parceiros de negócios ou clientes finais da empresa
Informações/dados pessoais recolhidos pela conta pertencem aos funcionários do cliente
Local de emprego/número de funcionário
Lugar de nascimento
Montante financeiro das deduções da folha de pagamento para planos de saúde familiar
Nacionalidade
Nome antigo
Nome da pessoa
Número da conta bancária
Número de identificação do contribuinte
Número de identificação do veículo
Número de identificação nacional
Número de licença do condutor (CNH)
Número de telefone comercial
Número de telefone pessoal
Número do cartão de crédito ou cartão de débito (parcial)
Número do cartão de crédito ou do cartão de débito (completo)
Número do passaporte
Número do PIN ou senha para acessar informações financeiras ou de seguro, e outras senhas
Números de identificação do seguro de saúde
Opinião política
Orientação sexual
Origem racial ou étnica
Planos de viagem ou itinerário
Pontuação de crédito que permite aos credores tomar a decisão de empréstimo ou



Uso Interno

Tipo de Documento:	Procedimento
Área de Aplicação:	Proteção de Dados
Título do Documento:	Norma de Privacy by Design

aprovação de cartão de crédito
Previdência/assistência social recebida
Private Key utilizada para autorizar a utilização eletrônica de documentos (por exemplo, através de assinatura eletrônica)
Referência ou verificação de antecedentes
Registros criminais
Registros de trabalhos
Relatórios de crédito financeiro
Quaisquer outros atributos de dado pessoal acessível na conta
Outros (indicar no campo Comentários Adicionais)