37. Política de Privacidade de Dados - LGPD

1 Identificação do Controlador

A Cooperativa de Crédito Cogem, inscrita no CNPJ sob o nº 44.401.800/0001-90, com sede na Rua José Versolato, 111, Torre B, salas 2607 / 2608 |Condomínio Domo Business Baeta Neves | São Bernardo do Campo – SP | CEP: 09750-730, na qualidade de Controladora de Dados, é responsável pelas decisões referentes ao tratamento de dados pessoais, nos termos da LGPD (Lei nº 13.709).

2 Objetivo

Estabelecer diretrizes, princípios e conceitos de Privacidade e Proteção de Dados pessoais/privados e informações sensíveis dos ativos de informações adotados pela Cogem inerentes ao disposto na Lei nº 13.709 (LGPD).

A Cogem através de seus colaboradores, fornecedores, prestadores de serviços, precisa realizar inúmeras operações de tratamento de dados pessoais e está comprometida em assegurar que essas operações de tratamento de dados estejam alinhadas às melhores práticas de mercado e às exigências legais.

3 Abrangência

Esta Política aplica-se a todas as áreas internas e atividades da Cogem.

4 Conceitos e Siglas

A sigla LGPD está sendo adotada nesta Política para designar a Lei Geral de Proteção de Dados (Lei nº 13.709).

Essa Lei, sancionada em 14 de agosto de 2.018, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Expressões utilizadas na Gestão de Privacidade e Proteção de Dados:

- Arquivamento: cópia de dados de um dispositivo de armazenamento a outro para que possa ser recuperado em caso de auditoria ou consulta de dados históricos, onde a mídia de destino é armazenada em cofre;
- Backup ou Salvaguarda: salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de recuperação em caso de incidente ou necessidade de restauração, ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada;
- Colaborador: funcionário, estagiário, prestador de serviço, terceirizado, fornecedor, menor aprendiz ou qualquer outro indivíduo ou organização que venham a ter relacionamento profissional, direta ou indiretamente, com a Cogem;
- Criptografia: mecanismo de segurança que visa proteger as informações permitindo que

somente o receptor da informação circulada leia-a com facilidade;

- Dados pessoais: é toda e qualquer informação relacionada a pessoa natural identificada ou identificável. Entre os exemplos de dados pessoais podemos citar o nome, RG, CPF, e-mail, telefone fixo e celular, endereço residencial etc.;
- Dados pessoais sensíveis: é todo dado pessoal que pode gerar qualquer tipo de discriminação, tais como os dados 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;
- Titular: pessoa natural a quem se referem os dados pessoais;
- Tratamento: 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;
- Disponibilidade: garantia de que as informações e os Recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso;
- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais;
- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- Encarregado: pessoa ou profissional designado pela organização que estará envolvido em todas as questões relacionadas com a proteção de dados privados, pessoais e/ou pessoais;
- Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- Anonimização: processos e técnicas por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- Dado anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. O dado anonimizado não é considerado dado pessoal para fins de aplicação da LGPD;
- Pseudoanonimização: processos e técnicas por meio dos quais um dado tem sua possibilidade de associação dificultada. O dado pseudoanonimizado é considerado dado pessoal para fins de aplicação da LGPD, tendo em vista a possibilidade de associação desse dado a uma pessoa natural;
- Evento: uma ocorrência que pode ser observada em uma rede ou sistema. Eventos incluem, mas não se limitam a um usuário conectando em um compartilhamento de arquivos, um servidor recebendo uma requisição de uma página web ou um usuário encaminhando um e- mail;
- Incidente: um evento adverso em uma rede, e/ou sistema, ou a ameaça de ocorrência de tal evento. Um incidente é uma violação ou ameaça eminente de violação de uma política de segurança ou boas práticas, que tenha causado prejuízo ou tentativa de causar;
- Incidente de segurança da informação: ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à Política de Segurança da Informação ou documentos complementares, falha de controles ou situação previamente desconhecida, que possa ser relevante à segurança da informação;
- Informação: é o conjunto de dados que, processados ou não, podem ser utilizados para

produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato;

- Recursos de TIC - Recursos de Tecnologia da Informação e Comunicação: hardware, software, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações;
- Restauração ou Restore: processo de recuperação dos dados salvaguardados e sua colocação em produção;
- Risco: combinação dos impactos advindos da ocorrência de um evento indesejado relacionado à segurança da informação e da probabilidade de sua ocorrência;
- Segurança da Informação: é a preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a informação dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidades de transação; e
- Tentativa de Burla: fazer esforços para não respeitar ou tentar violar as diretrizes estabelecidas nos normativos da Cogem.

5 Princípios de Proteção de Dados Pessoais

A Cogem dedica o devido cuidado, confidencialidade e privacidade das informações de associados que são acessadas por seus funcionários e colaboradores internos.

O mesmo princípio de preservação da segurança, confidencialidade e privacidade das informações aplicadas aos associados se estende também aos parceiros comerciais, fornecedores de serviços de tecnologia e demais prestadores de serviços em geral.

As informações coletadas serão usadas internamente apenas para os fins especificados que motivaram sua obtenção não devendo nunca serem usados para fins pessoais ou diferentes do seu propósito:

- Os dados privados, pessoais e/ou sensíveis do titular devem ser processados de forma legal, justa e transparente em relação aos seus titulares;
- Devem ser coletados para fins específicos, explícitos e legítimos e não processados posteriormente de maneira incompatível com esses objetivos;
- O tratamento posterior para fins de arquivo no interesse público, para fins de investigação científica ou histórica ou para fins estatísticos não é considerado incompatível com os fins iniciais;
- Devem estar adequados, relevantes e limitados ao uso necessário e em relação aos fins para os quais são destinados e/ou processados;
- Quando solicitado pelo titular e/ou quando necessário, os dados devem ser atualizados. Todas as medidas razoáveis devem ser tomadas para garantir que os dados pessoais imprecisos, sejam apagados e/ou retificados no tempo hábil e determinado pelo titular, observando os fins de destino para os quais os dados são armazenados, retidos e/ou processados;
- Devem ser mantidos num formato que permita a identificação dos titulares de dados por um período não superior ao necessário para os fins para os quais os dados pessoais são tratados;

- Os dados pessoais podem ser armazenados por períodos mais longos, desde que os dados pessoais sejam processados exclusivamente para arquivamento no interesse público, para fins de histórico das operações ou para fins estatísticos sujeitos à implementação das medidas técnicas e organizacionais apropriadas exigidas pela LGPD – Lei Geral de Proteção da Dados, a fim de preservar os direitos e liberdades das pessoas; e
- Devem ser processados de maneira que garantam a segurança apropriada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas ou organizacionais apropriadas.

6 Tratamento de Dados Pessoais/Privados Sensíveis

Para todos os ativos de informação que contenham dados pessoais/privados e informações sensíveis, sejam eles em meio magnético, ótico ou papel, devem ser observados os seguintes cuidados:

- Garantir que estejam guardados em lugar seguro e adequado, de acordo com as melhores práticas de segurança da informação, fazendo valer dos melhores esforços e investimentos necessários para a salvaguarda destas informações;
- Deve ser realizada a verificação do tempo de retenção e manipulação dos dados pessoais/privados e informações sensíveis e seu descarte assim que sua utilidade atender os fins de destino e em conformidade com o Termo de Aceite e Acordo de Privacidade estipulado; e
- Os ativos de informação contando dados pessoais/privados e informações sensíveis destinados aos propósitos específicos e interesses da COGEM devem estar identificadas quanto ao seu conteúdo, indicando, quando necessário, o prazo de retenção e observações sobre ela.

7 Titulares dos dados pessoais

São titulares dos dados pessoais alcançados por essa Política de Privacidade e Proteção de dados: associados, funcionários, prestadores de serviço, fornecedores e terceiros em geral que possuam vínculo indireto com a Cooperativa para adquirir ou fornecer algum benefício.

7.1 Direitos como Titular de Dados

O titular de dados pessoais tem direito a obter da COGEM, a qualquer momento e mediante requisição, conforme previsto no art. 18 da LGPD:

- **Confirmação e Acesso:** Confirmação da existência de tratamento e acesso aos dados.
- **Correção:** Correção de dados incompletos, inexatos ou desatualizados.
- **Anonimização e Bloqueio:** Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade.
- **Portabilidade:** Portabilidade dos dados a outro fornecedor, conforme regulamentação da ANPD.
- **Eliminação:** Eliminação dos dados tratados com base no consentimento, ressalvadas as hipóteses legais de conservação.

- **Informação:** Informação sobre entidades com as quais realizou uso compartilhado e sobre a possibilidade de não fornecer consentimento.
- **Revogação:** Revogação do consentimento a qualquer tempo. A COGEM disponibilizará canais específicos para o exercício desses direitos e observará os prazos legais para resposta.

8 Dados Pessoais Coletados - Regras para utilização

Os dados pessoais podem ser coletados dos Titulares dos Dados para assuntos relacionados a fornecimento de produtos/prestação de serviços efetuado diretamente ao Titular dos Dados ou vínculo trabalhista. No que se refere aos serviços e produtos relacionados à instituição financeira, alguns deles poderão beneficiar terceiros, ou seja, filho(s) até 18 (dezoito) anos ou cônjuge/companheiro do Titular dos Dados.

Abaixo seguem as categorias de dados pessoais:

Categoria de Dados Pessoais	Dado Pessoal Tratado
Nome e iniciais	Nome Completo
Características Pessoais	Idade Data e local de nascimento Gênero Nacionalidade Naturalidade Estado Civil Fotografia
Dependentes	Identificação de cônjuge/companheiro (a) Identificação filhos
Identificação	CPF RG CTPS CNH
Informações residenciais	Endereço Residencial Telefone Residencial E-mail pessoal Telefone Celular pessoal
Informações profissionais	Ocupação/Cargo Endereço comercial E-mail comercial Telefone comercial Data de admissão
Informações financeiras	Conta corrente
Informações fornecidas quanto da navegação por meio de dispositivos móveis	Cookies Endereço de IP
Outros	Histórico de atendimento: SAC/Ouvidoria/Canal de denúncias/Reclame Aqui/Proconsumidor/Consumidor.GOV/RDR Uso de imagem

9 Dados pessoais de menores

Quando coletados Dados Pessoais de crianças ou adolescentes, essa coleta é realizada para prestação de serviços ou fornecimento de produtos que beneficiam ao próprio menor, devidamente representado pelo seu tutor, respeitadas suas legítimas expectativas, direitos e liberdades fundamentais.

Para fins de admissão à Cooperativa, os dados coletados serão os acima descritos (tabela) e para outros fins que também visa prestação de serviços ou fornecimento de produtos para beneficiar esse menor, os dados coletados serão tão somente: nome, CPF e data de nascimento, tendo em vista que precipuamente instruirá documentos para crédito específico que beneficie, por exemplo, seus estudos, passeio ou outras atividades, conforme normativos internos. Os referidos dados sensíveis poderão ser coletados, inclusive com declaração ou prova de grau de parentesco para os mesmos fins e em todos os casos serão respeitadas as exigências legais para o tratamento desses Dados Pessoais.

10 Como os dados pessoais são coletados

Os dados podem ser fornecidos diretamente pelo Titular do Dado (cadastro, empréstimo etc.), ou podem ser fornecidos pelas empresas conveniadas ou por fontes externas legítimas, como: instituições do sistema financeiro, *bureaus* de crédito, órgãos públicos, correspondentes, empresas ou órgãos com os quais a Cogem possua vínculo ou relação, seja ela direta ou indireta. Os dados também podem ser obtidos de fontes públicas e/ou acessíveis publicamente, como Internet, meios de comunicação, mídias sociais e registros públicos e de outras fontes, conforme permitido na legislação aplicável.

11 Bases legais e finalidades

Os Dados Pessoais indicados acima são recebidos e tratados de acordo com as bases legais previstas na Lei Geral de Proteção de Dados (LGPD) para as seguintes atividades:

- Admissão de associados, atualização cadastral e devida identificação do associado e/ou seus filhos ou cônjuge/companheiro (a), conforme disposto anteriormente;
- Avaliar o risco de crédito, análise de riscos, verificação de SCR-BACEN, pesquisa nos órgãos de proteção ao crédito, ou seja, verificação das condições para concessão de crédito;
- Fornecer produtos financeiros;
- Cumprir contrato (inclusive na fase pré-contratual);
- Fornecer informações relativas a algum contrato, produto ou serviço da Cooperativa ao próprio Titular dos Dados;
- Dar atendimento e suporte pelos canais próprios, para prestar informações ou enviar comunicados sobre contratos, produtos, serviços ou questões de interesse do Titular dos dados, a ele mesmo, bem como para oferecer-lhe produtos de acordo com seu perfil;
- Prestar assistência ao Titular dos Dados;
- Efetuar comprovação de transações;
- Estabelecer estatísticas individuais, com base, por exemplo, na análise de transações, contribuindo para a definição da sua pontuação de risco de crédito;
- Formação cooperativista e financeira de associados e treinamento de colaboradores;

- Prevenção a fraudes e atos ilícitos ou aperfeiçoamento de processos, produtos e serviços, com a finalidade também de identificar, prevenir e gerenciar eventuais riscos;
- Realizar ações de marketing e campanhas promocionais, bem como avaliar comportamento de navegação e perfil dos usuários e associados;
- Apontamento e consulta junto aos órgãos de proteção ao crédito (SERASA, SCPC, dentre outros);
- Ingresso ou defesa em processos administrativos, judiciais ou reclamações pré-processuais;
- Seleção e contratação de empregados ou prestadores de serviços;
- Controle de acesso de visitantes como método do processo de segurança da empresa, colaboradores e terceiros; e
- Cumprimento de obrigações legais, procedimentos previstos nas resoluções e circulares do Banco Central do Brasil, inclusive como medida de prevenção do crime de lavagem de dinheiro e demais atos ilícitos, e cumprir ordens e decisões arbitrais, administrativas ou judiciais.

Todos os Dados Pessoais e informações, dispostos na tabela em epígrafe, são tratados como confidenciais, salvo se o próprio Titular dos Dados divulgá-las, e utilizados conforme as seguintes bases legais: execução de contrato ou procedimentos preliminares relacionados a contrato, cumprimento de obrigação legal ou regulatória, para exercício regular de direito, proteção da vida ou incolumidade física, para, eventualmente, realização de estudos por órgão de pesquisas, para atender interesses legítimos, exceto de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais e para proteção do crédito.

Quando solicitado pelos proprietários e detentores dos direitos dos dados pessoais/privados e informações sensíveis, a Cogem deve providenciar e viabilizar os canais de comunicação, portais de internet e/ou plataformas sistêmicas, cumprindo com a solicitação de atualização e/ou exclusão para que as solicitações sejam atendidas, fazendo valer dos melhores esforços e investimentos necessários para cumprir com todas as responsabilidades definidas na LGPD - Lei Geral de Proteção de Dados e demais diretrizes desta norma.

12 Mecanismos e controles

A Cogem deve elaborar e garantir que exista um relatório de impacto, descrevendo os processos e procedimentos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Os processos e procedimentos de proteção dos dados estão registrados no documento denominado “ROPA”.

ROPA é a sigla para Registro de Operações de Tratamento de Dados Pessoais, um documento exigido pela Lei Geral de Proteção de Dados (LGPD). O ROPA é um documento fundamental para que a Cogem atenda às diretrizes desta política.

Existindo o compartilhamento de informações privadas, pessoais e/ou sensíveis com terceiros, os contratos devem ser revisados e garantir a sua conformidade com a LGPD- Lei Geral de Proteção de Dados.

Para garantir que seu processamento de dados seja legal, justo e transparente, a Cogem deve manter a rastreabilidade dos dados privados e controlá-los durante todo o seu ciclo de vida de utilização, através de sistemas de controle e registro de dados privados.
O sistema de registro e controle de dados privados deverão ser revisados de acordo com alterações de processos relevantes e de acordo com novos normativos.

13 Retenção e/ou guarda para propósitos/fins legais

Os dados pessoais serão conservados pelo período máximo exigido para cumprir com as obrigações legais e regulamentares aplicáveis, ou por período relacionado com os requisitos operacionais da Cooperativa, ou seja, depende do propósito e da natureza do tratamento dos Dados.

Quando atividades e/ou campanhas de comunicação com os titulares forem enviadas com base em seu consentimento, a opção para o titular revogar o seu consentimento deve estar claramente disponível e os sistemas devem estar em pleno funcionamento garantindo que essa revogação seja refletida com precisão nos sistemas da Cogem.

14 Minimização de dados

A Cogem deve garantir que os dados pessoais sejam adequados, coerentes, relevantes e limitados ao que é necessário e para os fins aos quais são processados.

15 Arquivamento / remoção

A Cogem possui a Política de Retenção de Dados Pessoais e Sensíveis garantindo que os dados privados/pessoais sejam mantidos por tempo necessário aos fins específicos, explícitos e legítimos.

A Política de Retenção e Dados Pessoais e Sensíveis e a Política de Backup devem considerar quais dados devem ser mantidos, por quanto tempo e os motivos específicos, explícitos e legítimos de sua retenção e/ou armazenamento.

16 Segurança

O acesso aos dados privados/pessoais deve estar limitado aos colaboradores autorizados e os sistemas, controles, normas e procedimentos de segurança de dados privados/pessoais, evitando o compartilhamento não autorizado de informações.

Os dados privados/pessoais devem ser excluídos com segurança de modo que sejam irrecuperáveis.

17 Evidência digital

Os colaboradores e usuários autorizados para o processamento de dados pessoais/privados da Cogem devem coletar evidências (ex. print da tela, foto) em casos de incidentes que sejam contrários aos normativos da Cogem, à ética ou à legislação nacional vigente, além de informar o Departamento de Tecnologia da Informação e o Compliance, sempre que necessário.

18 Cuidados Gerais

A quebra de sigilo de informações acarreta responsabilidade civil e o responsável poderá ser acionado conforme penalidades previstas na legislação brasileira.

A Cogem mantém o compromisso de manter em sigilo e segurança as informações pessoais de seus associados, parceiros e fornecedores, tanto aqueles coletados através de Fichas Cadastrais preenchidas como também aqueles obtidos através de seu site considerando o seguinte:

- **Coleta e uso das informações:** As informações coletadas de associados, parceiros ou fornecedores são acessadas somente por funcionários autorizados, sendo proibida e passível de punição a veiculação, venda e divulgação a terceiros sem prévio conhecimento e autorização dos interessados.
- **Segurança de dados:** Os dados coletados e inseridos nos sistemas internos são protegidos de acessos não autorizados ou invasões externas através de utilização de softwares de segurança e firewall de forma a manter a integridade e sigilo das informações obtidas.
- **Senhas:** O acesso aos sistemas internos que contém informações de clientes, parceiros ou fornecedores é feito através de login e senha de acesso individual por usuário de forma a evitar acessos não autorizados e/ou ações fraudulentas.
  Os colaboradores não devem divulgar, ceder ou emprestar seus devidos logins e senhas de acesso a terceiros. As orientações sobre a composição de senhas estão contidas na Política de Segurança da Informação e Cibernética.

19 Regulamentação Associada

A Lei nº 13.709 de 14 de agosto de 2.018 (LGPD) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

20 Responsabilidade e Atribuições

20.1 Conselho de Administração

- Aprovar a Política interna de Privacidade e Proteção de Dados – LGPD; e
- Apoiar as áreas e incentivar a conscientização, capacitação e sensibilização dos colaboradores que desempenham qualquer atividade de tratamento de dados pessoais dentro da Cogem.

20.2 Diretoria Executiva

- Apoiar a área responsável pelas atividades que envolvem dados pessoais; e
- Aprovar o relatório RIPD – Relatório de Impacto a Proteção de Dados Pessoais.

20.3 Gerência

- Apoiar a área responsável pelas atividades que envolvem dados pessoais;

- Aprovar o relatório RIPD – Relatório de Impacto a Proteção de Dados Pessoais;
- Apoiar a elaboração e revisão desta política; e
- Garantir ao encarregado o acesso direto às pessoas de maior nível hierárquico dentro da organização, aos responsáveis pela tomada de decisões estratégicas que afetem ou envolvam o tratamento de dados pessoais, bem como às demais áreas da organização.

20.4 RH

- Gerenciar programas de treinamentos de privacidade de dados pessoais a todos os colaboradores da Cogem.

20.5 Tecnologia da Informação

- Definir, monitorar e executar as rotinas de proteção de dados privados/pessoais, guarda e retenção para fins legais, minimização, criptografia e/ou anonimização;
- Gerenciar o software de gestão de dados pessoais, denominado Be Compliance;
- Atualizar e revisar os dados pessoais cadastrados na plataforma Be Compliance;
- Garantir o perfeito funcionamento e manutenção dos recursos e softwares destinados a proteção de dados pessoais/privados;
- Elaborar relatório RIPD – Relatório de Impacto a Proteção de Dados;
- Gerenciar o mapeamento de processos que tratam dados pessoais juntamente com as áreas responsáveis;
- Revisar e atualizar esta política quando ocorrer alteração relevante;
- Zelar pela integridade, confidencialidade, disponibilidade, autenticidade e legalidade dos dados pessoais/privados armazenados na execução das atividades de proteção de dados pessoais/privados e salvaguarda de cópias de segurança;
- Instalar, desinstalar e atualizar agentes de proteção, criptografia e/ou anonimização de dados pessoais/privados;
- Definir horários, datas e frequências em que serão executadas as rotinas de criptografia, anonimização, salvaguarda, retenção legal e/ou proteção de dados pessoais/privados; e
- Gerenciar as chaves de criptografia utilizadas nas atividades de execução de proteção de dados pessoais/privados (quando utilizadas).

20.6 Encarregado de Dados

Responsável pelo entendimento de todo ciclo de vida dos dados pessoais instruindo os colaboradores para que todas as atividades relacionadas a privacidade e proteção de dados estejam em conformidade com a Lei Geral de Proteção de Dados.
Visando o acompanhamento dos trabalhos relacionados à LGPD, o Encarregado de Dados nomeado ficará responsável pelo desenvolvimento das atividades abaixo:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências cabíveis;
- Receber comunicações da ANPD e adotar providências;
- Orientar os colaboradores e os contratados do agente de tratamento a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- Executar as demais atribuições determinadas pelo agente de tratamento ou

estabelecidas em normas complementares.

Ao receber comunicações da ANPD, o encarregado deverá adotar as medidas necessárias para o atendimento da solicitação e para o fornecimento das informações pertinentes, adotando, entre outras, as seguintes providências:

- Encaminhar internamente a demanda para as unidades competentes;
- Fornecer a orientação e a assistência necessárias aos agentes de tratamento; e
- Indicar expressamente o representante do agente de tratamento perante a ANPD para fins de atuação em processos administrativos, quando esta função não for exercida pelo próprio encarregado.

20.7 Colaboradores

- Zelar pelos dados contidos nos sistemas internos utilizando-os apenas no uso exclusivo de suas atividades;
- Manter em segredo a sua senha de acesso, além de utilizar as tecnologias disponibilizadas pela Cogem;
- Proteger a privacidade das informações perante terceiros ou pessoas não autorizadas ao acesso das informações; e
- Cumprir rigorosamente todas as determinações e princípios dispostos nesta Política.

21 Canais de Comunicação

Em caso de dúvidas ou questões sobre a Política de Privacidade de Dados – LGPD e práticas de segurança e proteção de dados praticados pela Cogem, o titular deverá endereçar sua demanda ao nosso atendimento de Tratamento de Dados Pessoais, pelo canal mencionado abaixo:

- Encarregado de Dados: Carla Lonclofe Ilinski
- E-mail: tratamentodedados@Cogem.com.br

22 Comunicação de Incidentes de Segurança

A Cogem adota medidas técnicas e organizacionais para prevenir, identificar e mitigar incidentes de segurança que possam comprometer a integridade, a confidencialidade ou a disponibilidade de dados pessoais. No entanto, em casos em que incidentes de segurança sejam identificados, seguirá os seguintes procedimentos para assegurar conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

Identificação e Avaliação do Incidente: Qualquer incidente envolvendo dados pessoais será imediatamente reportado ao Encarregado de Proteção de Dados (DPO) e ao Departamento de Infraestrutura de TI.

Será realizada uma análise inicial para determinar:

- A natureza e o escopo do incidente;
- Os tipos de dados afetados;

- Os titulares potencialmente impactados; e
- A gravidade e os riscos associados ao incidente.

22.1 Comunicação à Autoridade Nacional de Proteção de Dados (ANPD)

Em casos em que o incidente apresente risco ou dano relevante aos titulares, a Autoridade Nacional de Proteção de Dados (ANPD) será notificada no prazo de até 3 (três) dias úteis após a identificação do incidente.

A notificação à ANPD incluirá, no mínimo:

- Descrição da natureza dos dados pessoais afetados;
- Identificação dos titulares envolvidos;
- Indicação das medidas técnicas e de segurança adotadas antes do incidente;
- Riscos relacionados ao incidente; e
- Medidas implementadas para reverter ou mitigar os danos.

22.1.1 Comunicação aos Titulares dos Dados: Caso o incidente represente riscos significativos aos direitos dos titulares, estes serão informados de forma clara e acessível por meio de canais apropriados, como e-mail, telefone ou notificações no site oficial.

A comunicação incluirá:

- A descrição do incidente;
- Os possíveis impactos;
- Medidas tomadas para conter o incidente; e
- Recomendações para que os titulares protejam seus dados, quando aplicável.

22.1.2 Registro do Incidente: Todos os incidentes serão documentados em um Relatório de Incidentes de Segurança, contendo:

- Data e hora do incidente;
- Descrição detalhada dos eventos;
- Dados pessoais afetados;
- Ações tomadas para contenção e mitigação; e
- Medidas preventivas para evitar novos incidentes.

Esse registro será mantido pelo Departamento de Infraestrutura de TI e pelo Encarregado de Proteção de Dados para fins de auditoria e melhoria contínua.

22.1.3 Monitoramento e Revisão Pós-incidente: Após a contenção do incidente, será conduzida uma revisão para:

- Avaliar a eficácia das medidas adotadas;
- Identificar vulnerabilidades ou falhas nos controles de segurança;
- Atualizar o plano de resposta a incidentes, quando necessário; e
- Deve ser preenchido um formulário com informações sobre o incidente, anexo a esta Política.

23 Transferência Internacional de Dados

Eventuais transferências internacionais de dados pessoais somente serão realizadas em conformidade com os arts. 33 a 36 da LGPD e com o Regulamento de Transferência Internacional de Dados da ANPD (Resolução CD/ANPD nº 19/2024), mediante:

- Decisão de adequação;
- Cláusulas-padrão contratuais aprovadas;
- Normas corporativas globais; ou
- Outros mecanismos autorizados pela ANPD.

A COGEM adotará salvaguardas contratuais, técnicas e organizacionais adequadas, assegurando nível de proteção equivalente ao previsto na legislação brasileira, e informará aos titulares, quando aplicável, sobre os países ou organismos internacionais destinatários dos dados e as bases legais da transferência.

24 Penalidade/Violações

Os incidentes de segurança da informação identificados devem ser avaliados pelas Áreas de Compliance, T.I, Gerência e Diretoria Executiva que, ao constatar uma violação, deverá encaminhar o formulário de Relato de Incidente com Dados Pessoais para o Conselho de Administração, que, após análise, poderá apurar as responsabilidades dos envolvidos em procedimento disciplinar, visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente.

No caso de uma violação de segurança que leve à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados privados/pessoais, a Cogem deverá providenciar imediatamente a avaliação do risco visando garantir os direitos e privacidade dos titulares.
A comunicação de incidentes à ANPD e aos titulares será realizada sempre que o incidente puder acarretar risco ou dano relevante, conforme determina o art. 48 da LGPD.
O comunicado deve conter as informações conforme normativos vigentes da ANPD – Agência Nacional de Proteção de dados.

25 Do Controle da Política

A Política de Privacidade de Proteção de Dados - LGPD deverá ser aprovada pelo Conselho de Administração e deverá ser publicada e comunicada para todos os colaboradores, membros dos Conselhos, diretores e partes externas relevantes para o necessário cumprimento.
Será revisada quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Anexo: Formulário de Relato de Incidente com Dados Pessoais

COGEM Valorizando seu sonho	Formulário de Relato de Incidente com Dados Pessoais

Informações do Incidente			
Data do Incidente:		**Hora do Incidente:**	
Nome do Relator:		**Cargo**	
Descrição do Incidente: (Descreva o incidente de forma detalhada, incluindo o que aconteceu, como aconteceu e as circunstâncias envolvidas.)			
Tipo de Dados: (Ex.: Nomes, E-mails, Telefones, Endereços, Informações Financeiras etc.)			

Descrição da natureza dos dados pessoais afetados.	
Identificação dos titulares envolvidos:	
Ações Tomadas: (Descreva as ações imediatas tomadas após o incidente para controlar a situação e minimizar danos.)	
Análise de Impacto: (Descreva o impacto potencial do incidente sobre as pessoas cujos dados pessoais foram afetados e a gravidade do incidente.)	
Medidas tomadas para conter o incidente:	
Medidas Corretivas: (Descreva as medidas implementadas ou planejadas para evitar a recorrência do incidente.)	
Medidas preventivas para evitar novos incidentes:	

Registro de Alteração			
Data	Versão	Páginas alteradas	Informações Relevantes
abr/25	2ª	2, 5, 8, 9, 10, 11, 12, 13	Capítulo 37.3 – Substituição do termo “processador” por “operador”. Capítulo 37.5 – Inclusão de novos dados pessoais tratados – órgãos de proteção ao consumidor. Capítulo 37.14 – Inclusão sobre a Política de retenção de dados pessoais e sensíveis. Capítulo 37.19 – Atualização das responsabilidades e atribuições. Capítulo 37.20 – Inclusão do nome do encarregado de dados. Capítulo 37.21 – Atualização sobre a comunicação de incidentes de segurança. Capítulo 37.22 – Atualização sobre o conteúdo do comunicado. Alteração do termo “cliente” para “associado” na política.
fev/26	3º	1, 4, 12 e 13	Capitulo 01 - Adicionada seção inicial com dados institucionais. Capitulo 07.1 - Inclusão detalhada dos direitos previstos no Art. 18 da LGPD. Capitulo 22.1 – Alterado prazo para 3 dias a comunicar a ANPD. Capitulo 23 - Adicionada cláusula de conformidade com os artigos 33 a 36 da LGPD. Capitulo 24 - Ajustada a redação para tornar a comunicação à ANPD um dever em casos de risco relevante, removendo a ambiguidade anterior.