



POLÍTICA DE

PROTEÇÃO DE DADOS E

PRIVACIDADE

semove

Índice

Mensagem da Gerência de Proteção de Dados e Privacidade	03
1. Objetivo	03
2. Abrangência	03
3. Referência legal e boas práticas	04
4. Vigência	05
5. Responsabilidades	06
6. Diretrizes da política de proteção de dados e privacidade	09
7. Instâncias corporativas de aprovações	26
8. Anexos	26
Anexo I	28
Anexo II	30
Anexo III	32

MENSAGEM DA GERÊNCIA DE PROTEÇÃO DE DADOS E PRIVACIDADE

A proteção de **dados pessoais** é um direito fundamental, inserido na Constituição Federal Brasileira. Nesse contexto, a Política de Proteção de Dados e Privacidade (PLGPD) discorre sobre os princípios, as boas práticas e as diretrizes que o grupo societário da Federação das Empresas de Mobilidade do Estado do Rio de Janeiro (Semove) determina, com o intuito de proteger a privacidade dos dados pessoais coletados e custodiados, no âmbito dos negócios celebrados com suas **partes interessadas** ou **relacionadas**, de modo que esses dados sejam tratados com segurança, confidencialidade e transparência, nos termos da Lei Federal nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD).

1. OBJETIVO

1.1. A PLGPD estabelece as diretrizes e os princípios a serem observados no **tratamento dos dados pessoais**, que consiste na coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, divulgação, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, transporte, difusão, cessão ou extração de informações, que contenham dados pessoais, sob custódia da Semove, tendo por objetivo garantir a confidencialidade e a privacidade da **informação**.

2. ABRANGÊNCIA

2.1. A PLGPD aplica-se a todos os **colaboradores, gestores, agentes de governança** do grupo societário da Semove, bem como suas partes interessadas ou relacionadas que, no âmbito da realização de atividades laborais ou da celebração de negócios, acessem ou tratem dados pessoais que estejam sob sua **custódia**.

2.2. Para fins da PLGPD, consideram-se informações os dados, processados ou não, que possam ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato, incluindo-se os dados pessoais sob a custódia da Semove, sejam estes dados de colaboradores, gestores, agentes de governança, fornecedores, clientes ou qualquer outra parte interessada ou relacionada. As informações podem ou não conter dados pessoais.

2.3. As diretrizes previstas na PLGPD aplicam-se a todos os dados pessoais (**sensíveis** ou não) tratados pela Semove em decorrência de suas atividades, seja como **controladora** ou **operadora de dados pessoais**.

2.4. A LGPD prevê situações em que suas diretrizes não se aplicam aos casos concretos. Dessa forma, esta PLGPD reconhece e reflete essas exceções, de modo a garantir simetria entre o presente instrumento e a legislação vigente.

2.5. A PLGPD não se aplica para fins exclusivamente (i) jornalísticos, artísticos ou acadêmicos; (ii) de segurança pública, defesa nacional ou de segurança do Estado; (iii) de investigação e repressão de infrações penais; (iv) para fins particulares e não econômicos; (v) a dados oriundos de fora do Brasil, que não sejam

objeto de **transferência internacional de dados** e que não sejam objeto de lei específica estrangeira que garanta a segurança do **tratamento de dados pessoais**.

2.6. No que tange ao item 2.5, (v), não se aplicará a PLGPD aos dados de indivíduos localizados fora do território nacional, tratados fora do Brasil, ou seja, qualquer dado pessoal de indivíduos localizados no território nacional será objeto desta PLGPD.

2.7. Sempre que houver referência à palavra **titular(es)**, significa a(s) pessoa(s) física(s) proprietária(s) do dado pessoal que é objeto de tratamento.

2.8. Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta, independentemente de sua nacionalidade.

2.9. Todas as palavras ou expressões destacadas em **negrito** estão definidas no Glossário da PLGPD (ANEXO III).

2.10. O nível de classificação desta PLGPD é público.

2.11. As diretrizes desta PLGPD não se sobrepõem às espécies normativas em vigor e se complementam com as definições previstas no contrato social, convenções, regimentos internos ou instrumentos normativos publicados pela Semove. No entanto, em caso de ausência de diretrizes publicadas por alguma autoridade brasileira ou instrumentos normativos internos, recomenda-se o uso de direito comparativo internacional, com a adoção das melhores práticas sobre o tema, como, por exemplo, a *General Data Protection Regulation (GDPR)* e as diretrizes publicadas pela *European Data Protection Board (EDPB)*.

2.12. As diretrizes previstas na PLGPD aplicam-se a todos os dados pessoais (sensíveis ou não) tratados pela Semove em decorrência de suas atividades, seja como controladora ou operadora de dados pessoais.

3. REFERÊNCIA LEGAL E BOAS PRÁTICAS

- ABNT NBR ISO/IEC 27.001:2006 – Tecnologia da Informação – Técnicas de Segurança, Sistemas de Gestão de Segurança da Informação - Requisitos.
- ABNT NBR ISO/IEC 27.002:2013 - Tecnologia da Informação – Técnicas de Segurança, Código de Prática para Controles de Segurança da Informação.
- ABNT NBR 16.167:2014 – Segurança da Informação – Diretrizes para Classificação, Rotulação e Tratamento da Informação.
- ABNT NBR ISO/IEC 27.701:2019 – Técnicas de Segurança para a Gestão de Privacidade da Informação – Requisitos e Diretrizes.
- Código de Conduta.
- Comitê de Pronunciamentos Contábeis (CPC) nº 05 (R1) /2008 – Divulgação sobre partes relacionadas.
- Constituição da República Federativa do Brasil/1988.

- Contrato Social.
- Decreto-Lei nº 2.848/1940, que institui o Código Penal.
- Decreto nº 48.891/2024 - Política de Governança em Privacidade e Proteção de Dados Pessoais do Estado do Rio de Janeiro.
- *GDPR*: regulamentação acerca das regras para tratamento de dados pessoais da União Europeia.
- Guias, Resoluções e Normas publicados pela **Autoridade Nacional de Proteção de Dados (ANPD)** ou Governo Federal.
- Lei nº 8.069/1990, que institui o Estatuto da Criança e do Adolescente.
- Lei nº 8.078/1990 - Código de Defesa do Consumidor (CDC).
- Lei nº 9.307/1996 - Lei de Arbitragem.
- Lei nº 10.406/2002, que institui no âmbito Federal, o Código Civil.
- Lei nº 10.741/2003 - Estatuto da Pessoa Idosa.
- Lei nº 13.709/2018 - LGPD.
- Política do Canal de Denúncia e Diálogo Voz Ativa.
- Política de Consequências.
- Política de Segurança da Informação (PSI).
- Pronunciamento Técnico do Comitê de Pronunciamentos Contábeis (CPC), nº 05 (R1)/2008 - Divulgação sobre Partes Relacionadas.
- Regimento Interno do **Comitê de Integridade e Conformidade (CIC)**.
- Resolução nº 245/2024, que dispõe sobre os direitos das crianças e adolescentes em ambiente digital.

4. VIGÊNCIA

4.1. Esta PLGPD entra em vigor a partir da data de sua publicação. A revisão deverá ser realizada em até 3 (três) anos, contados da data de sua efetiva publicação, ou sempre que a Gerência de Proteção de Dados e Privacidade julgar necessário.

4.2. Não obstante, ainda que não tenha sido renovada, suas diretrizes permanecem válidas até a publicação da próxima versão.

5. RESPONSABILIDADES

5.1. Todos devem cumprir as diretrizes e princípios desta PLGPD, legislação vigente e demais instrumentos normativos correlatos. No entanto, algumas funções, áreas ou órgãos de governança corporativa têm atribuições/responsabilidades adicionais, tais como:

i. Agente de Proteção de Dados e Privacidade: ser ponto focal da área de negócios que apoiará a Gerência de Proteção de Dados e Privacidade no desenvolvimento e monitoramento do **Programa de Governança em Proteção de Dados e Privacidade**, dentre outras ações preventivas, detectivas e corretivas identificadas através do **Programa de Integridade e Conformidade (PIC) e Planejamento Estratégico de Segurança da Informação (PESI)**.

ii. Assembleia Geral de Representantes dos Sindicatos (AGRS): seus representantes devem: i) tomar conhecimento desta PLGPD, após submissão e aprovação pelos conselheiros do **Conselho de Gestão (CG)**; ii) apoiar a disseminação desta PLGPD para que sua eficácia atinja todos os níveis organizacionais; iii) zelar para que os gestores e agentes de governança respeitem e cumpram as diretrizes desta PLGPD; iv) aplicar sanções ou medidas disciplinares ou, em última instância, requerer à Diretoria Jurídica/Coordenação Jurídica, o ajuizamento de ações de responsabilização legal contra o conselheiro ou delegados da AGRS, quando comprovado que tenham, direta ou indiretamente, contribuído para a ocorrência ou tenham se envolvido em violações à legislação, às diretrizes desta PLGPD, ou aos demais instrumentos normativos ou contratuais vigentes; e v) participar dos treinamentos acerca da LGPD.

iii. Comitê de Integridade e Conformidade (CIC): seus representantes devem i) tomar ciência, revisar e apoiar a disseminação desta PLGPD; ii) validar os riscos de não conformidade com as diretrizes desta PLGPD, identificados junto com as áreas de negócios e recomendar aos gestores e agentes de governança um conjunto de planos de ação que os mitiguem ou reduzam seu impacto no ambiente de negócios; iii) tomar ciência da implementação dos planos de ação submetidos à sua validação, por meio do monitoramento realizado pela Gerência de Auditoria Interna; e iv) em caso de denúncia, recomendar aos gestores e agentes de governança, quando cabível, a aplicação de sanções ou medidas disciplinares ou, em última instância, o ajuizamento de ações de responsabilização legal contra os infratores, por violações à legislação em vigor, às diretrizes desta PLGPD e/ou aos demais instrumentos normativos ou contratuais vigentes.

iv. Conselho de Gestão (CG): seus conselheiros devem: i) apoiar e monitorar as ações dos membros do **Órgão Diretivo** no sentido de assegurar a proteção e privacidade dos dados pessoais sob custódia da Semove; ii) aprovar esta PLGPD; iii) aplicar sanções ou medidas disciplinares ou, em última instância, requerer à Diretoria Jurídica/Coordenação Jurídica, o ajuizamento de ações de responsabilização legal contra o **diretor-executivo** ou **presidente-executivo**, quando comprovado que tenham, direta ou indiretamente, contribuído para a ocorrência ou tenham se envolvido em violações à legislação, às diretrizes desta PLGPD, ou aos demais instrumentos normativos ou contratuais vigentes; e iv) participar dos treinamentos acerca da LGPD.

v. Diretoria Jurídica/Coordenação Jurídica/Coordenação de Contratos: devem: i) integrar o **Grupo de Trabalho de Dados (GTD)** com o propósito de conferir suporte legal às diretrizes da PLGPD; ii) apoiar os gestores e membros do Órgão Diretivo, quando requerido, na definição da estratégia de aplicação de

sanções ou medidas disciplinares ou, em última instância, no ajuizamento de ações de responsabilização legal contra os infratores, acerca de violações às diretrizes previstas nesta PLGPD; iii) assegurar que os contratos contemplem em seu escopo, quando aplicável, o tratamento de dados pessoais e contenham cláusulas de confidencialidade e privacidade; iv) apoiar o encarregado de dados (*Data Protection Officer* ou *DPO*) na interface com a ANPD e demais órgãos fiscalizadores da LGPD; v) apoiar na coleta das assinatura dos **Termos de Aceite** da PLGPD (ANEXOS I e II) pelos conselheiros do CG e delegados da AGRS; e vi) dar suporte jurídico às revisões dos avisos e **Políticas de Privacidade** dos sistemas, *websites* e aplicativos disponibilizados aos clientes e demais partes interessadas ou relacionadas em prol da prestação de serviços.

vi. Gerência de Auditoria Interna: deve: i) assessorar a alta administração, o CIC e/ou demais órgãos fiscalizadores, quando instituídos, no monitoramento dos riscos e na identificação, investigação e tratamento de atos ilícitos e/ou em desacordo com esta PLGPD ou demais instrumentos normativos, visando, de forma independente e imparcial, apoiar os gestores e membros do Órgão Diretivo no aprimoramento dos processos das áreas de negócios sob sua estrutura organizacional; e ii) comunicar os agentes de governança, em caráter restrito, o resultado das auditorias internas realizadas nos processos das áreas de negócios, em relação aos riscos inerentes ao tratamento inadequado de dados pessoais, controles internos e monitoramento dos planos de ação acerca da proteção e privacidade dos dados pessoais.

vii. Gerência de Comunicação Institucional: deve divulgar esta PLGPD nos canais de comunicação da Semove.

viii. Gerência de Controles Internos e Riscos: deve i) integrar o GTD com o intuito de assessorar seus membros no diagnóstico dos riscos em áreas de negócios que podem comprometer, se materializados, a proteção e privacidade dos dados pessoais; ii) revisar e submeter a PLGPD às instâncias aprovadoras competentes; e iii) apoiar, quando requerido e em caráter consultivo, a Gerência de Auditoria Interna, em diligências ou investigações internas de condutas que indiquem a prática de atos ilícitos ou violações às diretrizes desta PLGPD, demais instrumentos normativos ou contratuais vigentes.

ix. Gerência de Dados: responsável por: i) integrar o GTD para dar o suporte técnico à Gerência de Proteção de Dados e Privacidade sobre os impactos nos **sistemas analíticos** decorrentes das deliberações relativas à proteção de dados e privacidade; ii) agir em sinergia e apoiar a Gerência de Proteção de Dados e Privacidade no tocante ao tratamento de dados pessoais dos sistemas analíticos, principalmente em relação às demandas por relatórios de inteligência empresarial (*Business Intelligence*), de ciência e engenharia de dados; iii) gerir o acesso aos dados dos sistemas analíticos e; iv) mitigar a criação de **ilhas de dados** dentro dos sistemas analíticos, a fim de assegurar sua rastreabilidade; v) monitorar e garantir, por meio de métricas e *feedbacks* mensais, que as diretrizes de proteção de dados e privacidade estejam sendo cumpridas nas demandas dos sistemas analíticos; e vi) revisar esta PLGPD.

x. Gerência de Desenvolvimento Organizacional: deve apoiar a Gerência de Proteção de Dados e Privacidade nos treinamentos que tratem da conscientização quanto às diretrizes desta PLGPD.

xi. Gerência de Infraestrutura: é área técnica responsável por: i) definir os requisitos técnicos minimamente necessários para assegurar o adequado funcionamento dos **recursos tecnológicos** (no âmbito de computadores, *tablets* e periféricos e servidores) disponibilizados para fins de trabalho, de modo que esses recursos tecnológicos estejam protegidos conforme as diretrizes desta PLGPD; e ii)

assegurar a **eliminação** das informações dos recursos tecnológicos antes da disponibilizá-los para doação, leilão, cessão, venda, envio para reparo, custódia por **terceiros** ou descarte como **resíduos sólidos**.

xii. Gerência de Projetos ou responsável por Gestão de Projetos: é responsável por: i) conceber, desenvolver, gerenciar e monitorar os projetos sistêmicos demandados pelas áreas de negócios, para fins de tratamento de **dados transacionais** e **dados analíticos** necessários à tomada de decisão; ii) garantir que todos os projetos, onde for necessário tratamento de dado pessoal, obedeçam aos princípios da **privacidade desde a concepção (Privacy By Design)**, devendo, para tanto, envolver, obrigatoriamente, a Gerência de Proteção de Dados e Privacidade, a Gerência de Dados e a Gerência de Segurança da Informação, desde a primeira oportunidade; e iii) revisar esta PLGPD.

xiii. Gerência de Proteção de Dados e Privacidade: é área técnica responsável por: i) liderar o GTD e definir as diretrizes sobre a proteção e privacidade de dados a serem cumpridas, com o apoio dos agentes de Proteção de Dados e Privacidade; ii) participar da concepção dos projetos que envolvam tratamento de dados pessoais; iii) apoiar tecnicamente as áreas de negócios a respeito das ações preventivas, detectivas e corretivas que visem à proteção e à privacidade dos dados pessoais, por meio de avaliações periódicas das ações que embasam o Programa de Governança em Proteção de Dados e Privacidade, identificando melhorias, vulnerabilidades e acompanhando suas evoluções; iv) solicitar e acompanhar a atualização dos **inventários de dados** e as correções identificadas no **gap analysis**; v) coordenar a elaboração, quando aplicável, do **Relatório de Impacto à Proteção de Dados Pessoais (Data Privacy Impact Assessment ou DPIA)** e do **Relatório de Avaliação de Legítimo Interesse (Legitimate Interest Assessment ou LIA)**; vi) monitorar a atualização de contratos pela Diretoria Jurídica/Coordenação de Contratos e áreas de negócios, visando à inclusão de cláusulas de confidencialidade e privacidade das informações; vii) validar e autorizar a prestação de esclarecimentos aos **titulares** no prazo estipulado na PLGPD; viii) monitorar os planos de ação recomendados para adequação dos controles internos à LGPD; ix) apoiar tecnicamente a Gerência de Auditoria Interna, em diligências ou investigações internas de condutas indevidas, que comprometam a proteção e privacidade dos dados pessoais; x) atender os requerimentos formais das auditorias ou de órgãos fiscalizadores; xi) apoiar a Gerência de Segurança da Informação, em um ambiente de crise, no entendimento e avaliação do grau de impacto de um **incidente de segurança da informação** quando este comprometer a proteção e privacidade de dados pessoais; xii) comunicar tempestivamente às autoridades fiscalizadoras da LGPD, no âmbito nacional ou global, eventual incidente de segurança da informação que prejudique a privacidade de dados pessoais, conforme previsto nesta PLGPD; e xiii) realizar a gestão dos Termos de Aceite desta PLGPD (ANEXO I), zelando para que todos a conheçam e adiram às suas diretrizes.

xiv. Gerência de Segurança da Informação: responsável por: i) integrar o GTD com o intuito de apoiar tecnicamente a Gerência de Proteção de Dados e Privacidade no entendimento e avaliação de impactos das deliberações relativas à proteção de dados e privacidade, no ambiente tecnológico da Semove, além de ser responsável por definir e monitorar os controles internos que precisam ser implementados nos processos das áreas de negócios e nos recursos tecnológicos da Semove, com a finalidade de preservar a confidencialidade, integridade e disponibilidade das informações; ii) participar da análise e validação de projetos sistêmicos, com o intuito de preservar as informações custodiadas pela Semove contra possíveis incidentes de segurança da informação; iii) realizar avaliação de risco de segurança da informação nas contratações que envolvam o uso de tecnologias da informação; e iv) coletar as assinaturas eletrônicas, em nome da Gerência de Proteção de Dados e Privacidade, apoiando-a na guarda segura e centralizada dos Termos de Aceite dessa PLGPD (ANEXO I).

xv. Gestor: responsável por: i) tratar adequadamente os dados pessoais na(s) área(s) de negócio(s) que lidera, independentemente de estarem armazenados ou transitarem por repositórios físicos ou digitais; ii) manter atualizados os inventários de dados pessoais e, quando aplicável, o *DPIA* e o *LIA*; iii) coletar as assinaturas eletrônicas dos Termos de Aceite desta PLGPD (ANEXO II) das pessoas jurídicas sob sua gestão, zelando para que todos a conheçam e adiram às suas diretrizes; iv) realizar a guarda segura dos Termos de Aceite desta PLGPD (ANEXO II); e v) aplicar sanções ou medidas disciplinares ou, em última instância, requerer à Diretoria Jurídica/Coordenação Jurídica o ajuizamento de ações de responsabilização legal contra os infratores (internos ou terceirizados) que, comprovadamente, tenham, direta ou indiretamente, contribuído para a ocorrência ou tenham se envolvido em violações à legislação, às diretrizes desta PLGPD, ou aos demais instrumentos normativos ou contratuais vigentes.

xvi. Grupo de Trabalho de Dados (GTD): deve analisar assuntos técnicos sobre LGPD, que possam ser úteis no desenvolvimento do Programa de Governança em Proteção de Dados e Privacidade junto às áreas de negócios.

xvii. Órgão Diretivo: deve: i) conhecer, cumprir e assegurar que seus subordinados ajam em conformidade com a legislação, instrumentos normativos e contratuais vigentes; ii) deliberar sobre o apetite e tolerância ao risco que impactem as áreas de negócios sob suas respectivas lideranças; iii) garantir que as soluções utilizadas pelas áreas de negócios que lidera não comprometam a integridade e privacidade dos dados pessoais; iv) aplicar sanções ou medidas disciplinares ou, em última instância, requerer à Diretoria Jurídica/Coordenação Jurídica o ajuizamento de ações de responsabilização legal contra os infratores internos (i.e., gestor ou **diretor**) ou terceirizados que, comprovadamente, tenham, direta ou indiretamente, contribuído para a ocorrência ou tenham se envolvido em violações à legislação, às diretrizes desta PLGPD, ou aos demais instrumentos normativos ou contratuais vigentes; e v) zelar para que seus colaboradores e gestores ou **empregados** terceirizados assinem o Termo de Aceite desta PLGPD (ANEXO I e II).

xviii. Supervisão Administrativa e de Manutenção: responsável por: i) definir, com a Gerência de Segurança da Informação e a Gerência de Infraestrutura, os requisitos técnicos dos aparelhos celulares disponibilizados pela Semove para fins de trabalho que tenham capacidade para suportar a instalação de soluções de segurança homologadas, capazes de proteger a informação, principalmente a privacidade dos dados pessoais, conforme as diretrizes desta PLGPD; e ii) assegurar a eliminação das informações dos aparelhos celulares e circuito fechado de televisão (CFTV) e demais recursos tecnológicos sob sua gestão, antes da disponibilizá-los para doação, leilão, cessão, venda, envio para reparo, custódia por terceiros ou descarte como resíduos sólidos.

6. DIRETRIZES DA POLÍTICA DE PROTEÇÃO DE DADOS E PRIVACIDADE

6.1. COMPROMISSOS INSTITUCIONAIS

6.1.1. A Semove assume o compromisso institucional de:

- manter relação de confiança com titular de dados pessoais, por meio de atuação transparente, salvo quando envolver informações confidenciais;
- manter atualizados processos e instrumentos normativos;
- investir nas melhores práticas de proteção de dados e privacidade, por meio de adoção de medidas eficazes, concretas e auditáveis, baseadas na avaliação de risco à privacidade e possíveis impactos na Semove e/ou titulares, e quando viável, utilizar, para esse fim, tecnologias da informação avançadas;
- investir na atualização técnica do seu capital humano sobre as práticas aderentes à LGPD;
- fornecer, no mínimo, 2 (dois) treinamentos para os colaboradores, gestores, **diretores** e presidente-executivo e, mensalmente, para os novos empregados admitidos (*onboarding*) e, pelo menos, 1 (um) treinamento anual para os agentes de governança;
- manter um plano de respostas a incidentes de segurança da informação atualizado e testado, além de estar regulamentado por instrumento normativo específico;
- auditar, periodicamente, os processos das áreas de negócios sob a ótica da aderência às diretrizes desta PLGPD e do conjunto de legislação que dispõe sobre a proteção e privacidade de dados.

6.2. PRINCÍPIOS DO TRATAMENTO DE DADOS

6.2.1. Todos devem cumprir as diretrizes da PLGPD e agregar, à sua rotina de trabalho e aos projetos, os princípios de proteção e privacidade dos dados pessoais:

- *Adequação*: assegura a compatibilidade do tratamento de dados pessoais com as finalidades informadas ao titular. O tratamento de dados deverá ser condizente com a destinação à qual se refere.
- *Finalidade*: assegura que o tratamento de dados pessoais seja feito com fins legítimos, específicos e informados ao titular. Assim, os dados pessoais não podem ser coletados com um propósito e utilizados para outro. A Semove tem o dever de esclarecer ao titular o motivo pelo qual estão utilizando o dado, não estando autorizadas a alterar a finalidade durante o tratamento.
- *Livre acesso*: assegura que os titulares tenham o direito à consulta facilitada e gratuita sobre a forma, duração do tratamento de dados pessoais, bem como sobre a integralidade de seus dados pessoais.
- *Necessidade*: assegura que a coleta de dados pessoais se limite aos dados minimamente necessários para determinada finalidade, preservando o que é realmente essencial (e não só conveniente) para os seus negócios, evitando, assim, a coleta de dados excessivos.
- *Não discriminação*: assegura que os dados pessoais não sejam, em qualquer circunstância, utilizados para fins discriminatórios, ilícitos ou abusivos.
- *Prevenção*: assegura o compromisso da Semove com a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

- *Qualidade dos dados*: refere-se ao compromisso da Semove em garantir aos titulares exatidão, clareza, relevância e atualização dos dados pessoais. A veracidade dos dados pessoais declarados pelo titular, dentro do princípio da boa-fé, deve ser coletada e averiguada pela Semove, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
- *Responsabilização e prestação de contas*: reflete o compromisso da Semove de apresentar provas e evidências de que as medidas adotadas com o intuito de garantir a proteção e privacidade dos dados pessoais são eficazes, demonstrando, deste modo, a boa-fé e a diligência no cumprimento da LGPD, da PLGPD e PSI, bem como demais instrumentos normativos que possuem diretrizes que discorrem sobre a proteção de dados pessoais.
- *Segurança*: reflete o compromisso da Semove com a proteção dos dados pessoais, utilizando-se de procedimentos e recursos tecnológicos aptos, capazes de proteger esses dados contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda ou alteração, comunicação ou difusão.
- *Transparência*: é garantida, aos titulares de dados pessoais, o acesso a informações claras e precisas sobre a realização do tratamento dos seus dados pessoais e aos respectivos **agentes de tratamento de dados pessoais**, devendo, para tanto, serem formuladas numa linguagem clara e simples, no idioma nacional e em idioma inglês, de abrangência internacional, salvo quando envolver segredos comercial, industrial e informações classificadas como sigilosas.

6.2.2. Desde que amparadas com alguma base legal, boa-fé e respeito aos princípios da LGPD, a Semove poderá tratar dados pessoais públicos ou não, para fins de investigações, diligências ou qualquer atividade capaz de detectar e combater fraudes, corrupção, lavagem de dinheiro ou qualquer outro ato ilícito.

6.2.3. A Semove está comprometida com a proteção de todos os dados pessoais que lhes foram confiados em decorrência de suas atividades, respeitando a privacidade dos seus colaboradores, gestores, agentes de governança, clientes, fornecedores, parceiros de negócios e demais partes interessadas ou relacionadas.

6.2.4. Todos deverão, obrigatoriamente, cumprir com as diretrizes e princípios da PLGPD e agregar às suas rotinas de trabalho, pois as consequências decorrentes do seu descumprimento, envolvem sanções contratuais (ex.: multas, postergação de pagamentos, distratos, dentre outros) ou legais, em caso de pessoa jurídica, ou aplicação de medidas disciplinares, em caso de pessoa física. Em ambas as situações, ainda há a possibilidade de, em última instância, os infratores se tornarem réus em processos de responsabilização legal. Nesse sentido, os colaboradores, gestores e agentes de governança devem seguir as seguintes recomendações, em especial:

- i. proteger todos os dados pessoais que estão sob sua custódia;
- ii. somente coletar dados pessoais que sejam estritamente necessários;
- iii. somente tratar dados pessoais que possuam uma finalidade específica, delimitada antes da coleta;
- iv. somente tratar dados pessoais que possuam uma autorização legal;

v. informar à Gerência de Proteção de Dados e Privacidade qualquer alteração no fluxo de dados (i.e., rastrear o fluxo de tratamento de dados pessoais contemplados entre os dados transacionais e dados analíticos durante o registro de operações);

vi. adotar o princípio da privacidade desde a concepção em todos os projetos em que houver tratamento de dados.

6.3. HIPÓTESE LEGAL DE TRATAMENTO DE DADOS

6.3.1. A Semove, representada pelos seus colaboradores, gestores, agentes de governança, somente está autorizada a realizar o tratamento de dados pessoais caso identificada, ao menos, uma das seguintes hipóteses:

- a) cumprimento de obrigação legal ou regulatória pela controladora de dados pessoais;
- b) celebração ou execução de um contrato ou procedimentos preliminares relacionados a contrato do qual o titular seja parte, a pedido deste, exceto em caso de dados pessoais sensíveis;
- c) para proteção da vida ou da incolumidade física do titular ou de terceiros;
- d) para tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- e) para proteção ao crédito, inclusive quanto ao disposto na legislação pertinente, exceto em caso de dados pessoais sensíveis;
- f) para atender legítimo interesse da controladora de dados pessoais ou de terceiros, conforme requisitos descritos no item 6.3.2 abaixo;
- g) para garantia da prevenção à fraude e proteção à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos do titular previstos no art. 9º da LGPD, exceto no caso em que prevaleçam direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
- h) para realização de estudos por **órgãos de pesquisa**, garantida, sempre que possível, a **anonimização** ou a **pseudonimização** dos dados pessoais;
- i) para exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último conforme a Lei de Arbitragem;
- j) pela administração pública, para o tratamento e **uso compartilhado de dados** com terceiros, agindo sob sua tutela, necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
- k) mediante o fornecimento de **consentimento** pelo titular ou pelo seu responsável legal.

6.3.2. Na hipótese de tratamento de dados pessoais com base no legítimo interesse, a Semove deve:

- i. comprovar que os dados coletados são mínimos, necessários para o atingimento da finalidade pretendida;
- ii. demonstrar que o uso atribuído ao dado pessoal é compatível com a legítima expectativa do seu titular, à luz da boa-fé objetiva e da análise contextual do tratamento;
- iii. realizar teste de balanceamento do legítimo interesse, a fim de assegurar transparência, oportunidade de oposição ao titular, esclarecer de que forma os titulares dos dados poderão ser impactados negativamente e quais medidas foram tomadas para mitigar os riscos associados ao tratamento.

6.3.3. O tratamento de dados pessoais cujo acesso é público, ou quando tornados manifestamente públicos pelo titular, deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua publicação pelo titular, portanto, está dispensado de consentimento prévio deste, mas precisa ser considerado o propósito legítimo e específico para esse tratamento pela controladora ou operadora de dados pessoais.

6.3.4. O tratamento de dados de acesso público, ou tornados manifestamente públicos pelo titular, bem como o tratamento de dados pessoais para finalidade diversa daquela informada para o titular no momento da sua coleta, seja pela Administração Pública, seja pela Semove, somente será permitido se:

- i. houver um interesse público que o justifique ou interesse legítimo da controladora ou de terceiro, conforme previsto no artigo 7º, inciso IX, da LGPD;
- ii. houver uma nova base legal que o autorize ou legítimo interesse da controladora;
- iii. a finalidade do tratamento secundário for compatível com a finalidade que justificou a publicação ou a coleta do dado pessoal;
- iv. o ato que determina a realização do tratamento secundário for devidamente motivado;
- v. forem respeitados os direitos do titular e os princípios gerais da proteção de dados pessoais; e
- vi. forem respeitados os pressupostos elencados no item 6.3.2 desta PLGPD.

6.4. MUDANÇA NA FINALIDADE DO TRATAMENTO DE DADOS

6.4.1. O titular deve ser informado a respeito da finalidade do tratamento no momento da coleta dos dados pessoais e, nos casos de impossibilidade imediata, tão logo seja possível.

6.4.2. O tratamento dos dados pessoais somente poderá ser realizado para o atingimento das finalidades informadas ao titular por ocasião da respectiva coleta.

6.4.3. Nas hipóteses em que o consentimento for requerido, caso haja mudanças relacionadas à finalidade do tratamento de dados pessoais que não sejam compatíveis com o consentimento original, a

controladora de dados pessoais deverá informar previamente ao titular sobre as mudanças de finalidade. Nesse momento, o titular poderá optar por renovar o consentimento ou revogá-lo.

6.4.4. Além das disposições legais previstas nos itens do tópico anterior, a Semove poderá se valer do consentimento do titular, desde que atendam a todos os requisitos previstos na lei.

6.4.5. A Semove deverá fornecer meios técnicos e procedimentos internos capazes de viabilizar a confirmação ou revogação do consentimento, sempre que solicitado pelo titular ou qualquer autoridade.

6.5. COMPARTILHAMENTO DE DADOS

6.5.1. Caso seja necessário compartilhamento de algum dado pessoal com novo **agente de tratamento de dados pessoais**, ou haja alguma alteração na finalidade, o agente de tratamento responsável deverá buscar todos os meios possíveis para obter um novo consentimento, específico, do titular para esta necessidade, ressalvadas as hipóteses de dispensa deste consentimento, previstas no item 6.3.1 desta PLGPD.

6.6. DADOS QUE REQUEREM PROTEÇÕES ESPECIAIS

6.6.1. TRATAMENTO DE DADOS SENSÍVEIS

6.6.1.1. O tratamento de dados pessoais sensíveis só deve ser realizado em casos específicos, previstos em lei, ou mediante consentimento explícito do titular. Nestes casos, deverão ser adotados padrões de segurança mais robustos do que os utilizados para proteger os demais dados pessoais.

6.6.2. TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES

6.6.2.1. O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais, previstas no art. 7º ou art.(s) 11º ao 14º da LGPD, desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14º da LGPD. Como boa prática, a Semove deverá realizar todos os esforços e buscar todos os meios possíveis, consideradas as tecnologias disponíveis, para solicitar o consentimento específico (i.e., por escrito ou digital) e em destaque de pelo menos um dos pais, ou do responsável legal do menor de 16 (dezesesseis) anos, prevalecendo, sempre, o melhor interesse do menor.

6.6.2.2. Além disso, a Semove deve prover as informações sobre o tratamento desses dados pessoais de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do titular, com uso de recursos audiovisuais, quando adequado, de forma a proporcionar o entendimento e esclarecimento adequado à criança, ao adolescente, bem como um de seus pais ou responsável legal.

6.6.2.3. A LGPD não é clara quanto à necessidade de consentimento de, pelo menos, um dos pais ou pelo responsável legal, para tratar dados de adolescentes, tampouco define a idade limite para a

Semove abster-se deste consentimento, citando apenas a necessidade de agir no melhor interesse do titular. Diante desta omissão, a Semove assume, para fins da PLGPD, que, a partir dos 16 (dezesseis) anos de idade, a sociedade, por si, já atribui ao adolescente certo grau de autonomia (ex.: votar, andar em transporte público desacompanhado, trabalhar, possuir certas modalidades de cartão de crédito, como jovem universitário ou jovem trabalhador que comprove renda etc.), o que o torna capaz de discernir por conta própria, quando devidamente esclarecido sobre os seus direitos como titular, em conformidade com as diretrizes e os princípios de proteção e privacidade de dados pessoais.

6.6.3. TRATAMENTO DE DADOS DE IDOSOS

6.6.3.1. A Semove deve garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta LGPD e do Estatuto da Pessoa Idosa, de modo a facilitar a obtenção de acesso a informações quanto ao tratamento de seus dados pessoais.

6.7. AGENTES DE TRATAMENTO DE DADOS

6.7.1. No papel central, por sua importância, tem-se o **titular**, qualquer pessoa natural, protegida pelo princípio da autodeterminação informativa (inciso II do art. 2º da LGPD).

6.7.2. O agente de tratamento de dados pessoais pode assumir as responsabilidades de controladora e/ou operadora de dados pessoais. Ambos são solidariamente responsáveis pelos danos causados pelo tratamento, quando houver descumprimento das obrigações da legislação de proteção de dados ou quando não tiverem sido seguidas as instruções lícitas da controladora de dados pessoais.

6.7.3. A Semove, seja no papel de controladora ou operadora, deve tratar apenas os dados pessoais necessários, de forma consistente com a legislação, e têm a tradição de manter os mais altos padrões de integridade na gestão de tais dados, e quando aplicável, dos consentimentos de seus titulares.

6.7.4. Sempre que assume o papel de controladora de dados pessoais, a Semove assume o compromisso de determinar os objetivos e os meios do tratamento de dados pessoais, sem ordens de um terceiro.

6.7.5. Já na posição de operadora de dados pessoais, a Semove processa os dados em nome de um terceiro, seguindo suas orientações, tais como: fornecedores, parceiros de negócios e órgãos públicos, conforme as instruções destes, mediante a celebração de um acordo no qual cada empresa se compromete com os ditames da legislação, em especial com a LGPD.

6.7.6. Tanto na condição de controladora como de operadora de dados pessoais, a Semove deve observar os princípios e diretrizes da PLGPD, além de cumprir com a legislação brasileira e internacional acerca da proteção e privacidade de dados pessoais.

6.7.7. O término de tratamento dos dados deve ocorrer quando a finalidade for alcançada, com o fim do período de tratamento ou mediante determinação da ANPD, por violações à LGPD.

6.8. PERÍODO DE RETENÇÃO DOS DADOS

6.8.1. A Semove não pode manter dados pessoais por período superior ao necessário para os motivos pelos quais foram coletados. Portanto, após o término da finalidade, os dados pessoais devem ser eliminados, no âmbito e limites técnicos das atividades, permitindo sua conservação somente nas hipóteses em que houver previsão legal.

6.8.2. Todo recurso tecnológico da Semove que for doado, leilado, cedido, vendido, enviado para reparo, com custódia por terceiros ou for descartado como resíduo sólido, somente poderá ser disponibilizado após confirmação da eliminação das informações pelas áreas técnicas responsáveis, de forma segura, garantindo que terceiros não as acessem. Caberá aos gestores que controlam esses ativos os encaminharem às áreas técnicas competentes.

6.8.3. Os procedimentos técnicos para eliminar os dados pessoais desnecessários dos seus computadores, dispositivos móveis, sistemas e servidores conectados à rede corporativa, de forma segura e definitiva, devem ser validados pela Gerência de Segurança da Informação e pela Gerência de Infraestrutura e, quando envolver dados pessoais, a Gerência de Proteção de Dados e Privacidade. Além disso, quando se tratar da eliminação de dados de **sistemas** analíticos ou **transacionais**, a Gerência de Dados e a Gerência de Projetos ou o responsável pela Gestão de Projetos deverão ser envolvidos para acompanhar as tratativas das áreas técnicas.

6.8.4. Já os dados mantidos em repositórios físicos, devem ser eliminados com segurança, preferencialmente destruídos, triturados, de modo que não seja possível sua reutilização.

6.8.5. A eliminação de documentos que contemplem dados pessoais deverá seguir as regras de temporalidade e gestão documental específicas a serem aprovadas, observadas as diretrizes da ANPD e dos demais órgãos públicos, e o disposto no art. 16º da LGPD.

6.8.6. Em caso de dúvidas, o gestor, diretor ou presidente-executivo poderá consultar diretamente a Gerência de Proteção de Dados e Privacidade, ou indiretamente, por intermédio do seu agente de Proteção de Dados e Privacidade, que tem o dever de apoiá-lo em todas as orientações e ações relativas à LGPD.

6.9. DIREITO DOS TITULARES

6.9.1. A Semove deve manter os titulares informados sobre todos os aspectos relacionados ao processamento de seus dados e disponibilizar canais de acesso do titular aos seus direitos, em especial:

- i. a finalidade do tratamento para o qual os dados pessoais foram coletados;
- ii. as hipóteses legais do tratamento do dado pessoal, previstos no item 6.3.1 desta PLGPD;
- iii. a descrição do legítimo interesse da Semove, quando aplicável;
- iv. o tempo de armazenamento do dado pessoal e/ou o critério utilizado para determinar o **período de retenção**;

v. informações sobre eventual compartilhamento dos dados pessoais com outras empresas, a finalidade do compartilhamento e informações sobre o destinatário;

vi. se há intenção de transferência de algum dado pessoal para outro país ou organização internacional, a finalidade e o país de destino;

vii. informações de contato do *DPO*.

6.9.2. Adicionalmente, a Semove deve estar apta a garantir que os titulares possam exercer livremente e de forma gratuita todos os direitos previstos na lei.

i. acesso aos dados pessoais;

ii. solicitar a exclusão, anonimização, pseudonimização, correção e/ou atualização dos dados pessoais, desde que não haja um impedimento ou exclusão legal e que não prejudique o legítimo interesse da Semove;

iii. solicitar informação das entidades públicas e privadas com as quais a controladora realizou uso compartilhado de dados;

iv. opor-se ao tratamento dos dados pessoais, desde que de forma motivada;

v. retirar o seu consentimento anteriormente concedido para o tratamento de seus dados pessoais;

vi. solicitar a portabilidade de seus dados pessoais, exceto se já tiver sido realizado procedimento de anonimização.

6.9.3. Para esse fim, todos os pleitos dos titulares, após análise prévia da área de negócio receptora, devem ser direcionados ao *DPO*, através do **Formulário Direito Titular LGPD (ANEXO IV)** disponível no *website* da Semove, que irá analisar sua completude e, após, definir uma devolutiva que deverá ser formalmente endereçada ao titular.

6.9.4. Os direitos do titular não são absolutos, razão pela qual a Semove se reserva o direito de rejeitar pedidos, desde que a resposta seja transparente, tempestiva e devidamente fundamentada.

6.9.5. O titular tem direito a solicitar a revisão, quando aplicável, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade, exceto se estas informações estiverem protegidas por segredos comercial e industrial, embora estejam suscetíveis às auditorias pela ANPD, **Fundação de Proteção e Defesa do Consumidor (Procon)**, **Secretaria Nacional do Consumidor (Senacon)** ou demais órgãos fiscalizadores, quando o tratamento automatizado do dado pessoal não for usado para fins discriminatórios.

6.9.6. O *DPO* é responsável, em nome da Semove, pela gestão das solicitações e consentimentos dos titulares, além de definir as devolutivas, padrões ou específicas, a serem formalizados dentro do prazo legal previsto na LGPD, salvo se determinado de forma diversa pelas autoridades fiscalizadoras.

6.9.7. No caso de **pleitos de baixa complexidade**, que demandem a confirmação de existência ou acesso aos dados pessoais, a devolutiva formal deve ser providenciada em formato simplificado, no prazo de 5 (cinco) dias úteis.

6.9.8. Para os **pleitos de alta complexidade**, a devolutiva formal deve ocorrer em um período igual ou inferior a 15 (quinze) dias do seu registro, por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios e a finalidade do tratamento dos dados pessoais, observados os segredos comercial e industrial.

6.9.9. Os prazos acima indicados poderão ser prorrogados caso haja dúvida, inconsistência ou insuficiência de informação prestada pelo titular. Nestes casos, os prazos passarão a contar após o fornecimento das informações complementares.

6.9.10. O GTD e/ou outras áreas de negócios da Semove poderão ser consultados, a critério do *DPO*, que possui independência e apoio inequívoco dos agentes de governança para se posicionar sobre o tratamento adequado dos dados pessoais em nome da Semove.

6.10. PRIVACIDADE NA COLETA DE DADOS

6.10.1. Ao coletar e tratar dados pessoais, a Semove deve obedecer aos princípios de necessidade e finalidade inerentes à LGPD, portanto, os dados pessoais deverão ser armazenados nos servidores de rede e/ou banco de dados (i.e., preferencialmente hospedados em nuvem), controlados pela Gerência de Infraestrutura pelo prazo mínimo necessário para cumprimento das finalidades para as quais foram coletados, incluindo obrigações legais, contratuais, de prestação de contas ou requisição de autoridades competentes.

6.10.2. Os dados pessoais coletados poderão variar de acordo com a relação mantida com a Semove e serão colhidos das seguintes formas:

- *Fornecimento pelo titular:* são inseridos ou encaminhados pelo titular do dado ou seu representante legal, decorrentes do contato, cadastro ou instrumento contratual firmado com a Semove, podendo ser, mas não limitados aos seguintes dados: nome completo, nº do CPF, nº do registro civil, data de nascimento, estado civil, nacionalidade, naturalidade, filiação, dependentes, profissão, dados da empresa de que é sócio, proprietário, representante legal ou preposto, endereço completo, dados bancários, endereço de *e-mail*, número de telefone e dados biométricos.
- *Coleta a partir do uso dos serviços:* são aqueles relacionados à utilização de meios eletrônicos para o processamento e liquidação de transações eletrônicas de pagamento ou para a transmissão de informações relativas a transações não financeiras, objeto de serviço prestado, capturadas pela Semove e transmitidas e/ou compartilhadas com terceiros no contexto e limite necessário para o cumprimento de sua finalidade, prevista em instrumentos contratuais ou legais.
- *Fornecimento por terceiros:* são os dados pessoais recebidos de terceiros, como parceiros de negócios, fornecedores ou demais partes interessadas ou relacionadas à Semove, desde que haja consentimento prévio do titular.

- **Coleta automática:** quando o **usuário** acessar o *website* oficial da Semove, algumas informações serão coletadas automaticamente, incluindo: características do dispositivo utilizado para o acesso, navegador utilizado para o acesso, origem do protocolo da *internet* (*Internet Protocol* ou *IP*, com data e hora), informações sobre a sua interação na página da Semove, coletadas por meio de **cookies**.

6.10.3. Em linhas gerais e, de forma não exaustiva, os dados pessoais serão coletados e armazenados pela Semove para:

- prover o cliente com o acesso às áreas restritas do *website*, aplicativo ou sistemas, oferta de serviços, bem como responder aos questionamentos, reclamações e solicitações feitas pelos usuários através dos meios de comunicação da Semove;
- cumprir obrigações legais ou contratuais, atender regulamentações governamentais, autoridades fiscais, Poder Judiciário, como sentenças e acordos, e/ou qualquer outra autoridade competente, bem como para o exercício regular de direito da Semove;
- proteger o titular e a Semove contra fraudes e quaisquer outros atos ilícitos, incluindo a troca de informações com órgãos públicos, outras empresas e organizações para fins investigativos e informativos;
- implementar medidas adequadas de segurança para resguardar os usuários e a Semove;
- atender aos interesses legítimos da Semove, desde que respeitados todos os direitos do titular;
- pesquisa sobre o nível de satisfação dos usuários em relação aos serviços prestados pela Semove, através de diferentes canais, desde que expressamente consentida pelo titular;
- investigações de condutas irregulares ou ilícitas, em especial, quando decorre de denúncias realizadas pelo Canal de Denúncia e Diálogo Voz Ativa (Voz Ativa).

6.11. CANAIS DE ATENDIMENTO AO TITULAR

6.11.1. Todos os pedidos relativos ao exercício de direitos previstos na LGPD e PLGPD devem ser formalizados por meio do Formulário Direito Titular LGPD (ANEXO IV) disponível no *website* da Semove.

6.11.2. Todos os pedidos serão analisados pela Gerência de Proteção de Dados e Privacidade, que responderá ou autorizará o envio das devolutivas formais ao titular, à ANPD ou demais órgãos fiscalizadores nos prazos previstos em lei, ou conforme definido nos itens 6.9.7 e 6.9.8 desta PLGPD.

6.12. PRIVACIDADE NAS RELAÇÕES DE TRABALHO

6.12.1. Em relação aos dados de seus colaboradores, gestores e agentes de governança, a Semove deve coletar dados pessoais exclusivamente para fins relacionados ao trabalho, investigações internas, diligências, cumprimento de obrigações acessórias junto aos órgãos públicos fiscalizadores ou de

obrigações contratuais e legais. Para esses fins, poderá também coletar dados pessoais dos seus **parentes** ou **aparentados por afinidade**, uma vez que existe um fundamento legal ou contratual que dispensa a necessidade de consentimento do titular (ex.: programa de benefícios, dependentes para fins de Imposto de Renda, *Background Check*, *Due Diligence* etc.).

6.12.2. A Semove possui o direito de monitorar, fiscalizar e acessar, sem autorização prévia do titular, todos os recursos tecnológicos corporativos, como: aparelho celular, computador, *tablet*, CFTV, dentre outros, conforme a PSI. É proibido o monitoramento de recursos tecnológicos privados, sem o consentimento do proprietário.

6.12.3. As dependências da Semove poderão se utilizar de câmeras do CFTV, para garantir a segurança do titular, resguardado o direito de informação, afixada de forma clara e de fácil acesso ao público. As referidas imagens só serão acessadas por pessoas autorizadas, em caráter restrito, por áreas responsáveis pela segurança patrimonial, por investigação interna ou por atender autoridade policial ou judicial.

6.12.4. As imagens possuem restrição de acesso e serão visualizadas apenas por profissionais qualificados e autorizados, tais como: equipe de segurança patrimonial, **equipe investigativa**, autoridade policial ou judicial, mediante formalização da solicitação de acesso, por *e-mail*, direcionado ao gestor responsável pela gestão do contrato que regulamenta os serviços do CFTV utilizado nas dependências da Semove.

6.12.5. O período de retenção das gravações, que são dados pessoais sensíveis, deve ser estabelecido pela área de negócios competente, pelo prazo mínimo necessário ao cumprimento de sua finalidade, respeitada a capacidade de memória do CFTV da Semove, e deve ser regulamentado por instrumento normativo específico.

6.13. PRIVACIDADE NO GERENCIAMENTO DE PROJETOS

6.13.1. Todos os projetos devem surgir dentro do conceito de “*Privacy by Design*” e devem estar aderentes à legislação em vigor e aos princípios e diretrizes da PLGPD e da PSI.

6.13.2. Desde a sua concepção, o gestor responsável pelo gerenciamento de projetos (sistêmicos ou não) que envolvam o tratamento de dados pessoais deve submetê-los à análise obrigatória da Gerência de Proteção de Dados e Privacidade. E, quando envolver criação ou desenvolvimento de melhorias sistêmicas, à análise da Gerência de Segurança da Informação, a fim de validar sua aderência aos requisitos das boas práticas de segurança da informação, da PSI e demais regulamentações sobre confidencialidade da informação. Quando houver impacto nos sistemas analíticos, a Gerência de Dados também deverá ser obrigatoriamente envolvida em sua homologação.

6.13.3. A Diretoria Jurídica/Coordenação Jurídica deverá ser consultada sempre que houver necessidade de obter posicionamento legal ou esclarecimento acerca da legislação ou regulamentação que, de certa forma, possa impactar o projeto.

6.13.4. A Gerente de Projetos ou o responsável pela Gestão de Projetos deverão garantir que os projetos sistêmicos sejam devidamente homologados pelas áreas de negócios demandantes, considerando a avaliação técnica e formal de todas as áreas acima, em conformidade com a legislação em vigor, a PLGPD e a PSI.

6.13.5. Não obstante, quando se tratar de sistema desenvolvido internamente que já esteja em funcionamento (i.e., sistemas legados), o gestor da área de negócios será responsável por solicitar à Gerência de Projetos ou ao responsável pela gestão de projetos sistêmicos a adequação desse sistema aos princípios e diretrizes desta PLGD e da PSI. Caso contrário, em caso de ocorrência de incidente de segurança da informação envolvendo vulnerabilidades nos sistemas internos sob sua gestão, ele estará suscetível à aplicação de medidas disciplinares, ou em última instância, ao ajuizamento de processos de responsabilização legal, conforme previsto na Política de Consequências, por ter sido omissos ou negligente, quanto às medidas preventivas de proteção da informação custodiada pela Semove.

6.14. PRIVACIDADE NAS RELAÇÕES COM O PODER PÚBLICO

6.14.1. A Semove está sujeita a determinações do Poder Público, tais como a prestação de contas decorrente de responsabilidades regulatórias e de interesse público, decisões judiciais e administrativas, motivo pelo qual não pode garantir a privacidade total dos dados pessoais em tais hipóteses.

6.14.2. A Semove, enquanto exerce um papel de operadora de dados pessoais, por orientações e atribuições emanadas de autoridades públicas, devem apoiá-las na prestação de contas à ANPD ou demais órgãos fiscalizadores, sendo sua responsabilidade limitada aos dados pessoais sob sua custódia, por força de acordos, convênios ou outros instrumentos contratuais celebrados com a administração pública, seja na esfera Federal, Estadual ou Municipal.

6.15. PRIVACIDADE NO RELACIONAMENTO COM DEMAIS PARTES INTERESSADAS OU RELACIONADAS

6.15.1. A Semove deve assegurar a confidencialidade e privacidade das informações recebidas dos seus clientes, observando-se também os ditames previstos na LGPD, CDC, PSI e nesta PLGD, sendo certo que a violação dos direitos dos consumidores constitui infração penal. Assim, a conduta de impedir ou dificultar o acesso do consumidor, bem como deixar de corrigir ou lhe entregar informações a seu respeito, configura crime com pena de detenção ou multa, nos termos dos artigos 72 e 73 do CDC, além do infrator poder responder por medidas disciplinares ou processos de responsabilização legal. Os dados pessoais de fornecedores, clientes e demais parceiros de negócios devem ser tratados pela Semove somente para fins legais e regulares, previstos em instrumentos legais e contratuais, e condizentes com a LGPD.

6.15.2. A Semove se reserva o direito de compartilhar informações com terceiros, com o objetivo de cumprir com o escopo contratado, desde que haja cláusulas ou um acordo de confidencialidade e privacidade celebrado entre as partes. No entanto, se essas informações contiverem dados pessoais, o compartilhamento só é permitido mediante consentimento do titular ou, sem consentimento, desde que enquadradas nas hipóteses previstas no item 6.3.1 desta PLGD.

6.15.3. É importante enfatizar que todos os pleitos dos titulares requerem um posicionamento formal que, direta ou indiretamente, passarão pelo crivo do *DPO*. Nesse sentido, se decorrerem de relacionamentos com outras partes interessadas ou relacionadas à Semove, cabe ao gestor responsável ou seu superior imediato, através do seu agente de Proteção de Dados e Privacidade, direcioná-los ao

DPO, de acordo com os procedimentos e orientações internas, visando esclarecer tempestivamente ao titular seus direitos, justificativas para o tratamento, metodologias, período de retenção (quando aplicável) de cada dado pessoal, dentre outras informações que podem ser requeridas.

6.16. SEGURANÇA DOS DADOS

6.16.1. A Semove deve adotar medidas de segurança, técnicas e administrativas, para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, divulgação ou qualquer forma de tratamento inadequado ou ilícito. Tais mecanismos devem ser utilizados como atenuantes de responsabilidade em eventuais processos de apuração de acessos não autorizados ou criminosos.

6.16.2. Para manter a confidencialidade, integridade e privacidade de todos os dados pessoais armazenados em seus servidores, arquivos físicos ou hospedados em nuvem, devem ser utilizadas chaves ou tecnologias da informação avançadas e eficazes para a proteção desses dados, em conformidade com a legislação.

6.16.3. Ao assegurar a proteção da informação, desde a sua criação até a eliminação, a mesma deve ser classificada sob a perspectiva de níveis de confidencialidade e relevância, conforme as boas práticas de segurança da informação, a PSI e demais instrumentos normativos correlatos. Para classificá-la, deverão ser consideradas seu uso em projetos estratégicos ou em cumprimento de obrigações contratuais e legais. Quanto maior o nível de confidencialidade e relevância da informação, maior a necessidade de controles internos preventivos, visando protegê-la.

6.16.4. Os dados pessoais não serão publicamente disponibilizados ou comercializados em nenhuma circunstância, sendo vedada sua utilização para finalidades distintas da justificativa dada ao titular, no momento da coleta.

6.16.5. A Semove deverá, quando viável, adotar mecanismos de anonimização e pseudonimização dos dados pessoais, sem prejuízo do compromisso de protegê-los contra crimes cibernéticos.

6.16.6. Os fornecedores terceirizados ou parceiros de negócios que tratem dados pessoais sob as instruções da Semove devem obrigatoriamente se comprometer, mediante acordo ou instrumento contratual por escrito, a:

- i. adotar todas as medidas de segurança, bem como todos os controles técnicos e administrativos apropriados para garantir a confidencialidade e segurança dos dados pessoais;
- ii. processar os dados pessoais somente conforme instruções da Semove;
- iii. eliminar, de forma segura e sustentável, ou devolver os dados pessoais após o término da prestação de serviço;
- iv. relatar imediatamente qualquer violação de dados à Semove;

v. permitir que a Semove realize auditorias, de forma a demonstrar que seus sistemas e processos internos estejam aderentes às boas práticas de segurança da informação e às diretrizes da PLGPD, PSI e demais instrumentos normativos correlatos.

6.16.7. Todas as suspeitas ou ocorrência de incidentes de segurança da informação devem ser reportadas à Gerência de Segurança da Informação; à Gerência de Proteção de Dados e Privacidade, quando contemplar dados pessoais, e à Gerência de Dados, quando envolver sistemas analíticos, de forma que haja tempo hábil de estabelecer um plano de gestão de incidentes de segurança, com o apoio do GTD e demais áreas de negócios que tenham alguma ação mitigadora do incidente de segurança da informação. Os incidentes de segurança da informação **significativos** devem ser reportados ao Órgão Diretivo da Semove e à Gerência de Auditoria Interna, que deverá realizar ou acompanhar as etapas de investigação interna e a execução das medidas mitigadoras da crise.

6.16.8. Todo incidente de segurança da informação significativo, contendo ou não dados pessoais, que requeira uma investigação interna para se determinar a culpabilidade de algum colaborador, gestor, agente de governança ou terceiro, deve obrigatoriamente ser registrado no Voz Ativa, para que se estabeleça um processo de investigação interna ou externa, de forma imparcial e independente, que passe pela avaliação dos representantes do CIC e mantenha o reporte aos agentes de governança competentes.

6.16.9. Cabe à Semove implementar procedimentos para gerir incidentes de segurança da informação ocorridos e notificar eventuais vazamentos de dados.

6.16.10. Diante de um incidente de segurança da informação que possa resultar em dano significativo ao titular, a Semove, por meio da Gerência de Proteção de Dados e Privacidade, deverá avaliá-lo e providenciar uma comunicação formal à ANPD, no prazo de 2 (dois) dias úteis, através do preenchimento do formulário *on-line* disponibilizado no *website* <https://www.gov.br/anpd/pt-br>. Tal comunicação deverá ser realizada também, em um prazo razoável, ao titular e, quando demandado, às demais autoridades fiscalizadoras da privacidade de dados.

6.17. SANÇÕES JUDICIAIS E ADMINISTRATIVAS

6.17.1. A Semove está sujeita à fiscalização da ANPD, autoridades judiciais, órgãos setoriais reguladores do transporte público de passageiros, Senacon e Procon.

6.17.2. O regulamento de dosimetria da ANPD busca garantir a proporcionalidade entre a sanção aplicada e a gravidade da conduta do agente de tratamento dos dados pessoais, além de proporcionar segurança jurídica aos processos fiscalizatórios e garantir o direito ao devido processo legal e ao contraditório. As infrações sujeitarão as empresas infratoras às seguintes sanções administrativas:

i. advertência;

ii. multa simples, de até 2% (dois por cento) do faturamento da empresa, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais), por infração;

iii. multa diária, com limite total de R\$ 50.000.000,00 (cinquenta milhões de reais);

- iv. publicização da infração;
- v. bloqueio dos dados pessoais;
- vi. eliminação dos dados pessoais;
- vii. suspensão parcial do funcionamento do banco de dados por, no máximo, 6 (seis) meses, prorrogável por igual período, até que se regularize a situação;
- viii. suspensão do exercício da atividade de tratamento dos dados pessoais por, no máximo, 6 (seis) meses, prorrogável por igual período;
- ix. proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

6.17.3. As sanções são aplicadas depois de uma análise feita em processo administrativo caso a caso. A empresa infratora terá a oportunidade de ampla defesa, de acordo com as peculiaridades do caso concreto. São parâmetros para aplicação das sanções:

- a) gravidade e natureza das infrações e dos direitos pessoais afetados;
- b) boa-fé do infrator;
- c) vantagem auferida ou pretendida pelo infrator;
- d) condição econômica do infrator;
- e) reincidência;
- f) grau do dano;
- g) cooperação do infrator;
- h) adoção de mecanismos e procedimentos internos capazes de minimizar o dano;
- i) adoção de boas práticas e governança;
- j) pronta adoção de medidas corretivas; e
- k) proporcionalidade entre a gravidade da falta e a intensidade da sanção.

6.17.4. As empresas infradoras que não se adequarem às disposições da LGPD estarão sujeitas a infrações como o bloqueio ou a eliminação definitiva dos dados pessoais irregularmente tratados.

6.17.5. Para além das sanções administrativas, a Semove também poderá responder judicialmente por possíveis infrações no âmbito de proteção de dados, ficando submetidas à legislação sobre o tema e às penalidades estabelecidas em lei.

6.18. INFORMAÇÕES DO *DPO*

6.18.1. A Semove disponibiliza, em todos os seus canais de diálogo e atendimento ao cliente, aplicativos, *websites*, redes sociais, *Intranet*, as informações de contato do *DPO*.

6.18.2. Os pleitos provenientes de outras partes interessadas ou relacionadas à Semove devem ser analisados previamente pelo(s) agente(s) de Proteção de Dados e Privacidade alocado(s) em cada área de negócios que interaja com essas partes e, após, redirecionados ao *DPO*, por meio de telefone, *e-mail* ou o preenchimento do Formulário Direito Titular LGPD (ANEXO IV).

6.18.3. Quaisquer esclarecimentos sobre a LGPD ou legislação complementar que disponha sobre a proteção de dados e privacidade da informação ou sobre a PLGPD e instrumentos normativos correlatos devem ser direcionados à Gerência de Proteção de Dados e Privacidade ou, alternativamente, serem registrados na sessão “esclarecer dúvidas”, por meio do Voz Ativa, uma vez que também serão redirecionados ao *DPO*, para que haja uma devolutiva ao relator.

6.18.4. As informações do *DPO* são:

- nome: Renato de Araújo Cid Santa Rita
- *e-mail*: renato.araujo@semove.org.br

6.18.5. Essas informações estão disponíveis às partes interessadas ou relacionadas interna ou externamente ao ambiente de negócio da Semove. No entanto, para o registro de pleitos dos titulares, sejam de baixa ou alta complexidade, conforme as diretrizes estabelecidas nos itens 6.9.7 e 6.9.8 desta PLGPD, devem ser exclusivamente registrados e centralizados no Formulário Direito Titular LGPD (ANEXO IV).

6.19. CONSEQUÊNCIAS PUNITIVAS

6.19.1. Todos devem ser diligentes e responsáveis por suas ações no trabalho, portanto, cada indivíduo, independentemente do cargo/função que ocupe, responde integralmente por qualquer conduta que resulte em danos significativos ao negócio, imagem e reputação da Semove e suas partes interessadas ou relacionadas. Toda conduta ou deliberação que conflite com as diretrizes desta PLGPD é proibida, portanto, a comprovação de uma infração pode acarretar aplicação de medidas disciplinares ou, em última instância, o ajuizamento de ação de responsabilização administrativa, civil ou penal contra o colaborador, gestor ou agente de governança que infringir ou incentivar sua violação, conforme Política de Consequências. Para esse fim, a Semove disponibiliza o Voz Ativa, que permite o registro de relatos anônimos ou identificados nos seguintes canais:

- *website*: <https://www.canalconfidencial.com.br/vozativa/>;
- telefone: 0800 741 0003 (atendimento pessoal, de segunda a sábado, das 12h às 22h);
- *e-mail*: vozativa@canalconfidencial.com.br;
- caixa postal: 521 CEP 06320-971.

6.19.2. As diretrizes sobre o funcionamento do Voz Ativa estão previstas na Política do Canal de Denúncia e Diálogo Voz Ativa, divulgada nos meios de comunicação da Semove.

7. INSTÂNCIAS CORPORATIVAS DE APROVAÇÕES

7.1. Esta PLGPD foi revisada pela Gerência de Proteção de Dados e Privacidade e submetida à análise dos representantes do CIC em 06/02/2024.

7.2. Foi aprovada pelo Órgão Diretivo em 14/05/2024 e submetida à aprovação dos conselheiros do CG em 20/06/2024, que, no conjunto, autorizaram sua publicação.

7.3. Recomenda-se, como boa prática de governança corporativa, submetê-la a todas as instâncias responsáveis por sua aprovação, sempre que houver alterações significativas em seu conteúdo. Caso contrário, poderá ser publicada com o propósito de se realizarem pequenas atualizações.

8. ANEXOS

8.1. A PLGPD possui os seguintes anexos:

- ANEXO I - Termo de Aceite - Pessoa Física.
- ANEXO II - Termo de Aceite - Pessoa Jurídica.
- ANEXO III – Glossário.
- ANEXO IV - Formulário Direito Titular LGPD.

8.2. Os anexos são partes integrantes desta PLGPD, embora sejam divulgados separadamente, pois podem sofrer constantes atualizações.

8.3. Todos os colaboradores, gestores, diretores, presidente-executivo e demais pessoas físicas consideradas partes interessadas ou relacionadas à Semove devem conhecer e assinar os Termos de Aceite desta PLGPD (ANEXOS I e II).

8.4. A Gerência de Proteção de Dados e Privacidade deverá realizar a gestão das assinaturas dos Termos de Aceite (ANEXO I) desta PLGPD.

8.5. A Diretoria Jurídica/Coordenação Jurídica coletará as assinaturas dos Termos de Aceite da PLGPD (ANEXOS I e II) pelos conselheiros do CG e delegados da AGRS.

8.6. Com o intuito de apoiar os gestores na gestão dos Termos de Aceite desta Norma (ANEXOS I), a Gerência de Segurança da Informação realizará a coleta de assinaturas eletrônicas dos colaboradores, gestores, diretores e presidente-executivo da Semove, por meio de sistema de gestão de instrumentos normativos.

8.7. Também recomendamos que os gestores ou membros do Órgão Diretivo demandem a assinatura eletrônica dos Termos de Aceite desta PLGPD (ANEXO II) dos empregados pertencentes às partes interessadas ou relacionadas, que se relacionem com a Semove por meio de acordo, proposta, instrumento contratual ou em função da legislação vigente, desde que neste relacionamento, haja tratamento de dados pessoais, que se encontrem sob custódia da Semove.

8.8. Os Termos de Aceite (ANEXO I e II) desta PLGPD devem ser mantidos em local seguro, de acordo com o prazo previsto nesses instrumentos contratuais.

ANEXO I - TERMO DE ACEITE - PESSOA FÍSICA

Pelo presente instrumento ("Termo de Aceite"), _____
_____, [Nome completo do empregado(a) (Declarante)], inscrito(a) no CPF/MF sob
o nº [_____.____.____ - ____], empregado(a) da [Federação das Empresas de Mobilidade do Estado do Rio de
Janeiro (Requerente)] _____,
DECLARA que:

i. Tomou conhecimento e compreendeu as disposições previstas na POL001.005.DPO.SEM - Política de Proteção de Dados e Privacidade, divulgada nos canais de comunicação da Requerente, se comprometendo a respeitar, no desempenho de suas atividades, todos os seus termos, condições e princípios, estando sujeito(a) às medidas disciplinares cabíveis advindas do descumprimento, sem prejuízo de responder por processos de responsabilização legal;

ii. As diretrizes da Política de Proteção de Dados e Privacidade não se sobrepõem à legislação vigente, convenção, contrato social, regimento interno e, se complementam aos demais instrumentos normativos ou contratuais publicados pela Requerente;

iii. O Termo de Aceite tem o propósito de evidenciar a eficácia dos instrumentos normativos como padrão de conduta de uma organização, pilar específico do Programa de Integridade e Conformidade da Requerente, conforme art. 57, inciso II, do Decreto nº 11.129/2022 (novo Decreto Anticorrupção). Por esse motivo, é importante que o(a) Declarante tome conhecimento, concorde e cumpra com as diretrizes aqui estabelecidas e aprovadas pelo Órgão Diretivo da Requerente, bem como por instâncias superiores de governança corporativa.

iv. Os dados pessoais coletados neste Termo de Aceite serão mantidos pela Requerente pelo tempo necessário ao cumprimento de sua finalidade, conforme tabela abaixo:

Dados pessoais coletados	Finalidade de tratamento de dados pessoais
Nome completo, nº do CPF e o aceite digital do Declarante (campo de preenchimento obrigatório)	Identificar o(a) Declarante que anuiu com as diretrizes desta Política. O nº do CPF é necessário para se evitar homônimos, ou seja, pessoas com nomes iguais.
E-mail do(a) Declarante (campo de preenchimento obrigatório)	Contatar o(a) Declarante, caso seja necessário. Coletar a assinatura eletrônica do Termo de Aceite desta Política, além de enviar ao(à) Declarante uma comprovação desta assinatura.

v. Este Termo de Aceite não será compartilhado com terceiros, salvo se decorrer de: i) investigações internas, ii) ação ajuizada no âmbito administrativo ou judicial em face da Requerente ou iii) requerimento legal por parte de órgãos fiscalizadores, situação que não requer consentimento do(a) Declarante.

vi. Este Termo de Aceite será armazenado pela Requerente, de forma segura, enquanto o(a) Declarante permanecer com contrato de trabalho estabelecido com a Requerente ou após 3 (três) anos contados da data de término desse contrato de trabalho, quando será excluído, salvo se for ajuizada ação, pelo(a) Declarante, em face da Requerente. Neste caso, este documento ficará armazenado até o término da ação.

Rio de Janeiro, ____ de _____ de 20__.

Aceite digital do(a) empregado(a) (Declarante)

E-mail corporativo do(a) Declarante:

ANEXO II - TERMO DE ACEITE - PESSOA JURÍDICA

Pelo presente instrumento (“Termo de Aceite”), _____
_____ [Nome completo do(a) empregado(a) (Declarante)], inscrito(a) no CPF/MF sob
o nº _____, empregado(a) da (nome da Empresa) ¹ _____
_____, inscrito(a) no CNPJ sob o nº _____,
DECLARA para a [Semove - Federação das Empresas de Mobilidade do Estado do Rio de Janeiro.
(Requerente)] _____, que:

i. Tomou conhecimento e compreendeu as disposições previstas na POL001.005.DPO.SEM - Política de Proteção de Dados e Privacidade, divulgada nos canais de comunicação da Requerente, se comprometendo a respeitar, no desempenho de suas atividades, todos os seus termos, condições e princípios, estando sujeito(a) às sanções cabíveis advindas do descumprimento, sem prejuízo de responder por processos de responsabilização legal;

ii. As diretrizes da Política de Proteção de Dados e Privacidade não se sobrepõem à legislação vigente, convenção, contrato social, regimento interno e, se complementam aos demais instrumentos normativos ou contratuais publicados pela Requerente;

iii. O Termo de Aceite tem o propósito de evidenciar a eficácia dos instrumentos normativos como padrão de conduta de uma organização, pilar específico do Programa de Integridade e Conformidade da Requerente, conforme art. 57, inciso II, do Decreto nº 11.129/2022 (novo Decreto Anticorrupção). Por esse motivo, é importante que o(a) Declarante tome conhecimento, concorde e cumpra com as diretrizes aqui estabelecidas e aprovadas pelo Órgão Diretivo da Requerente, bem como por instâncias superiores de governança corporativa.

iv. Os dados pessoais coletados neste Termo de Aceite serão mantidos pela Requerente pelo tempo necessário ao cumprimento de sua finalidade, conforme tabela abaixo:

Dados pessoais coletados	Finalidade de tratamento de dados pessoais
Nome completo, nº do CPF e o aceite digital do Declarante (campo de preenchimento obrigatório)	Identificar o(a) Declarante que anuiu com as diretrizes desta Política. O nº do CPF é necessário para se evitar homônimos, ou seja, pessoas com nomes iguais.
E-mail do(a) Declarante (campo de preenchimento obrigatório)	Contatar o(a) Declarante, caso seja necessário. Coletar a assinatura eletrônica do Termo de Aceite desta Política, além de enviar ao (à) Declarante uma comprovação desta assinatura.

¹ Empresa: refere-se a qualquer pessoa jurídica que estabelecer instrumento contratual, acordo, convênio ou instrumento correlato com a Semove (ex.: fornecedores, parceiros e demais partes interessadas ou relacionadas).

v. Este Termo de Aceite não será compartilhado com terceiros, salvo se decorrer de: i) investigações internas, ii) ação ajuizada no âmbito administrativo ou judicial em face da Requerente ou iii) requerimento legal por parte de órgãos fiscalizadores, situação que não requer consentimento do(a) Declarante.

vi. Este Termo de Aceite será armazenado pela Requerente, de forma segura, enquanto a empresa do(a) Declarante mantiver contrato, acordo, convênio ou instrumento correlato com a Requerente ou por 5 (cinco) anos contados da data de término desta contratação, quando será excluído, salvo as situações previstas no item (v) acima. Neste caso, este documento ficará armazenado até o término destas situações previstas no item precedente.

Rio de Janeiro, _____ de _____ de 20____.

Aceite digital do(a) empregado(a) (Declarante)

E-mail corporativo do(a) Declarante:

ANEXO III - GLOSSÁRIO

Agente de governança: indivíduo que ocupa um papel de liderança no Órgão Diretivo (ex.: diretor ou presidente-executivo) e qualquer membro dos órgãos envolvidos no sistema de governança corporativa (ex.: representantes do CIC, conselheiros do CG, delegados da AGRS). Os agentes de governança têm influência significativa sobre as decisões estratégicas da Semove.

Agente de Proteção de Dados e Privacidade: é o profissional designado por seu superior imediato como a pessoa-chave, a ser capacitada nas regras e boas práticas de proteção e privacidade de dados. É o ponto focal da Gerência de Proteção de Dados e Privacidade dentro da área de negócios que a apoiará no desenvolvimento e monitoramento do Programa de Governança em Proteção de Dados e Privacidade, dentre outras ações preventivas, detectivas e corretivas identificadas através do Programa de Integridade e Conformidade (PIC).

Agente de tratamento de dados pessoais: o controlador e/ou o operador dos dados pessoais.

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.

Aparentado por afinidade: refere-se aos parentes originados não por vínculo sanguíneo ou adoção, mas por vínculo matrimonial ou relação afetiva (ex.: cônjuge, companheiro(a), enteado(a), sogro(a) e cunhado(a) ou namorado(a)).

Assembleia Geral de Representantes dos Sindicatos (AGRS): órgão máximo da Semove, composto de delegados indicados por seus acionistas/cotistas, capaz de decidir soberanamente sobre todas as matérias de seu interesse, aprovar o contrato social e propostas do CG em relação ao direcionamento estratégico necessário à consecução dos seus objetos sociais, eleger e destituir integrantes do CG, dentre outras atribuições não incluídas nas atribuições do CG.

Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e observância dos segredos comerciais e industriais, fiscalizar e aplicar sanções administrativas, editar regulamentos, normas e diretrizes para assegurar a proteção de dados e privacidade.

Colaborador: indivíduo que exerce atividade laboral, regulamentada por lei específica (ex.: estagiários) ou regulamentada pela CLT (ex.: jovem aprendiz, empregado subordinado aos cargos de gestão e direção).

Comitê de Integridade e Conformidade (CIC): órgão colegiado e fiscalizador instituído pelo CG no sistema de governança da Semove, no intuito de assessorar seus representantes na implantação do PIC. Seus poderes, escopo e composição estão definidos em seu regimento interno.

Conselho de Gestão (CG): órgão colegiado de governança corporativa responsável pelo direcionamento estratégico, por aprovação dos regimentos internos, contrato social e suas alterações, orçamentos,

contratação e destituição de diretores-executivos, presidente-executivo, auditores internos, bem como, em suas responsabilidades, manifestar opinião sobre propostas direcionadas à AGRS.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controladora do dado pessoal: pessoa física natural ou jurídica, de direito público ou privado, a quem competem as decisões do tratamento de dados pessoais. O controlador determina as finalidades, condições e meios do processamento desses dados pessoais.

Cookies: são arquivos criados com base na coleta automática e consentida de dados de navegação dos usuários (ex.: seu *ID*) nos *websites*.

Custódia: consiste na posse e responsabilidade de se guardar, manter ou proteger algo de terceiros.

Dado analítico: é o conjunto de dados extraídos de sistemas com o objetivo de gerar informação estruturada através de painéis com indicadores (*dashboards*) para auxiliar o processo de tomada de decisão.

Dado pessoal: é a informação relacionada a uma pessoa natural, identificada ou identificável, ou seja, quando é possível a identificação, direta ou indireta, da pessoa natural por trás do dado, como, por exemplo: nome, sobrenome, data de nascimento, documentos pessoais (como CPF, RG, CNH, Carteira de Trabalho, passaporte, número do título de eleitor e crachá de acesso corporativo), endereço residencial ou comercial, número de telefone, *e-mail*, número do cartão de crédito, código de matrícula, número do cartão de vale-transporte, *cookies*, credencial de acesso, protocolo de rede (*internet protocol* ou *IP*).

Dado pessoal sensível: dado pessoal que possui maior proteção da lei e requer maior cuidado no tratamento, pelo fato de poder gerar alguma discriminação ao titular. São considerados dados pessoais sensíveis aqueles que possam, de alguma forma, vir a ter um caráter discriminatório, quando vinculados a uma pessoa natural, tais como: origem racial ou étnica, convicção religiosa, opinião política, filiação a entidades representativas de caráter religioso, filosófico ou político, dados referentes à saúde ou orientação sexual, dados genéticos ou biométricos, dados de apoio a entidades de práticas desportivas.

Dado transacional: é o conjunto de dados registrados em sistemas de informação que apoiam rotineiramente a operação e suas atividades comerciais.

Diretor: indivíduo que ocupa cargo de direção na Semove com o objetivo de executar e cumprir o planejamento estratégico. Quando houver referência ao **diretor-executivo**, significa o diretor com atribuições previstas no contrato social, caso contrário, significa o diretor celetista.

Eliminação: exclusão de um dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Empregado: é o indivíduo contratado para prestar serviços para um empregador, numa carga horária definida, mediante o recebimento de um salário, com vínculo empregatício regulamentado pela CLT.

Equipe investigativa: grupo de profissionais qualificados que integram o grupo dedicado ao procedimento de investigação interna conduzido prioritariamente pela Gerência de Auditoria ou delegada a terceiros, especializados na matéria apurada, acerca de eventual denúncia registrada no Voz Ativa.

Formulário Direito do Titular LGPD: formulário por meio do qual podem ser requeridos pelo titular que tenha algum relacionamento com a Semove, seus direitos à proteção e privacidade dos dados pessoais, garantidos pela LGPD, disponível no *website* da Semove.

Fundação de Proteção e Defesa do Consumidor (Procon): é um órgão público que atua recebendo reclamações no que tange ao direito do consumidor e mediando conflitos entre consumidor, empresas e prestadores de serviços de forma extrajudicial. O órgão também se dedica a fornecer orientações sobre questões de consumo, além de atuar com medidas administrativas para cessar práticas abusivas de empresas. Existem unidades do Procon em todos os estados brasileiros, além de em alguns municípios.

Gap analysis: documento utilizado para identificar as lacunas regulatórias de LGPD, objetivando a definição das medidas de mitigação e o plano de ação baseado nos riscos identificados.

Gestor: indivíduo que ocupa cargo de confiança para gerir uma ou mais áreas de negócios (ex.: coordenadores, supervisores, líderes de loja e gerentes), alocado (direta ou indiretamente) sob a estrutura organizacional de uma Gerência, Diretoria ou da Presidência-Executiva.

Grupo de Trabalho de Dados (GTD): junta técnica de profissionais especializados nas diretrizes da LGPD, objetivando suportar as áreas de negócios na adequação de seus processos aos requerimentos legais. É liderado pelo gerente de Proteção de Dados e Privacidade, que, quando necessário, aciona os agentes de Proteção de Dados e Privacidade da Gerência de Segurança da Informação, Gerência de Dados e Gerência de Controles Internos e Riscos, que integram permanentemente o GTD. Em situações especiais, outras áreas de negócios poderão ser convocadas, temporariamente, a participarem das ações mitigadoras do risco de proteção e privacidade de dados.

Ilha de dados: consiste na extração de dados transacionais e na réplica em sua máquina local, de onde extrai informações para análise e tomada de decisões. Nesse contexto, os dados são passíveis de manipulação manual, sujeitos à desatualização e não estão aderentes aos pilares de segurança da informação (i.e., Confidencialidade, Integridade e Disponibilidade).

Incidente de segurança da informação: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizado pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de instrumentos normativos e procedimentos de segurança ou de uso. De maneira geral, os tipos de atividade comumente reconhecidas como incidentes cibernéticos são: a) tentativas de obter acesso não autorizado a um sistema ou a dados armazenados; b) tentativa de utilização não autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados; c) mudanças não autorizadas de *firmware*, *hardware* ou *software* em um ambiente computacional; d) ataques de negação de serviço (*Denial-of-service attack* ou *DoS*); e e) demais ações que visem afetar a disponibilidade ou integridade dos dados. Um incidente de segurança da informação não significa necessariamente que a informação já esteja comprometida; significa apenas que a informação está ameaçada.

Informação: é o conjunto de dados e conhecimentos organizados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato, incluindo-se os dados que possam constituir referências sobre um determinado indivíduo (i.e., dados pessoais) ou sobre determinado acontecimento, ocorrência ou fenômeno dentro da Semove. A informação é um ativo intangível de propriedade ou custodiado pela Semove, que gera valor para o negócio. Deve estar sempre classificada como pública ou segundo os níveis de confidencialidade: interno, restrito ou sigiloso.

Inventário de dados: documento que reflete o caminho percorrido pelo dado pessoal dentro da Semove, incluindo os processos e procedimentos pelos quais o dado transita. É o registro da origem do dado, a base legal que respalda o seu tratamento, o nível de segurança da base de dados à qual o dado pertence, entre outras informações necessárias para a análise de vulnerabilidades técnicas e jurídicas.

Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta, ou pessoa jurídica de direito privado, sem fins lucrativos, legalmente constituído sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Órgão Diretivo: é o conjunto formado pelos diretores e presidente-executivo da Semove, responsáveis por liderar e conduzir seus negócios/operações alinhados aos interesses legítimos, íntegros e lícitos da alta administração, respeitando seus valores organizacionais. Para esse fim, podem atuar em uma ou mais áreas de negócios no nível estratégico, tático ou operacional.

Operadora de dado pessoal: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador e de acordo com suas orientações.

Parente: refere-se aos parentes originários por vínculo sanguíneo ou adoção, tais como pai, mãe, filhos biológicos ou adotivos, irmãos e irmãs. Para mais detalhes, consulte a definição dos artigos 1.591 a 1.595 do Código Civil.

Parte interessada: é toda pessoa física ou pessoa jurídica envolvida, direta ou indiretamente, nos projetos, atividades, negócios e operações da Semove, tais como: colaboradores, gestores, agentes de governança, financiadores, fornecedores, conveniados, sindicatos de ônibus, permissionários e concessionários do transporte público do estado do Rio de Janeiro, controladas, coligadas, agentes intermediários, agentes públicos e equiparados, comunidades, governo, entidades de classe, organizações não governamentais, dentre outros.

Parte relacionada: é toda pessoa física ou pessoa jurídica que, direta ou indiretamente, por meio de um ou mais intermediários:

- a) controle ou exerça influência significativa no controle da Semove;
- b) seja controlada pela Semove;
- c) seja empreendimento sob o controle comum da Semove ou de sua controladora com outros sócios/acionistas;

d) seja coligada da Semove;

e) for um agente de governança, ou parente, ou aparentado por afinidade de agente de governança das empresas enquadradas nos itens (a), (b) e (c) acima, por ter condições de exercer influência significativa nas diretrizes de governança destas empresas;

f) for uma empresa de transporte público coletivo de passageiros, no modal ônibus, que firme instrumento contratual ou acordo com a Semove e/ou suas controladas, na qualidade de fornecedora, cliente, parceira ou conveniada (excetuadas as transações de mobilidade urbana ressarcidas às operadoras de transporte após processamento no sistema de bilhetagem eletrônica);

g) toda parte relacionada à Semove é considerada parte interessada, mas nem toda parte interessada é relacionada. Para mais detalhes, consultar o pronunciamento do CPC, nº 05 (R1)/2008 - Divulgação sobre Partes Relacionadas.

Período de retenção: período de armazenamento do dado pessoal.

Planejamento Estratégico de Segurança da Informação (PESI): é um conjunto estruturado de mecanismos preventivos, detectivos e corretivos que visam monitorar, de forma abrangente, a aderência da Semove às boas práticas de segurança da informação, à PSI e demais instrumentos normativos, contratuais ou legais em vigor. É um programa estratégico liderado pela Gerência de Segurança da Informação junto às áreas de negócios, que envolve ações focadas em capacitação e treinamento de usuários, aprimoramento da efetividade dos controles internos dos processos internos segundo as boas práticas de segurança da informação, gestão de incidente de segurança da informação e monitoramento de ameaças frente as vulnerabilidades sistêmicas ou em tecnologias projetadas para proteger os recursos tecnológicos corporativos contra ameaças ou incidentes de segurança da informação (decorrente ou não de crimes cibernéticos).

Pleito de alta complexidade: é o conjunto de demandas de clientes que desejam eliminar, anonimizar, pseudonimizar, fazer a portabilidade ou obter informações de confidencialidade restrita ou sigilosa acerca do tratamento de seus dados pessoais.

Pleito de baixa complexidade: é o conjunto de demandas de clientes que solicitam o acesso ou confirmação de existência de dados pessoais.

Política de Privacidade: é o documento, divulgado nos *websites* e aplicativos da Semove, que informa aos seus clientes, de forma clara e transparente, todos os direitos, obrigações e garantias do titular, formas de tratamento de dados pessoais, finalidade de coleta, prazo de retenção e demais requisitos da LGPD.

Presidente: é o líder máximo do Órgão Diretivo e contratado sob regime do Contrato Individual de Trabalho. Quando denominado **presidente-executivo**, significa que também possui atribuições previstas no contrato social da Semove, que se reporta diretamente ao CG e indiretamente à AGRS.

Privacidade desde a concepção (Privacy by design): é a metodologia baseada em assegurar a proteção e privacidade dos dados pessoais, desde a concepção de projetos ou definição de processos/atividades das áreas de negócios, para que estes se mantenham em conformidade com a LGPD.

Programa de Governança em Proteção de Dados e Privacidade: é um conjunto de mecanismos ou instrumentos, definidos pelo Gerente de Proteção de Dados, capaz de demonstrar a aderência, de forma abrangente, da Semove à LGPD, às boas práticas e demais instrumentos legais, contratuais ou normativos, que versem sobre a proteção e privacidade dos dados pessoais, em termos de processos, projetos, celebração de contratos, gestão de incidentes de segurança da informação e instrumentos normativos relativos à integridade e ao comprometimento do agente de tratamento de adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais. Nesse sentido, cabe destacar alguns processos e políticas importantes para a governança dos dados pessoais: mapeamento dos dados pessoais, política de privacidade e direito dos titulares, planos de resposta a incidentes, políticas e salvaguardas adotadas. Estas devem ser implementadas de acordo com um processo de avaliação sistemática de impactos e riscos à privacidade.

Programa de Integridade e Conformidade (PIC): conjunto de mecanismos e procedimentos internos baseado na aderência às leis, regulamentos e instrumentos normativos ou contratuais, com o objetivo de disseminar uma cultura baseada nos princípios e valores organizacionais, gestão integrada de riscos e melhoria dos controles internos.

Pseudonimização: é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Relatório de Avaliação do Legítimo Interesse (*Legitimate Interest Assessment* ou *LIA*): é o relatório que avalia a adequação do fluxo de tratamento de dados pessoais em legítimo interesse para fins de LGPD, evitando-se que seja utilizado de forma arbitrária e não fundamentada, sem uma ponderação dos interesses dos titulares de dados.

Relatório de Impacto à Proteção de Dados Pessoais (*Data Privacy Impact Assessment* ou *DPIA*): é o relatório que demonstra os processos de tratamento de dados pessoais e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e os direitos fundamentais do titular desses dados.

Recursos tecnológicos: são ativos e direitos tangíveis ou intangíveis, de natureza tecnológica, utilizados como meios de armazenamento, processamento, comunicação, transmissão de dados e/ou voz. Podem ser privados, corporativos ou de terceiros. Os recursos tecnológicos tangíveis possuem uma forma física, tais como: equipamentos, máquinas, *hardwares*, *notebooks*, computadores, *tablets*, aparelhos celulares, placas de rede, servidores ativos de conectividade etc. Os recursos tecnológicos intangíveis carecem de forma física, pois são ativos digitais, tais como: licenças de *softwares*, patentes, conhecimentos (*know-how*), direitos autorais de sistemas, rede ou outros tipos de propriedade intelectual.

Resíduo sólido: material, substância, objeto ou ativo descartado resultante de atividades humanas em sociedade, a cuja destinação final se procede, se propõe proceder ou se está obrigado a proceder, nos estados sólido ou semissólido, bem como gases contidos em recipientes e líquidos cujas particularidades tornem inviável o seu lançamento na rede pública de esgotos ou em corpos d'água, ou exijam para isso soluções técnica ou economicamente inviáveis em face da melhor tecnologia disponível.

Secretaria Nacional do Consumidor (Senacon): é um órgão que integra o Ministério da Justiça e Segurança Pública e atua, principalmente, no planejamento, elaboração, coordenação e execução da Política

Nacional das Relações de Consumo, com os objetivos de: (i) garantir a proteção e exercício dos direitos dos consumidores; (ii) promover a harmonização nas relações de consumo; (iii) incentivar a integração e a atuação conjunta dos membros do Sistema Nacional de Defesa do Consumidor (SNDC); e (iv) participar de organismos, fóruns, comissões ou comitês nacionais e internacionais que tratem da proteção e defesa do consumidor ou de assuntos de interesse dos consumidores.

Significativo(a): o termo refere-se, quando mensurável, a algo que tenha valor material em termos monetários ou a algum fato ou acontecimento relevante, capaz de influenciar a tomada de decisão pelo Órgão Diretivo ou instâncias superiores de governança da Semove com o propósito de proteger seus interesses legítimos e lícitos, preservando sua imagem, reputação e as diretrizes operacionais, táticas ou estratégicas dos seus negócios.

Sistemas analíticos: são sistemas responsáveis por correlacionar dados com o objetivo de gerar informação através de painéis com indicadores (*dashboards*), para auxiliar o processo de tomada de decisão.

Sistemas transacionais: são sistemas utilizados na operação, portanto possuem um conjunto de dados (quantitativos ou qualitativos) resultantes de suas atividades operacionais e comerciais.

Terceiro: toda pessoa física ou jurídica que mantenha relação direta ou indireta com a Semove. Trata-se de uma parte interessada ou relacionada.

Termo de Aceite: acordo assinado pelos colaboradores, gestores, diretores e presidente-executivo e demais partes interessadas ou relacionadas à Semove, pelo qual assumem, de forma livre, informada e inequívoca, o compromisso de conhecer e cumprir as diretrizes desta Política.

Titular: pessoa física proprietária do dado pessoal que é objeto de tratamento.

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro, ou organismo internacional do qual o país seja membro.

Tratamento de dados pessoais: conjunto de ações referentes à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, divulgação, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, transporte, difusão, cessão ou extração da informação. A informação pode ou não conter dados pessoais.

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

Usuário: é o indivíduo que possui autorização de acesso aos recursos tecnológicos para execução de suas atividades profissionais. O usuário pode ser categorizado como usuário interno, quando a credencial de acesso aos recursos tecnológicos tem domínio corporativo “@semove.org.br”, caso contrário, será categorizado como usuário externo.



semove