

## 1. Mensagem da Diretoria, Objetivo e Abrangência

A busca constante pela excelência e o compromisso ético na prestação de serviços de segurança exigem uma atuação pautada na legalidade e no respeito aos direitos fundamentais de todos os cidadãos. Sob a liderança do Coronel da Reserva da Polícia Militar do Estado de Mato Grosso, Eduardo Henrique de Souza, a **General Smart Segurança Privada e Terceirizações Ltda.** adota como premissa corporativa inegociável o conceito de segurança inteligente e planejada, em que oferecer inteligência antes do emprego de qualquer força é fundamental para entender e mitigar os riscos na medida exata das necessidades dos clientes. Esta filosofia operacional, que alinha a larga experiência em segurança pública aplicada à iniciativa privada com as melhores práticas de governança e integridade corporativa, determina que o tratamento de dados pessoais no âmbito de nossas atividades seja conduzido com o máximo rigor, transparência, segurança técnica e em absoluta conformidade com as normas legais vigentes no país.

A presente Política de Privacidade e Proteção de Dados Pessoais é o instrumento oficial de governança da **General Smart Segurança Privada e Terceirizações Ltda.**, estabelecido com o propósito de nortear todas as atividades corporativas que envolvam o tratamento de dados pessoais. O objetivo primordial deste documento é orientar os colaboradores da instituição, os parceiros tecnológicos e os prestadores de serviços terceirizados, além de informar aos clientes, visitantes, moradores de condomínios atendidos e usuários das áreas monitoradas acerca dos critérios e procedimentos adotados para a proteção de sua privacidade e intimidade. Ademais, esta política atua como um pilar essencial do nosso programa de compliance, sendo peça indispensável para os processos formais de auditoria, credenciamento e homologação rigorosa de fornecedores perante grandes organizações nacionais e internacionais, com destaque para a Petrobras, instituições financeiras, cooperativas de crédito e órgãos governamentais de elevado nível de governança corporativa.

A abrangência deste regulamento interno é total e imperativa, aplicando-se obrigatoriamente a todos os sócios, diretores, administradores, gestores, colaboradores administrativos e, com especial relevo, a todos os profissionais que atuam nas atividades operacionais de campo, tais como vigilantes, porteiros, zeladores, auxiliares de manutenção e conservação, fiscais de ronda e operadores de monitoramento da central de controle. Igualmente, as diretrizes aqui consolidadas vinculam contratualmente todos os prestadores de serviços autônomos, fornecedores de tecnologia, integradores de sistemas de segurança e

parceiros de negócios que venham a ter acesso, de forma direta ou indireta, a dados pessoais mantidos sob a custódia ou responsabilidade da empresa, cabendo à coordenação corporativa fiscalizar seu fiel cumprimento.

## **2. Princípios e Definições de Proteção de Dados**

A correta aplicação das diretrizes de privacidade pressupõe o domínio preciso dos conceitos jurídicos instituídos pela legislação nacional de proteção de dados pessoais, notadamente a Lei Geral de Proteção de Dados, Lei Federal nº 13.709/2018. Para os fins desta política corporativa, considera-se dado pessoal toda e qualquer informação relacionada a uma pessoa física identificada ou identificável, o que abrange desde dados cadastrais simples até identificadores eletrônicos e registros de fluxo de movimentação. O dado pessoal sensível consiste em informações que exigem maior grau de proteção por estarem associadas a aspectos íntimos e suscetíveis a discriminações, abrangendo origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, bem como dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

O titular dos dados pessoais é a pessoa física a quem se referem as informações objeto de tratamento, tais como colaboradores, candidatos a postos de trabalho, prestadores de serviços, clientes, moradores e visitantes de perímetros protegidos. O tratamento compreende toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. O controlador, figura exercida precipuamente pela **General Smart Segurança Privada e Terceirizações Ltda.** em suas relações corporativas, é a pessoa jurídica a quem competem as decisões referentes ao tratamento de dados, ao passo que o operador é quem realiza as atividades de tratamento em nome e sob as orientações do controlador. O Encarregado pelo Tratamento de Dados Pessoais, também denominado Data Protection Officer, é o profissional indicado pela empresa para atuar como canal de comunicação entre a organização, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. Por fim, o incidente de segurança constitui qualquer evento confirmado ou sob suspeita fundamentada que resulte em acesso não autorizado, destruição, perda, alteração ou difusão indevida de dados pessoais sob controle da companhia.

As atividades operacionais de tratamento de dados desenvolvidas pela organização encontram-se estritamente subordinadas aos princípios gerais de proteção de dados estabelecidos na legislação nacional, com foco primordial na eficiência e conformidade dos serviços sob medida prestados pela instituição. O princípio da finalidade determina que o tratamento seja realizado somente para propósitos legítimos, específicos e previamente informados aos titulares, sendo vedado qualquer desvio posterior para fins incompatíveis. O princípio da adequação garante a estrita compatibilidade entre o tratamento executado e os objetivos comunicados ao cidadão, enquanto o princípio da necessidade impõe que o volume de dados tratados seja limitado ao mínimo indispensável para o alcance das finalidades pretendidas, evitando coletas excessivas ou desproporcionais.

Em acréscimo, os princípios do livre acesso e da qualidade dos dados asseguram aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento de suas informações, bem como a exatidão, clareza e atualização dos dados sob custódia da empresa. O princípio da transparência garante a prestação de informações claras, precisas e facilmente acessíveis sobre os agentes de tratamento e os fluxos de dados, respeitados os segredos comerciais e industriais da prestadora de segurança. A segurança e a prevenção são pilares práticos e fundamentais de nossa atuação, materializados na adoção de medidas técnicas e administrativas avançadas para proteger os dados pessoais de acessos não autorizados ou incidentes danosos, agindo de forma proativa para mitigar riscos inerentes à atividade de vigilância física e eletrônica. Finalmente, os princípios da não discriminação e da responsabilização e prestação de contas vedam qualquer tratamento para fins discriminatórios ilícitos ou abusivos, impondo à empresa o dever de manter registros detalhados de suas operações e demonstrar a eficácia de suas medidas de conformidade legal de modo contínuo.

### **3. Dados Pessoais Tratados e Finalidades do Tratamento**

No desempenho de suas funções especializadas de segurança privada, vigilância patrimonial, portaria, controle de acessos, monitoramento eletrônico e terceirização de mão de obra qualificada, a **General Smart Segurança Privada e Terceirizações Ltda.** realiza o processamento de variadas categorias de dados pessoais, estruturadas sob critérios de absoluta necessidade e estrita aderência ao objeto das relações contratuais vigentes. Em relação aos colaboradores contratados sob regime trabalhista e prepostos da empresa, os dados tratados abrangem informações qualificativas e cadastrais, tais como nome completo, filiação, números de documentos de identificação civil (RG, CPF e carteira profissional), dados de contato

residencial, estado civil, histórico profissional, registros acadêmicos, dados financeiros para processamento de pagamentos, além de exames de saúde ocupacional indispensáveis para a comprovação da aptidão laborativa exigida na atividade de vigilância armada e operacional. De igual forma, no âmbito dos processos seletivos para novas vagas, são coletados currículos profissionais, registros de experiências anteriores e certidões de antecedentes civis e criminais de candidatos, cuja análise técnica é indispensável para preencher os rigorosos requisitos de idoneidade inerentes ao setor de segurança privada.

Quanto aos clientes, fornecedores de tecnologia e parceiros comerciais corporativos, o tratamento alcança as informações dos representantes legais, prepostos e pontos de contato indicados nos respectivos instrumentos de contrato, incluindo nome completo, cargo, CPF, endereço eletrônico e telefones profissionais, dados estes indispensáveis para a regular gestão administrativa, faturamento de mensalidades, prestação de suporte e fiscalização contratual comum. No tocante aos moradores, inquilinos, visitantes e prestadores de serviços temporários que ingressam ou transitam nos condomínios horizontais, condomínios verticais, sedes de indústrias, agências bancárias ou áreas de mineração sob a proteção contratual da empresa, as informações coletadas incluem registros cadastrais básicos, documentos de identidade oficial apresentados nas portarias, placas de veículos, registros eletrônicos de datas e horários de entrada e saída, além de identificadores biométricos e registros de imagem facial nos locais equipados com sistemas inteligentes de controle de acesso por reconhecimento facial de alta eficiência.

As imagens captadas por meio de câmeras e circuitos fechados de televisão (CFTV) instalados nos perímetros protegidos e áreas comuns constituem categoria de dado pessoal de alta relevância sob a custódia operacional da organização, englobando aspectos biométricos e comportamentais dos indivíduos que ali circulam. O tratamento de todas estas categorias de dados atende a finalidades específicas e estritamente delimitadas pela atividade de proteção de vidas e patrimônios. O controle de acesso a portarias e o livro de ocorrências digital destinam-se a impedir a intrusão de pessoas não autorizadas e a assegurar o registro rastreável de acessos nos ambientes protegidos, de modo a resguardar a coletividade e o patrimônio privado. O monitoramento eletrônico por sensores, alarmes e câmeras de segurança de alta tecnologia, gerido por nossas equipes qualificadas e centrais de monitoramento automatizadas, busca identificar em tempo real incidentes, sinistros, arrombamentos ou ameaças à integridade física das pessoas e à inviolabilidade dos edifícios monitorados.

Na esfera dos recursos humanos e do departamento de pessoal, o tratamento de dados visa a garantir o cumprimento do contrato de trabalho, o processamento correto de salários, o recolhimento de tributos federais, o cumprimento de normas de medicina e segurança do trabalho, bem como a fiscalização interna e o treinamento contínuo das equipes em conformidade com o Procedimento Operacional Padrão da organização. Em todas as hipóteses referidas, a atuação da empresa restringe-se às finalidades anunciadas, sendo vedada a utilização das informações para propósitos de enriquecimento de bases de dados externas, marketing invasivo, compartilhamento comercial não autorizado ou qualquer atividade incompatível com a proteção dos direitos fundamentais e das legítimas expectativas dos titulares de dados pessoais.

#### **4. Bases Legais Utilizadas para o Tratamento de Dados**

A conformidade regulatória da **General Smart Segurança Privada e Terceirizações Ltda.** com os preceitos da Lei Geral de Proteção de Dados Pessoais exige que toda e qualquer atividade de tratamento esteja indissociavelmente vinculada a uma das hipóteses de legitimação expressamente autorizadas pelo ordenamento jurídico brasileiro. Para os fluxos de dados relacionados aos nossos colaboradores, prestadores de serviços contratados e clientes corporativos, o tratamento é legitimado pela base legal da execução de contratos ou de procedimentos preliminares relacionados a contratos dos quais o titular seja parte, bem como pela necessidade de cumprimento de obrigação legal ou regulatória pelo controlador, com especial relevo para as obrigações acessórias de natureza trabalhista, previdenciária e tributária, além das rigorosas exigências de fiscalização estipuladas pela Polícia Federal para as empresas prestadoras de segurança privada armada.

Nas operações táticas e preventivas de vigilância patrimonial, rondas móveis, fiscalização operacional, monitoramento eletrônico e controle de acessos em ambientes de terceiros, a base legal prioritária utilizada para amparar o tratamento de dados pessoais e imagens reside na hipótese do legítimo interesse do controlador ou de terceiros, bem como no exercício regular de direitos em contratos e processos judiciais ou administrativos, quando houver necessidade de preservar acervos probatórios face a eventuais incidentes ou ilícitos civis e penais. O recurso ao legítimo interesse fundamenta-se na proteção da segurança das instalações vigiadas, na incolumidade física de moradores, colaboradores, visitantes e usuários em geral, bem como na integridade dos bens móveis e imóveis confiados contratualmente à proteção da empresa, respeitando-se as legítimas expectativas e salvaguardando-se os direitos

e liberdades fundamentais do cidadão comum. O permissivo legal que fundamenta o recurso ao legítimo interesse do controlador está esculpido no diploma nacional de proteção de dados:

Art. 7, inciso IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

A ponderação cuidadosa dos interesses da organização em face dos direitos individuais do titular de dados pessoais orienta a elaboração dos nossos relatórios de impacto de privacidade. A empresa atesta que a captação e o processamento de tais registros de segurança não sobrecarregam de maneira desproporcional os direitos dos indivíduos, porquanto os dados coletados limitam-se ao mínimo estritamente indispensável para a manutenção da segurança comum e prevenção ativa de riscos, mantendo-se em ambiente de absoluto sigilo e restrição técnica de acesso. A base legal do exercício regular de direitos, por sua vez, protege o direito do titular à preservação de garantias individuais ao mesmo tempo em que legitima o arquivamento técnico de dados de fluxo de segurança de modo a aparelhar defesas jurídicas ou instruir demandas processuais legítimas de nossos contratantes e da própria organização, conforme estipulado expressamente no texto legal:

Art. 10, inciso II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

O entendimento jurisprudencial consolidado chancela de forma inequívoca o enquadramento dessas atividades de segurança à hipótese do legítimo interesse e do exercício regular de direito, atestando a plena legalidade de tratamentos de dados que visem à segurança coletiva e ao dever de informação em ambientes controlados, desde que resguardados a transparência operacional, o livre acesso do titular às informações e o fornecimento de canais adequados para o eventual exercício do direito de oposição, sem que se faça necessária a obtenção de consentimento formal individualizado em cada ato de controle de perímetro. Em acórdão recente que versou sobre a dispensa de consentimento específico e a conformidade do tratamento informacional amparado na hipótese legal do legítimo interesse do controlador em face dos princípios da transparência, a Quarta Câmara de Direito Privado do Tribunal de Justiça de Mato Grosso fixou a seguinte tese jurídica em julgamento de relatoria da Desembargadora Serly Marcondes Alves:

EMENTA: DIREITO DIGITAL E PROTEÇÃO DE DADOS. AGRAVO DE INSTRUMENTO. UTILIZAÇÃO DE DADOS PESSOAIS DE USUÁRIOS PARA TREINAMENTO DE INTELIGÊNCIA ARTIFICIAL GENERATIVA. ALEGADA VIOLAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS. INEXISTÊNCIA DE INDÍCIOS ROBUSTOS DE

ILEGALIDADE OU ABUSIVIDADE. RECURSO DESPROVIDO. I. CASO EM EXAME Agravo de instrumento interposto pela Associação de Defesa de Direitos Digitais (ADDD) contra decisão que indeferiu tutela cautelar para suspender a utilização de dados pessoais de usuários da rede social X (antiga Twitter) no treinamento do modelo de inteligência artificial generativa "Grok". A agravante sustenta que a empresa X Brasil Internet Ltda. alterou sua política de privacidade para permitir tal uso sem consentimento prévio e informado dos usuários, violando a Lei Geral de Proteção de Dados (LGPD). Requer a concessão da tutela para impedir o tratamento dos dados sem novo consentimento específico. II. QUESTÃO EM DISCUSSÃO A questão em discussão consiste em determinar se a agravada utiliza indevidamente dados pessoais dos usuários para treinar modelos de inteligência artificial, sem consentimento específico e em violação aos princípios da transparência e do dever de informação previstos na LGPD. III. RAZÕES DE DECIDIR O art. 7º da LGPD permite o tratamento de dados pessoais não apenas com base no consentimento, mas também em outras hipóteses legais, como o legítimo interesse do controlador, invocado pela agravada. A agravada demonstrou que informou os usuários sobre a nova finalidade do tratamento de dados por meio da política de privacidade, notificações e páginas da central de ajuda. A opção de oposição ao tratamento foi disponibilizada aos usuários por meio de mecanismo acessível e de fácil utilização, descaracterizando a alegação de impossibilidade de recusa. Não há indícios robustos de ocultação intencional de informações ou prática comercial desleal por parte da agravada. A Autoridade Nacional de Proteção de Dados (ANPD) analisou o caso e, até o momento, não identificou irregularidades na conduta da empresa. Decisão de tribunal estrangeiro sobre o uso de dados na União Europeia não vincula a jurisdição brasileira e não comprova ilegalidade do tratamento realizado no Brasil. O julgamento do mérito prejudica o Agravo Interno interposto pela agravante. IV. DISPOSITIVO E TESE Recurso desprovido. Tese de julgamento: O tratamento de dados pessoais pode ocorrer sem consentimento específico quando baseado em hipóteses legais previstas na LGPD, como o legítimo interesse do controlador, desde que observados os princípios da transparência e do direito de oposição do titular. A disponibilização de informações claras e acessíveis ao titular, bem como a existência de mecanismo efetivo de oposição ao tratamento, afastam a alegação de violação ao dever de informação. Decisões de tribunais estrangeiros não vinculam a jurisdição brasileira e não comprovam, por si só, a ilegalidade do tratamento de dados sob a legislação nacional. Dispositivos relevantes citados: LGPD, arts. 7º e 305; CPC, art. 305. (N.U 1034362-91.2024.8.11.0000, CÂMARAS ISOLADAS CÍVEIS DE DIREITO PRIVADO, SERLY MARCONDES ALVES, Quarta Câmara de Direito Privado, Julgado em 02/05/2025, Publicado no DJE 02/05/2025)

Adicionalmente, nas atividades específicas de monitoramento de condomínios residenciais e comerciais, a jurisprudência pátria reconhece que o registro de acessos e imagens de segurança comuns não configura ato ilícito ou violação abusiva ao direito de imagem, constituindo estrito exercício regular de direito e dever de administração em prol do bem comum, de modo que a ausência de consentimento não induz a qualquer dever reparatório civil se observados os propósitos puramente informativos e técnicos do monitoramento, sem exposição vexatória dos usuários. Em julgamento versando sobre a utilização e compartilhamento técnico restrito de imagens captadas por CFTV para fins informativos e de segurança coletiva em ambiente condominial, a Quarta Câmara de Direito Privado do Tribunal de Justiça de Mato Grosso firmou idêntico entendimento, nos termos do julgado relatado pelo Desembargador Rubens de Oliveira Santos Filho:

EMENTA: APELAÇÃO CÍVEL. AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS. DIREITO À IMAGEM DE MENOR. COMPARTILHAMENTO DE IMAGEM CAPTADA POR CFTV EM GRUPO DE MORADORES. FINALIDADE INFORMATIVA E DE SEGURANÇA. INCIDENTE EM ELEVADOR. AUSÊNCIA DE CONTEÚDO OFENSIVO OU VEXATÓRIO. INEXISTÊNCIA DE ATO ILÍCITO OU DANO MORAL. EXERCÍCIO REGULAR DE DIREITO PELA ADMINISTRAÇÃO CONDOMINIAL. SENTENÇA MANTIDA. RECURSO NÃO PROVIDO. I. CASO EM EXAME Apelação cível interposta contra sentença que julgou improcedente pedido de indenização por danos morais formulado por menor de idade, em razão da divulgação de vídeo de câmeras de segurança de condomínio em grupo de mensagens de moradores. O vídeo registrou um incidente técnico no elevador envolvendo o apelante e seus genitores, tendo sido compartilhado pelo subsíndico para fins de esclarecimento técnico sobre o uso do equipamento. II. QUESTÃO EM DISCUSSÃO A questão em discussão consiste em determinar se a divulgação de imagem de menor de idade, captada por sistema de segurança e compartilhada em ambiente restrito de moradores para fins informativos e de segurança coletiva, configura ato ilícito e dano moral presumido, ante a ausência de consentimento específico previsto na LGPD e no ECA. III. RAZÕES DE DECIDIR O direito à imagem, embora constitucionalmente protegido, deve ser ponderado com o legítimo interesse da coletividade e o dever de informação técnica da administração condominial acerca da segurança de áreas e equipamentos comuns. A divulgação ocorrida em grupo restrito de moradores, acompanhada de mensagem de teor neutro e técnico, sem cunho vexatório, comercial ou discriminatório, não caracteriza abuso de direito ou violação à dignidade da criança. Segundo a orientação do Superior Tribunal de Justiça (REsp 1.893.877/SC), a responsabilidade civil por dano à imagem em contextos informativos pressupõe a demonstração de circunstâncias capazes de atingir a honra ou a dignidade, o que não se verifica quando a imagem é acessória a um fato de interesse comum. A ausência de consentimento formal previsto na LGPD não induz, por si só, ao dever de indenizar se o tratamento do dado (imagem) ocorreu para a proteção da segurança e no exercício regular de gestão do condomínio, sem exposição pública ou humilhante. IV. DISPOSITIVO E TESE Recurso não provido. Tese de julgamento: A divulgação de imagem de menor captada por CFTV, realizada em ambiente restrito de condomínio com finalidade exclusivamente informativa e técnica sobre segurança comum, sem conteúdo ofensivo ou comercial, não configura ato ilícito nem dano moral in re ipsa. (N.U 1020318-41.2024.8.11.0041, CÂMARAS ISOLADAS CÍVEIS DE DIREITO PRIVADO, RUBENS DE OLIVEIRA SANTOS FILHO, Quarta Câmara de Direito Privado, Julgado em 20/05/2026, Publicado no DJE 26/05/2026)

## 5. Tratamento de Imagens e Sistemas de CFTV

O monitoramento eletrônico por meio de sistemas de câmeras e circuitos fechados de televisão (CFTV) de última geração representa um dos vetores essenciais na estrutura de inteligência operacional empregada pela **General Smart Segurança Privada e Terceirizações Ltda.** para garantir a segurança integral de condomínios residenciais, comerciais, agências financeiras, estabelecimentos industriais, perímetros rurais e grandes eventos sob nossa responsabilidade técnica. A operação de captação, transmissão, processamento, visualização em tempo real e armazenamento dessas imagens é conduzida de forma técnica e responsável, restrita única e exclusivamente à consecução das finalidades de segurança patrimonial, controle físico de perímetros, prevenção contra intrusões ilegais, proteção da vida das pessoas e



instrução de eventuais procedimentos administrativos ou judiciais de apuração de ilícitos comuns.

A instalação dos equipamentos ópticos e o posicionamento das câmeras de CFTV nas dependências vigiadas obedecem a rigorosos padrões éticos e técnicos, sendo absolutamente proibida a inserção de câmeras em ambientes de legítima expectativa de privacidade individual dos cidadãos, tais como o interior de sanitários públicos ou privativos, vestiários, refeitórios, salas de descanso de funcionários, ambientes privativos de moradia ou quaisquer locais assemelhados. A captação de imagens dar-se-á sempre de modo ostensivo, com a devida e clara sinalização dos perímetros monitorados por meio de avisos e placas visuais informativas, assegurando-se ampla transparência sobre a existência do sistema de monitoramento eletrônico e permitindo que qualquer titular de dados que ingresse no ambiente esteja plenamente consciente do tratamento de suas imagens faciais e comportamentais para fins de segurança.

A preservação das imagens captadas no âmbito operacional ocorre de forma segura e com restrições severas de acesso, sendo vedada qualquer utilização recreativa, compartilhamento recreativo, exposição indevida ou destinação comercial dos arquivos. Os operadores de monitoramento e vigilantes encarregados de visualizar os painéis táticos de controle de câmeras atuam sob rigorosos deveres contratuais de sigilo profissional e confidencialidade, sendo as ações de exportação, cópia ou extração de mídias de vídeo registradas eletronicamente por meio de auditoria de sistema para prevenir desvios de finalidade e vazamentos indesejados de dados pessoais. Os registros de vídeo que não contenham ocorrências anômalas ou incidentes de segurança são submetidos a ciclos de expiração automática e descarte definitivo nos prazos estipulados por esta política.

Caso ocorra algum incidente de segurança, crime, colisão de veículos, invasão perimetral ou descumprimento de normas regulamentares registrado pelas câmeras, o respectivo trecho da gravação será extraído de forma justificada pela equipe de segurança cibernética e armazenado em ambiente digital isolado e criptografado para servir como evidência material idônea. No que concerne à transferência ou fornecimento destas gravações de imagem a terceiros, a corporação adota postura extremamente rígida e defensiva do direito de privacidade do cidadão comum, viabilizando o compartilhamento apenas mediante a apresentação de ordem judicial específica, de requisição formal e fundamentada subscrita por autoridade policial em sede de inquérito criminal, ou em virtude do regular exercício de direito processual de colaboração na produção de provas. O Tribunal de Justiça de Mato Grosso, ao

julgar questões alusivas ao dever processual de exibição de registros eletrônicos e documentação de fluxo face às alegações de sigilo fundadas na LGPD, manifestou de forma cristalina que a legislação de proteção de dados não atua como bloqueio artificial para deveres de colaboração processual ou obrigações operacionais legítimas de exibição, conforme julgado proferido pela Quinta Câmara de Direito Privado sob a relatoria do Desembargador Luiz Octavio Oliveira Saboia Ribeiro:

EMENTA: DIREITO PROCESSUAL CIVIL E DIREITO DO CONSUMIDOR. EMBARGOS DE DECLARAÇÃO EM AGRAVO DE INSTRUMENTO. PLATAFORMA DE APOSTAS DIGITAIS. EXIBIÇÃO DE DOCUMENTOS. ALEGAÇÃO DE OMISSÃO QUANTO À POSSE DOS DOCUMENTOS, AUTONOMIA DAS PESSOAS JURÍDICAS, REGIME REGULATÓRIO E LGPD. INEXISTÊNCIA DE VÍCIOS DO ART. 1022 DO CPC. INCONFORMISMO. PREQUESTIONAMENTO. EMBARGOS REJEITADOS. I. Caso em exame 1. Embargos de declaração opostos em face de acórdão que, à unanimidade, negou provimento a agravo de instrumento, mantendo decisão que determinou a apresentação integral de documentos relacionados à conta da embargada em plataforma de apostas digitais, nos autos de Ação de Obrigação de Fazer c/c Indenização por Danos Morais. A embargante aponta omissões quanto aos arts. 396 e 400 do CPC, ao art. 49-A do Código Civil, à Lei nº 14.790/2023 e à aplicação da LGPD, além de buscar prequestionamento. II. Questão em discussão 2. Há quatro questões em discussão: (i) saber se o acórdão foi omisso quanto ao requisito de posse ou disponibilidade jurídica dos documentos, nos termos dos arts. 396 e 400 do CPC; (ii) saber se houve omissão quanto à autonomia patrimonial das pessoas jurídicas prevista no art. 49-A do Código Civil; (iii) saber se o acórdão deveria ter analisado o regime jurídico da Lei nº 14.790/2023 sobre apostas de quota fixa; e (iv) saber se houve omissão quanto à aplicação da LGPD e à delimitação objetiva da ordem de exibição. III. Razões de decidir 3. O acórdão embargado enfrentou expressamente a questão da disponibilidade dos documentos, adotando interpretação contextualizada dos arts. 396 e 400 do CPC ao reconhecer que, em plataformas digitais, a disponibilidade de dados abrange a capacidade técnica de acesso ou recuperação de informações utilizadas operacionalmente pela empresa, não se restringindo à posse formal. A divergência da embargante quanto à interpretação conferida não configura omissão. 4. A autonomia patrimonial entre pessoas jurídicas foi objeto de análise expressa no acórdão, que distinguiu o plano da separação patrimonial societária do plano da efetividade da instrução probatória, concluindo que a continuidade operacional da relação de consumo impede a utilização de reorganização societária como barreira artificial à produção de prova. 5. Não configura omissão a ausência de manifestação sobre norma que não se revela determinante para a solução da controvérsia. A matéria devolvida ao Tribunal versava sobre questão processual relativa à disponibilidade informacional para exibição de documentos, sendo que o regime regulatório da Lei nº 14.790/2023 não tem o condão de afastar o dever processual de colaboração na produção da prova. 6. O acórdão tratou expressamente da LGPD, consignando que a lei autoriza o tratamento de dados para cumprimento de obrigação legal e exercício regular de direitos em processo judicial, além de assegurar ao titular o direito de acesso aos seus próprios dados. A delimitação da ordem de exibição foi especificada em rol de nove itens, com ressalva para demonstração de impossibilidade técnica concreta. 7. A finalidade de prequestionamento não dispensa a demonstração dos vícios previstos no art. 1.022 do CPC. Havendo o acórdão apreciado efetivamente todas as questões jurídicas suscitadas, a mera indicação de dispositivos legais não caracteriza omissão a ser suprida pela via dos embargos declaratórios. IV. Dispositivo e tese 8. Embargos de declaração conhecidos e rejeitados. Tese de julgamento: "1. Não configura omissão a adoção de interpretação contextualizada dos arts. 396 e 400 do CPC que reconhece, em plataformas digitais, a disponibilidade

de dados como capacidade técnica de acesso ou recuperação de informações utilizadas operacionalmente pela empresa. 2. A ausência de manifestação sobre norma regulatória não determinante para a solução da controvérsia processual não constitui vício sanável por embargos de declaração. 3. A finalidade de prequestionamento não autoriza o acolhimento de embargos declaratórios quando ausentes os vícios do art. 1.022 do CPC." Dispositivos relevantes citados: CPC, arts. 396, 400 e 1.022; CC, art. 49-A; Lei nº 13.709/2018 (LGPD), arts. 7º, II e VI, e 18, II; Lei nº 14.790/2023. Jurisprudência relevante citada: TJMT, Embargos de Declaração em Apelação Cível n. 1032165-11.2022.8.11.0041, Rel. Des. Marcos Regenold Fernandes, Quinta Câmara de Direito Privado, j. 16/09/2025; Súmula nº 98/STJ. (N.U 1009104-11.2026.8.11.0000, CÂMARAS ISOLADAS CÍVEIS DE DIREITO PRIVADO, LUIZ OCTAVIO OLIVEIRA SABOIA RIBEIRO, Quinta Câmara de Direito Privado, Julgado em 05/05/2026, Publicado no DJE 12/05/2026)

## **6. Controle de Acesso e Registros de Visitantes**

A segurança das instalações sob a responsabilidade operacional da organização fundamenta-se na excelência técnica e na aplicação rigorosa de controles de acesso físico e eletrônico. O procedimento de identificação e cadastramento de visitantes e de prestadores de serviços temporários nas portarias de condomínios residenciais, comerciais, indústrias e órgãos públicos constitui a primeira linha de defesa contra sinistros e intrusões ilícitas. Ao ingressar nas áreas protegidas, o indivíduo é submetido à triagem em que os profissionais de portaria devidamente instruídos realizam a coleta de dados qualificativos, exigindo a apresentação de documentos de identificação oficiais e registrando a finalidade específica do acesso, o destino pretendido e a indicação do morador ou preposto responsável pela autorização de entrada.

Além do cadastro qualificativo e documental básico, o controle operacional engloba a gestão das correspondências recebidas e o registro sistemático de todas as anormalidades e ocorrências identificadas na rotina de vigilância. A empresa utiliza ferramentas de tecnologia para a automatização desses fluxos operacionais, assegurando que o recebimento de encomendas e as notificações de entregas sejam lançados de forma digital no livro de ocorrências da portaria, o que mitiga sensivelmente a possibilidade de erros e fraudes operacionais, além de manter o histórico de acessos plenamente rastreável para fins de auditoria de segurança e controle interno de qualidade. O processamento eletrônico dessas rotinas operacionais obedece ao princípio da necessidade, restringindo-se as informações ao mínimo indispensável para conferir efetividade e rapidez à guarda e à distribuição de encomendas, sem retenção desproporcional de registros por prazos indefinidos.

Na vertente do desenvolvimento tecnológico voltado à eficácia protetiva, a organização implementa sistemas de controle de acessos integrados com tecnologia inovadora de reconhecimento facial de alta eficiência, em parceria estratégica com as empresas de

tecnologia H3 Tecnologia e SafeBras. O tratamento de dados biométricos faciais, classificados como dados sensíveis pela legislação nacional de proteção de dados, ocorre sob rígido protocolo de governança corporativa e segurança cibernética. A captação biométrica destina-se exclusivamente à identificação precisa e instantânea de moradores, colaboradores internos e prestadores frequentes autorizados a transitar pelos perímetros protegidos, mitigando de forma definitiva o risco de acessos não autorizados mediante fraudes documentais ou falsidade ideológica nas portarias de controle.

A segurança dos bancos de dados que abrigam as biometrias faciais dos usuários é garantida por meio do emprego de técnicas avançadas de criptografia na origem e na transmissão de dados. Os modelos matemáticos gerados a partir do mapeamento dos pontos faciais dos titulares não são associados de forma direta ou desprotegida a dados cadastrais em ambientes públicos de rede, impedindo que acessos ilícitos possam expor os dados biométricos de maneira inteligível ou prejudicial à privacidade dos cidadãos. Todo o ecossistema tecnológico empregado na portaria e no controle perimetral foi desenvolvido em consonância com as exigências de confidencialidade da Lei Geral de Proteção de Dados, conciliando a rapidez indispensável para o fluxo de moradores e prestadores com a inviolabilidade exigida para os bancos de dados corporativos sob a nossa custódia operacional.

## **7. Direitos dos Titulares dos Dados e Canal de Atendimento (DPO)**

A proteção de dados pessoais sob a guarda da corporação estende-se para além das medidas de segurança técnica, englobando a garantia plena e efetiva do exercício dos direitos previstos em benefício dos cidadãos pela Lei Geral de Proteção de Dados. A organização disponibiliza aos seus colaboradores, parceiros de negócios, clientes, moradores, visitantes e usuários de ambientes monitorados mecanismos céleres e simplificados para que possam, a qualquer momento e mediante requisição formal, exercer as prerrogativas asseguradas pelo artigo 18 do diploma nacional de privacidade. Dentre os direitos fundamentais garantidos pela instituição, destaca-se a faculdade de requerer a confirmação da existência de operações de tratamento e o subsequente acesso simplificado aos respectivos registros, permitindo ao cidadão conhecer detalhadamente quais informações pessoais estão sob a guarda da empresa.

Os titulares também possuem o direito de solicitar a imediata correção de dados incompletos, inexatos ou manifestamente desatualizados mantidos em nossos cadastros de portaria e registros trabalhistas, o que se revela fundamental para assegurar a higidez operacional e evitar equívocos no controle de acessos. Do mesmo modo, é assegurado ao titular

o direito de requerer a anonimização, o bloqueio ou a eliminação de dados pessoais que se mostrarem desnecessários, excessivos ou tratados em desconformidade com a legislação federal, além da portabilidade de suas informações a outro fornecedor de serviços de segurança e da revogação expressa do consentimento outorgado para fins específicos, ressalvadas as hipóteses em que a manutenção e o armazenamento seguro dos dados sejam obrigatórios para o cumprimento de obrigações contratuais, legais ou regulatórias pelo controlador.

Para viabilizar o acolhimento, a triagem e o atendimento tempestivo de todas as demandas e esclarecimentos de dúvidas formulados pelos titulares de dados pessoais, a corporação institui e divulga de forma ampla o seu Canal de Atendimento ao Titular. O contato formal e simplificado com o Encarregado pelo Tratamento de Dados Pessoais, também denominado DPO, deve ser realizado por intermédio do endereço eletrônico institucional [contato@generalsmart.com.br](mailto:contato@generalsmart.com.br), ou alternativamente pelos telefones de suporte técnico (65) 3052-8141 e (65) 99638-2185. O canal atua de forma centralizada e independente para receber petições, sugestões, reclamações e requerimentos de direitos apresentados pelos titulares de dados.

O Encarregado pelo Tratamento de Dados Pessoais da instituição tem o dever profissional de analisar cada requisição recebida sob a ótica dos preceitos legais e técnicos aplicáveis. Havendo a solicitação de acesso a gravações de imagens de CFTV ou logs de registros de portaria, o Encarregado avaliará a viabilidade técnica e a necessidade de resguardar a privacidade e os dados pessoais de terceiros eventualmente presentes nas mídias, procedendo, quando viável, à edição das imagens de modo a isolar apenas os dados pessoais pertencentes ao próprio requerente. As respostas formais serão direcionadas ao titular no prazo legal estipulado pela autoridade nacional, registrando-se internamente todas as etapas do processo de atendimento para fins de fiscalização e auditoria de conformidade.

## **8. Compartilhamento de Dados com Terceiros**

O tratamento de dados pessoais no ecossistema da organização pauta-se pelo princípio da estrita confidencialidade, de modo que o compartilhamento e a transferência de informações com terceiros ocorrem unicamente sob critérios rigorosos de segurança e legitimidade operacional, limitando-se aos propósitos indispensáveis de faturamento, gestão de contratos, conformidade regulatória e segurança física comum. No âmbito da prestação dos serviços especializados contratados por nossos clientes corporativos, órgãos públicos, condomínios residenciais e empresariais, como prefeituras, grandes cooperativas de crédito e

indústrias de renome de Mato Grosso, o compartilhamento restringe-se ao repasse de relatórios de fluxo de entradas e saídas de visitantes e prepostos, registros biométricos de moradores e mídias de vídeo específicas necessárias para as auditorias internas de segurança dos próprios contratantes.

O tráfego dessas informações pessoais com os clientes tomadores de serviços é efetuado por meio de plataformas eletrônicas dedicadas, dotadas de ferramentas avançadas de autenticação em dois fatores e criptografia na transmissão, o que obsta a interceptação ou a visualização indevida dos dados por indivíduos não autorizados. Fica expressamente vedado o fornecimento de acessos irrestritos e desregulados aos bancos de dados de controle de acesso ou de monitoramento por câmeras para pessoas alheias às equipes táticas de segurança e de tecnologia da General Smart, preservando-se a higidez e a custódia responsável dos dados pessoais coletados nas áreas de vigilância patrimonial e portaria digital.

No relacionamento com nossos parceiros de negócios e fornecedores de tecnologia, com destaque para a H3 Tecnologia e a SafeBras, a empresa adota idêntica rigidez regulatória. Estes integradores atuam na condição de operadores de dados pessoais em nome e sob as ordens estritas da nossa corporação, desempenhando funções de infraestrutura de software de portaria inteligente, armazenamento em nuvem de filmagens, gerenciamento de alarmes e controle de sensores biométricos de acesso. A formalização de qualquer parceria tecnológica está condicionada à assinatura prévia de termos de confidencialidade adicionais e de cláusulas de conformidade com a Lei Geral de Proteção de Dados, as quais estabelecem obrigações de segurança cibernética simétricas às adotadas internamente por nossa organização.

As diretrizes vigentes proíbem terminantemente qualquer utilização de dados pessoais ou sensíveis sob nossa responsabilidade para finalidades comerciais diversas, publicidade dirigida, monetização de dados ou repasse a terceiros com o fito de marketing ou formação de perfis de consumo. Nossos parceiros tecnológicos estão contratualmente impedidos de reutilizar as informações tratadas para benefício próprio ou de terceiros sob pena de rescisão contratual imediata e aplicação de sanções indenizatórias civis cabíveis. O fluxo de compartilhamento externo de dados opera-se sob o absoluto controle de nossa central de tecnologia, visando de modo exclusivo a eficiência de um serviço sob medida e a total segurança e tranquilidade dos usuários e clientes.

## **9. Segurança da Informação e Prevenção de Incidentes**

A efetividade das atividades especializadas de vigilância e monitoramento eletrônico prestadas pela corporação está intimamente associada ao emprego de rígidos controles de segurança da informação física e digital. A central de monitoramento inteligente, ambiente tático responsável pelo controle de alarmes, sensores e câmeras de última geração instalados nas sedes de nossos contratantes, condomínios residenciais e empresariais, é protegida por barreiras de acesso físico com identificação biométrica e controle contínuo de entrada, impedindo que pessoas não autorizadas adentrem o recinto de segurança ou interajam de forma desregulada com as telas operacionais e sistemas eletrônicos de tratamento de imagens.

No plano da segurança cibernética e dos controles digitais de sistemas, a empresa adota políticas severas de controle de acessos, exigindo de todos os operadores e pessoal administrativo a utilização de senhas individuais complexas, sujeitas a ciclos de troca periódica compulsória e com mecanismos obrigatórios de autenticação multifatorial para acesso a qualquer plataforma ou banco de dados corporativo. As imagens de CFTV e os cadastros mantidos sob custódia são processados eletronicamente por meio de canais de transmissão protegidos por algoritmos de criptografia de alta segurança, impedindo a interceptação por terceiros maliciosos e salvaguardando a integridade e a confidencialidade das mídias digitais.

O acesso direto a mídias gravadas e servidores de imagem é uma atribuição tática excepcional, restrita unicamente a analistas técnicos devidamente autorizados e à coordenação do Encarregado pelo Tratamento de Dados Pessoais, sendo terminantemente proibido o desvio de finalidade por operadores comuns do sistema. Os softwares operacionais utilizados na portaria inteligente e na gestão do livro de ocorrências digital registram de maneira irrecusável os logs de atividades de cada usuário do sistema, registrando o horário, a máquina e a ação exata realizada por cada colaborador, o que viabiliza auditorias digitais constantes e imediatas face a eventuais condutas atípicas.

No tocante à segurança documental física, a organização impõe a seus vigilantes, porteiros e atendentes administrativos o estrito cumprimento de normas de conduta operacional, as quais preconizam que todas as fichas cadastrais de portaria, correspondências e relatórios de ronda impressos sejam manuseados em ambiente reservado e arquivados em armários trancados com acesso restrito aos supervisores. Fica terminantemente proibido aos colaboradores operacionais a reprodução fotográfica de telas de sistemas com dados de moradores ou o compartilhamento de imagens de trânsito em grupos particulares de mensagens ou redes de comunicação social não oficiais, caracterizando o descumprimento de tais preceitos falta grave

passível de demissão por justa causa e instauração de procedimentos disciplinares de apuração civil e criminal correlatos.

## **10. Retenção e Descarte Seguro de Dados Pessoais**

A estipulação dos prazos de guarda para todas as informações sob a responsabilidade de tratamento da organização pauta-se estritamente pelos postulados da necessidade, finalidade e do término do tratamento estatuídos pela legislação federal de privacidade, garantindo-se que nenhum dado seja mantido por tempo superior ao indispensável para a consecução de suas legítimas finalidades institucionais. As imagens brutas colhidas pelo circuito fechado de televisão (CFTV) e sistemas ópticos de segurança são armazenadas de forma segura em nossos servidores de monitoramento eletrônico pelo período ordinário de até trinta dias, lapso temporal em que a finalidade de segurança preventiva é integralmente satisfeita, ocorrendo ao término desse prazo a exclusão lógica definitiva e automática das mídias por meio de processos técnicos de sobrescrita programada.

Caso se verifique a ocorrência de incidentes de segurança, sinistros, infrações cíveis ou penais registradas pelas câmeras de monitoramento, o trecho específico da filmagem que contenha a evidência do fato é imediatamente extraído e isolado pela equipe de segurança da informação, passando a ser mantido em arquivo criptografado de segurança pelo prazo prescricional para o exercício regular de direitos em juízo, estipulado ordinariamente em até cinco anos, ou até o trânsito em julgado das discussões conexas. Por sua vez, os registros eletrônicos de cadastros de visitantes, correspondências de portaria e diários eletrônicos de ronda são mantidos em banco de dados ativo pelo período máximo de noventa dias para auditorias comuns de segurança e, após esse prazo, excluídos de forma lógica das plataformas operacionais ordinárias, ressalvadas as exigências de cumprimento de obrigações contratuais de nossos clientes tomadores de serviço.

Os dados de departamento pessoal de ex-colaboradores da empresa, incluindo fichas funcionais, registros de jornada, exames de medicina ocupacional e contracheques, são retidos após o término das relações laborais em arquivo físico ou digital de segurança de acordo com os prazos prescricionais de natureza trabalhista, previdenciária e tributária federal, que podem variar de cinco a trinta anos de duração. A conservação autorizada de dados pessoais após o término do tratamento é permitida nas hipóteses previstas em lei, assegurando a conformidade e a segurança das operações corporativas mesmo diante do encerramento das



atividades de tratamento originais, consoante dispõe o permissivo contido na legislação geral de proteção de dados:

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

A responsabilidade pelo controle dessas operações de tratamento de dados e pela auditoria de seus prazos de armazenamento impõe ao controlador a manutenção contínua de registros operacionais precisos de todas as etapas de processamento das informações pessoais sob sua guarda. A legislação geral de privacidade prevê que a Autoridade Nacional de Proteção de Dados possui plena competência para intervir nestes fluxos, ditando e disciplinando parâmetros interoperáveis de portabilidade de dados e os tempos de guarda recomendáveis para os registros eletrônicos de atividades, sempre de forma proporcional à necessidade de transparência de cada segmento operacional do mercado, conforme estabelece o dispositivo normativo:

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

A legitimidade da adoção de medidas rigorosas e restritivas de controle, guarda e sigilo de registros eletrônicos e bancários também encontra respaldo no entendimento jurisprudencial dominante, o qual valida a decretação de segredo de justiça ou de restrição pública a repositórios contendo dados pessoais de relevo quando houver risco concreto à

privacidade ou de fraudes em massa, harmonizando o princípio da publicidade com as normas protetivas de intimidade e com as diretrizes preventivas da Lei Geral de Proteção de Dados. No âmbito do julgamento do Agravo de Instrumento número 1017587-64.2025.8.11.0000, sob a relatoria do Desembargador Jones Gattass Dias, a Terceira Câmara de Direito Público e Coletivo do Tribunal de Justiça de Mato Grosso reconheceu a legalidade de medidas severas de segurança e sigilo de dados financeiros e cadastrais sob a ótica de mitigação de riscos de incidentes coletivos e segurança dos indivíduos.

Ao atingirem os limites temporais e operacionais previstos nesta política corporativa, todas as mídias, cadastros e registros em papel são submetidos a procedimentos específicos de descarte seguro e definitivo. Os arquivos eletrônicos e registros digitais são eliminados de nossos servidores mediante o emprego de algoritmos especializados de apagamento seguro, os quais impedem de forma absoluta qualquer tentativa técnica posterior de recuperação dos dados de mídia. Os documentos e relatórios impressos em papel que contenham qualquer categoria de dados qualificativos pessoais são recolhidos e destruídos fisicamente em fragmentadoras industriais de alta segurança, as quais reduzem as mídias a fragmentos em partículas microscópicas, inviabilizando a reconstrução das peças ou a leitura de dados residuais por terceiros.

## **11. Responsabilidades de Colaboradores, Gestores e Parceiros**

A consolidação de uma cultura de privacidade, conformidade e proteção de dados no ecossistema operacional da corporação é uma atribuição coletiva, a qual exige de cada participante da cadeia de serviços o cumprimento rigoroso de deveres e responsabilidades específicos inerentes ao seu nível hierárquico e funcional. Os colaboradores que atuam diretamente nas funções operacionais de campo, tais como porteiros, vigilantes de postos físicos, operadores de ronda móvel, auxiliares de conservação e manutenção, recepcionistas e atendentes, possuem o dever profissional intransponível de sigilo profissional absoluto acerca de todas as informações pessoais, dados de tráfego, rotinas diárias de moradores, placas de veículos e imagens de CFTV a que tenham acesso em razão do exercício regular de suas atividades corporativas nas portarias e centrais de monitoramento.

Os prepostos operacionais estão pessoalmente sujeitos às regras de conduta estipuladas nos Procedimentos Operacionais Padrão da organização, restando expressamente vedada a manipulação, o repasse, o desvio de finalidade ou a divulgação inadequada de registros cadastrais ou gravações físicas para pessoas estranhas à atividade tática autorizada. A

supervisão das equipes e a fiscalização de campo sobre o cumprimento destas normas de conduta cabe de modo prioritário aos gestores administrativos, coordenadores e gerentes operacionais de área, os quais devem assegurar que todas as diretivas de proteção de dados pessoais sejam implementadas nos respectivos postos de serviço sob sua responsabilidade técnica direta, cabendo-lhes ainda reportar de imediato ao Encarregado de Proteção de Dados (DPO) qualquer indício de desvio de comportamento ou irregularidades no tratamento eletrônico ou físico de dados pessoais.

No plano dos fornecedores de infraestrutura técnica, integradores de sistemas de segurança e parceiros comerciais de tecnologia, com relevo para a H3 Tecnologia e a SafeBras, os contratos corporativos celebrados impõem obrigações contratuais de integridade e deveres severos de governança cibernética. Os parceiros tecnológicos são classificados como operadores de dados pessoais para os fins legais, respondendo de forma objetiva por danos patrimoniais ou morais decorrentes do tratamento irregular de dados sob sua responsabilidade eletrônica direta ou por descumprimento de ordens claras emanadas do controlador. As empresas parceiras devem assegurar que seus engenheiros de software, administradores de rede e prepostos de manutenção atuem com os mesmos níveis de sigilo e sob o manto de fortes restrições tecnológicas de acesso aos dados que circulam nas plataformas digitais e centrais automatizadas sob sua gerência técnica.

## **12. Treinamento, Auditoria, Melhoria Contínua e Disposições Finais**

A governança corporativa de dados na organização não se limita ao plano normativo formal, materializando-se em ações contínuas de conscientização, reciclagem de rotinas e monitoramento de desempenho operacional. A instituição adota como política obrigatória a realização de treinamentos periódicos compulsórios destinados a todos os seus colaboradores administrativos e operacionais sobre a legislação de proteção de dados pessoais, privacidade, sigilo de correspondências e segurança física de cadastros. Estes ciclos de treinamento integram o Procedimento Operacional Padrão exclusivo e os programas de capacitação e aprimoramento contínuo da organização, garantindo que as equipes estejam tecnicamente preparadas para alinhar a larga experiência de segurança pública ao dinamismo da segurança privada, agindo com planejamento, sabedoria e conformidade em suas operações diárias de controle e vigilância de áreas comuns.

A fiscalização e o controle das práticas de tratamento de dados são assegurados por meio de mecanismos internos de auditoria técnica programados e coordenados diretamente pelo

Encarregado pelo Tratamento de Dados Pessoais (DPO). As centrais de tecnologia e os computadores das portarias integradas passam por varreduras eletrônicas regulares para identificar vulnerabilidades técnicas, analisar possíveis tentativas de acesso indevido e garantir que o armazenamento de mídias de CFTV e biometria facial esteja ocorrendo de forma criptografada nos servidores autorizados das parceiras tecnológicas. As vistorias presenciais dos gerentes de área também alcançam a verificação da integridade física dos cadastros físicos e armários de guarda documental nas sedes das portarias.

A presente Política de Privacidade e Proteção de Dados Pessoais constitui um documento corporativo dinâmico e flexível, que passará por processos constantes de revisão, adaptação técnica e melhoria contínua sob a orientação e acompanhamento direto da Diretoria e do DPO da General Smart. As alterações serão implementadas sempre que houver modificações relevantes nos fluxos operacionais, adoção de novas tecnologias de monitoramento ou mediante a publicação de novas diretrizes regulatórias e normativos vinculantes pela Autoridade Nacional de Proteção de Dados (ANPD).

Este instrumento entra em vigor e produz efeitos jurídicos plenos em caráter imediato a partir de sua publicação oficial no sítio corporativo da instituição, ato formalizado na data de 05/06/2026, revogando-se integralmente quaisquer normativos internos, orientações ou procedimentos anteriores em sentido contrário. A aprovação formal deste normativo vincula e sela o compromisso institucional da **General Smart Segurança Privada e Terceirizações Ltda.** com a integridade, transparência e respeito incondicional aos direitos fundamentais de intimidade e proteção de dados de todos os cidadãos.

### **13. Termo de Ciência, Anexo I (Confidencialidade) e Anexo II (Solicitacao)**

Termo de Ciência e Compromisso do Corpo de Gestão e Diretoria

Eduardo Henrique de Souza, Coronel da Reserva da Polícia Militar do Estado de Mato Grosso na condição de fundador da General Smart Segurança Privada e Terceirizações Ltda. e os diretores e gestores da instituição declaram, por meio deste instrumento oficial de compromisso corporativo, plena ciência e total adesão às diretrizes operacionais de privacidade e proteção de dados estabelecidas nesta política, obrigando-se a conduzir as atividades diretivas com foco na integridade, na honestidade, na sabedoria e no planejamento estratégico, assegurando que o tratamento de dados pessoais no âmbito operacional seja mantido sob rígidos controles e que os valores éticos institucionais guiem o aprimoramento contínuo das rotinas operacionais.

#### Anexo I: Termo de Confidencialidade e Sigilo Profissional do Colaborador

Pelo presente instrumento de aditivo contratual e termo de compromisso de sigilo profissional, o colaborador qualificado perante o departamento pessoal da General Smart Segurança Privada e Terceirizações Ltda. declara e concorda que, em virtude de suas funções de campo de vigilância armada, fiscalização operacional, portaria física ou monitoramento eletrônico, terá acesso a dados pessoais sensíveis, imagens de segurança e cadastros eletrônicos de moradores e visitantes, assumindo a obrigação intransponível de manter absoluto sigilo profissional sobre todos os dados e rotinas de segurança sob sua atuação. Compromete-se a não divulgar, repassar, fotografar ou extrair registros eletrônicos sem autorização fundamentada, ciente de que o descumprimento intencional acarretará a imediata instauração de procedimento administrativo disciplinar para demissão por justa causa, sem prejuízo da responsabilização civil e criminal por eventuais perdas e danos decorrentes do vazamento de informações.

#### Anexo II: Formulário Padrão de Requisição de Direitos do Titular de Dados

Nome Completo do Requerente: campo para identificação obrigatória do titular.

Documento de Identidade: inserção do RG e CPF com cópia simples para conferência.

Telefone e Endereço Eletrônico: contatos do requerente para retorno das providências.

Relação com a General Smart: indicação de vínculo como morador, visitante, colaborador, prestador ou usuário monitorado.

Descrição Detalhada do Pedido: espaço reservado para que o titular formalize o objeto de seu requerimento, como confirmação de dados cadastrais, acesso simples a imagens específicas de CFTV com indicação de data, hora e local exato, correção de dados inexatos, oposição ao tratamento de dados ou exclusão segura de informações não fundamentadas em lei.

Assinatura Física ou Assinatura Digital do Titular de Dados Pessoais: campo final reservado para o encerramento do formulário de solicitação de direitos.

#### **14. Anexo III (Resposta a Incidentes) e Anexo IV (Declaracao de Ciencia)**

Anexo III: Procedimento Simplificado de Resposta a Incidentes de Segurança da Informação

O fluxograma organizacional para contenção célere e tratamento de eventos adversos ou suspeitas fundamentadas de incidentes com dados pessoais no âmbito da General Smart obedece às seguintes etapas:

**Identificação e Alerta:** o colaborador que identificar qualquer vulnerabilidade técnica, perda de arquivos físicos, extravio de relatórios cadastrais ou indício de acesso cibernético não autorizado nos servidores deve reportar imediatamente o fato por meio de canal interno seguro à gerência operacional.

**Isolamento e Contenção:** o departamento de segurança e tecnologia cibernética isolará o servidor afetado, suspenderá temporariamente as credenciais eletrônicas comprometidas ou confiscará os documentos físicos extraviados para conter o impacto imediato do incidente em no máximo doze horas.

**Notificação e Avaliação:** a gerência comunicará formalmente o fato ao Encarregado pelo Tratamento de Dados Pessoais (DPO), que iniciará o diagnóstico de impacto, avaliando a natureza das informações expostas, as possíveis consequências para a privacidade dos titulares e as medidas de remediação recomendadas.

**Comunicação e Registro:** caso se identifique risco relevante ou de danos significativos para os direitos e liberdades dos titulares, o DPO conduzirá a comunicação obrigatória à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados no prazo legal, registrando todas as fases do incidente em relatório específico para fins de auditoria de conformidade regulatória.

**Anexo IV: Declaração de Ciência e Adequação à LGPD para Fornecedores e Parceiros**

A empresa parceira qualificada no contrato principal, atuando no fornecimento de sistemas de controle, alarmes, sensores, licenciamento de softwares de portaria e integradora de monitoramento eletrônico, declara e assegura, por meio desta declaração institucional de ciência e adequação, que possui conhecimento integral das diretrizes desta Política de Privacidade e dos preceitos estabelecidos pela Lei Geral de Proteção de Dados, obrigando-se a tratar todas as informações em nome da General Smart estritamente sob as nossas ordens e para as finalidades contratuais de segurança pactuadas. Compromete-se a implementar e manter medidas técnicas avançadas de segurança cibernética, como criptografia de transmissão, controle rígido de logins de manutenção e canais de auditoria digital dos logs de operação, abstendo-se de reutilizar os dados pessoais em benefício próprio ou para fomento de bases

comerciais terceiras, sob pena de rescisão contratual imediata e aplicação de multas rescisórias indenizatórias cumulativas correspondentes.