TARGET.IT

POLÍTICA DE PRIVACIDADE

1. Objetivo

Esta Política de Privacidade estabelece diretrizes para o tratamento e a proteção de dados pessoais realizado pela TARGET.IT, buscando preservar a privacidade dos titulares e a confidencialidade, integridade e disponibilidade das informações. Complementa as políticas e procedimentos internos de Segurança da Informação, classificação da informação, controle de acesso, avaliação e gerenciamento de riscos, conformidade, gestão de vulnerabilidades e resposta a incidentes.

O tratamento de dados pessoais deverá observar a legislação aplicável, incluindo a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), e os compromissos legais, regulatórios e contratuais pertinentes.

2. Abrangência

Aplica-se às empresas integrantes da TARGET.IT, seus colaboradores, administradores, estagiários, prestadores de serviços, fornecedores, parceiros e demais terceiros que tratem dados pessoais em seu nome ou tenham acesso a informações e sistemas da organização. Abrange dados tratados em meios físicos ou digitais, nas instalações da empresa, em trabalho remoto e por meio de dispositivos, redes, aplicações, infraestrutura própria ou serviços contratados.

Quando a TARGET.IT tratar dados pessoais em nome de clientes ou de terceiros, o tratamento deverá respeitar as instruções documentadas, os contratos aplicáveis e as responsabilidades atribuídas a cada parte.

3. Princípios

A TARGET.IT deverá orientar o tratamento de dados pessoais pelos princípios e requisitos previstos na legislação aplicável, incluindo:

- Finalidade: tratar dados para propósitos legítimos, específicos e informados, quando aplicável.
- Adequação e necessidade: limitar o tratamento ao que for pertinente, proporcional e necessário à finalidade.
- Livre acesso e transparência: fornecer informações claras sobre o tratamento, respeitados os limites legais e a segurança de terceiros.
- Qualidade dos dados: adotar medidas razoáveis para manter dados exatos, claros, relevantes e atualizados quando necessário.
- Segurança e prevenção: empregar medidas técnicas e administrativas para prevenir acessos não autorizados, perdas, alterações, divulgações ou tratamentos inadequados.
- Não discriminação e responsabilização: não utilizar dados para finalidades discriminatórias ilícitas e manter condições de demonstrar a adoção de medidas de conformidade.

4. Categorias de dados, titulares e finalidades

Conforme a atividade e a relação estabelecida, a TARGET.IT poderá tratar dados pessoais de colaboradores e candidatos, clientes e seus representantes, fornecedores, parceiros, visitantes, usuários de sistemas e demais pessoas que interajam com a organização. As categorias efetivamente tratadas, as finalidades e os dados necessários deverão ser identificados pelos responsáveis por cada processo.

As finalidades podem incluir, conforme aplicável e legítimo: execução e gestão de contratos; prestação, suporte, manutenção e segurança de serviços; gestão de relacionamento com clientes e fornecedores; recrutamento e gestão de pessoas; controle de acesso físico e lógico; prevenção e investigação de fraudes e incidentes; atendimento de obrigações legais, regulatórias e contratuais; exercício regular de direitos; auditorias, gestão de riscos e melhoria de processos.

Esta política não presume que todas essas categorias ou finalidades sejam utilizadas em todos os processos. Cada área deverá documentar o tratamento que efetivamente realiza e limitar a coleta ao necessário.

5. Bases legais e transparência

Cada atividade de tratamento deverá possuir uma base legal válida, definida e documentada pelo responsável pelo processo com apoio das áreas competentes. Conforme o caso concreto, poderão ser aplicáveis bases legais previstas na LGPD, como execução de contrato ou procedimentos preliminares, cumprimento de obrigação legal ou regulatória, exercício regular de direitos, legítimo interesse após avaliação pertinente, proteção do crédito ou consentimento, quando este for adequado.

Quando o consentimento for utilizado, deverá ser obtido de forma válida, livre, informada e inequívoca, para finalidades determinadas, e sua revogação deverá ser tratada nos termos da legislação. O consentimento não deverá ser adotado como base automática quando outra base for mais apropriada.

Avisos de privacidade, contratos, formulários ou comunicações pertinentes deverão informar, conforme aplicável, quem realiza o tratamento, as finalidades, categorias de dados, compartilhamentos relevantes, direitos dos titulares e canal para solicitações.

6. Dados pessoais sensíveis e de crianças e adolescentes

O tratamento de dados pessoais sensíveis deverá ocorrer somente quando houver hipótese legal aplicável e controles proporcionais à sensibilidade e ao risco. O acesso deverá ser restrito às pessoas autorizadas que necessitem dos dados para suas atribuições.

O tratamento de dados de crianças e adolescentes deverá observar a legislação aplicável e seu melhor interesse, com os requisitos específicos de transparência, autorização e proteção que sejam pertinentes à situação.

7. Classificação, acesso e armazenamento

Os dados pessoais e os ativos de informação que os contenham deverão ser classificados de acordo com seu valor, sensibilidade, criticidade, riscos e obrigações legais, regulatórias e contratuais, observando-se a Política de Classificação da Informação da TARGET.IT. Dados pessoais sensíveis e

grandes conjuntos de dados pessoais deverão receber proteção compatível com sua classificação e risco.

- O acesso deverá ser concedido segundo a função, a necessidade de conhecimento e o princípio do menor privilégio, com revisão e revogação quando necessário.
- Deverão ser utilizados os mecanismos de autenticação corporativos e, quando exigido pelas regras internas, autenticação multifator, especialmente em acessos remotos, contas privilegiadas e ambientes em nuvem.
- As informações deverão ser armazenadas preferencialmente em sistemas corporativos, armazenamento em nuvem aprovado ou unidades de rede autorizadas. Deve-se evitar armazenamento local não aprovado.
- A transmissão, cópia, impressão, exportação e compartilhamento de dados pessoais deverão ser limitados ao necessário e realizados por meios autorizados, com proteção adequada ao nível de classificação.
- Projetos, processos e sistemas novos ou alterados que envolvam dados pessoais deverão considerar questões de privacidade desde o início e identificar medidas de mitigação de riscos.

8. Compartilhamento e operadores

O compartilhamento de dados pessoais com clientes, fornecedores, parceiros, prestadores de serviço, autoridades ou outras partes somente poderá ocorrer quando houver finalidade legítima, base legal e autorização apropriada, respeitando a legislação, os contratos e as instruções aplicáveis.

Antes de contratar ou utilizar terceiros que tratem dados pessoais, as áreas responsáveis deverão avaliar, conforme o risco, as necessidades de segurança, confidencialidade, uso limitado, subcontratação, apoio no atendimento aos titulares, comunicação de incidentes, retenção e descarte. Contratos e acordos pertinentes deverão definir as obrigações de cada parte.

Não deverão ser divulgados dados pessoais a pessoas não autorizadas. Solicitações externas de informação deverão ser encaminhadas à área competente, incluindo Jurídico e Segurança da Informação quando aplicável.

9. Transferências internacionais

Quando houver transferência internacional de dados pessoais ou acesso a partir de outro país, a área responsável deverá avaliar previamente a aplicabilidade da LGPD e assegurar a existência de mecanismo válido de transferência, garantias contratuais e medidas de proteção exigidas pela legislação. A existência de infraestrutura ou fornecedor no exterior deverá ser identificada no inventário do tratamento, quando aplicável.

10. Retenção, arquivamento e descarte

Os dados pessoais deverão ser mantidos somente pelo período necessário para cumprir as finalidades do tratamento, obrigações legais ou regulatórias, contratos, exercício regular de direitos e outras hipóteses legítimas de conservação. Cada processo deverá estabelecer critérios ou prazos de retenção, considerando os requisitos legais e contratuais.

Encerrado o prazo de conservação e inexistindo fundamento legítimo para manutenção, os dados deverão ser eliminados, anonimizados ou submetidos a outra forma de descarte seguro compatível com o meio utilizado e com os procedimentos corporativos. Eventuais bloqueios de eliminação por obrigação legal, litígio ou investigação deverão ser documentados e limitados ao necessário.

11. Direitos dos titulares

A TARGET.IT deverá manter um processo para receber, verificar, encaminhar e responder solicitações de titulares, observados os prazos, as condições e as exceções previstos na legislação. Conforme aplicável, os titulares poderão solicitar confirmação da existência de tratamento, acesso, correção, anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade, portabilidade nos termos regulamentares, informações sobre compartilhamento, informações sobre consentimento e sua revogação, bem como revisão de decisões automatizadas quando prevista em lei.

A identidade e a legitimidade do solicitante poderão ser verificadas de forma proporcional para proteger os dados contra divulgação indevida. A resposta deverá considerar direitos de terceiros, segredos comerciais e demais limites legais. Solicitações recebidas por qualquer área deverão ser encaminhadas sem demora ao canal interno designado.

Canal para solicitações de privacidade: a definir pela TARGET.IT antes da publicação desta política. O e-mail seginf@targetit.com.br está indicado nos procedimentos internos como canal de reporte de eventos de segurança ou privacidade; até que haja canal específico aprovado para titulares, poderá ser usado para encaminhamento interno de solicitações, sem substituir a definição formal do canal externo.

12. Segurança da informação

A TARGET.IT deverá manter medidas técnicas e administrativas proporcionais aos riscos para proteger dados pessoais contra acesso não autorizado e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

- Gestão de acessos, segregação de funções, autenticação apropriada e revisão de privilégios.
- Classificação das informações, armazenamento aprovado, controle de acesso físico e lógico e proteção de registros.
- Gestão de vulnerabilidades, varreduras periódicas, testes de intrusão e correção conforme criticidade e procedimentos internos.
- Avaliação e tratamento de riscos, registro das decisões e acompanhamento das medidas de mitigação.
- Treinamento e conscientização de colaboradores e terceiros relevantes.
- Registros e evidências necessários à investigação, auditoria, conformidade e responsabilização, com acesso restrito.

13. Incidentes de segurança e privacidade

Qualquer suspeita ou ocorrência que possa afetar dados pessoais, incluindo acesso indevido, divulgação acidental, perda, alteração, indisponibilidade ou comprometimento de sistemas, deverá

ser reportada o mais breve possível ao canal interno definido no Procedimento de Resposta a Incidentes: seginf@targetit.com.br.

O reporte deve incluir, quando conhecido, data e hora, descrição do evento, tipo de informação envolvida, como foi identificado, pessoas potencialmente afetadas, sistemas envolvidos e evidências disponíveis, como tickets, e-mails e logs. O relato deverá limitar-se às informações necessárias e evitar disseminar dados pessoais por canais não autorizados.

A equipe designada deverá analisar, conter, erradicar e remediar o incidente, documentar decisões e promover atividades pós-incidente e lições aprendidas. As áreas competentes, incluindo jurídico e responsáveis por privacidade, deverão avaliar se o evento constitui incidente envolvendo dados pessoais e se exige comunicação a titulares, à Autoridade Nacional de Proteção de Dados (ANPD) ou a outras partes, conforme a legislação e os prazos aplicáveis. As comunicações externas deverão ser coordenadas por pessoas autorizadas.

14. Avaliação de riscos e conformidade

Os tratamentos de dados pessoais deverão ser considerados nos processos de avaliação e gerenciamento de riscos da TARGET.IT. A avaliação deverá levar em conta a natureza, o contexto, a finalidade, o volume, a sensibilidade dos dados, as ameaças e vulnerabilidades, os possíveis impactos sobre os titulares e os controles existentes.

Quando o risco justificar, poderão ser necessários registros adicionais, avaliação de impacto à proteção de dados pessoais, controles compensatórios ou plano de mitigação. Riscos residuais e decisões de aceitação deverão ser documentados e aprovados conforme a governança interna.

A Segurança da Informação – Compliance deverá realizar verificações de conformidade de acordo com os processos e políticas internas, registrar desconformidades, acompanhar planos de ação e reportar os resultados às partes responsáveis. O descumprimento poderá resultar nas medidas previstas nas regras internas e na legislação aplicável.

15. Responsabilidades

- Liderança da TARGET.IT: aprovar esta política, definir diretrizes e assegurar recursos e governança apropriados.
- Segurança da Informação – Compliance: manter esta política em conjunto com as áreas competentes, apoiar avaliações de risco, monitorar conformidade e coordenar o tratamento de incidentes de segurança conforme os procedimentos internos.
- Jurídico e responsável formal por privacidade/encarregado, quando designado: apoiar a interpretação dos requisitos legais, as respostas a titulares e as avaliações sobre comunicações regulatórias.
- Proprietários de processos, sistemas e ativos: identificar os dados pessoais tratados, finalidades, bases legais, acessos, compartilhamentos e prazos de retenção; implementar controles e considerar privacidade em projetos e mudanças.
- PeopleOps, Infraestrutura e administradores de sistemas: executar as atividades de concessão, alteração e revogação de acessos e apoiar os controles operacionais sob suas responsabilidades.
- Colaboradores e terceiros: cumprir esta política, proteger credenciais e informações, utilizar somente meios autorizados e reportar imediatamente suspeitas de incidentes.

16. Treinamento e conscientização

A TARGET.IT deverá comunicar esta política às pessoas abrangidas e promover orientação compatível com suas funções e riscos. As equipes envolvidas em tratamento de dados pessoais, gestão de acessos, sistemas e resposta a incidentes deverão conhecer os procedimentos pertinentes e participar dos treinamentos aplicáveis.

17. Exceções

Qualquer exceção deverá ser formalmente justificada, avaliada quanto ao risco, documentada e submetida à aprovação da autoridade interna competente. A exceção deverá indicar escopo, duração, controles compensatórios e responsável. Não poderá afastar obrigação legal ou contratual aplicável.

18. Revisão e vigência

Esta política deverá ser revisada periodicamente e sempre que houver mudanças relevantes na legislação, nos serviços, nos processos, nos riscos ou nos controles da TARGET.IT. A versão vigente deverá ser disponibilizada em repositório corporativo aprovado. Esta minuta somente entrará em vigor após validação jurídica e de privacidade, definição dos campos pendentes e aprovação formal da liderança.

19. Documentos relacionados

- Procedimento de Gerenciamento de Risco – TARGET.IT.
- Procedimento de Resposta a Incidentes – TARGET.IT.
- Política de Conformidade – TARGET.IT.
- Política de Controle de Acesso – TARGET.IT.
- Política de Avaliação de Risco – TARGET.IT.
- Política de Classificação da Informação – TARGET.IT.
- Política de Gestão de Vulnerabilidades e Patches de Segurança – TARGET.IT.
- Políticas Anticorrupção – TARGET.IT (referência de governança e conformidade).

Anexo A – Itens para validação antes da publicação

Os documentos fornecidos descrevem controles de segurança, risco, classificação, acesso, conformidade e resposta a incidentes, mas não definem integralmente o inventário de dados pessoais, o canal público para titulares, o encarregado formal, os prazos específicos de retenção por processo ou todas as atividades de tratamento. Antes da publicação, a TARGET.IT deverá validar e completar, no mínimo, os itens abaixo:

- Identificação da pessoa ou área responsável por privacidade e, se aplicável, do encarregado de dados pessoais, com dados de contato aprovados.
- Canal externo oficial para solicitações de titulares e avisos de privacidade.
- Inventário das atividades de tratamento, categorias de titulares e dados, finalidades, bases legais e destinatários.
- Critérios e prazos de retenção e descarte por processo, incluindo backups e registros técnicos.

- Fornecedores e serviços que tratem dados pessoais, incluindo eventuais transferências internacionais.
- Fluxo de avaliação de impacto e critérios para comunicação de incidentes à ANPD e aos titulares.
- Aprovação formal, código documental definitivo, proprietário da política e calendário de revisão.

Nota de elaboração: este documento foi estruturado a partir dos documentos internos fornecidos e de requisitos gerais da LGPD. Os pontos não explicitamente definidos nos documentos foram indicados como itens de validação, e não devem ser considerados decisões já aprovadas pela TARGET.IT.