

Política de Privacidade do **smarters**

Índice

1. Objetivos da política
2. Definições
3. Princípios da LGPD
4. Organização interna
 - Encarregado
 - Comitê de Proteção de Dados Pessoais
5. Treinamentos, conscientização e engajamento
6. Direitos e obrigações do titular
7. Papel do smarterts
8. Compartilhamento de dados (com parceiros, operadores e suboperadores)
9. Transferência internacional de dados
10. Consentimento para tratar dados
11. Deleção de dados pessoais
12. Incidente de segurança da informação
13. Mudanças na política

Objetivos da Política

1. Fornecer informações, facilitar a compreensão, definir, determinar e orientar as diretrizes para a realização do TRATAMENTO de DADOS PESSOAIS no SMARTERS
2. Garantir a privacidade e proteção dos DADOS PESSOAIS em conformidade com a LGPD
3. Indicar as hipóteses de *compliance* entre os procedimentos do SMARTERS relativos à proteção de DADOS PESSOAIS e a ISO 27001
4. Treinar e engajar todos do TIME SMARTERS sobre o TRATAMENTO de DADOS PESSOAIS de terceiros
5. Empoderar todos do TIME SMARTERS sobre o TRATAMENTO de seus próprios DADOS PESSOAIS na empresa
6. Documentar as boas-práticas de governança adotadas pelo SMARTERS



ISO/IEC 27002:2013 extensão ISO/IEC 27701:2019 - Item 8.4.2 Atendimento a LGPD - A política deve estar disponível a qualquer momento para assegurar o cumprimento de normas e boas práticas relativas à proteção de DADOS PESSOAIS.

WHY

Por que: o SMARTERS reconhece, promove e difunde a importância da privacidade dos TITULARES e o impacto positivo do TRATAMENTO de DADOS PESSOAIS, quando adequado.



Como: a atuação do SMARTERS e do TIME SMARTERS será sempre de acordo com as melhores práticas, inclusive de segurança, e sempre em conformidade com a lei e os princípios de proteção dos direitos dos TITULARES.



Valor: TRATAMENTO responsável de DADOS PESSOAIS.



Aplicação: a POLÍTICA se aplica ao TIME SMARTERS, incluindo seus sócios, e a quaisquer terceiros atuando em nome do SMARTERS.



Legislação e políticas: a POLÍTICA se relaciona diretamente com todas as leis, normas e regulamentos aplicáveis ao tema e com as demais políticas do SMARTERS correlacionadas, como a Política de Consentimentos, e é por elas complementada, no que couber.



ISO/IEC 27002:2013 extensão ISO/IEC 27701:2019 - Item 6.2. Atendimento a LGPD - Prover orientação da direção da empresa e apoio para a privacidade e proteção de DADOS PESSOAIS, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Definições

Todos os termos definidos abaixo terão a mesma definição no plural ou singular. Além disso, alguns termos que são definidos pela lei terão a definição legal  e a definição smarters - ou simplificada, para que todos realmente entendam!

POLÍTICA = este documento, com os objetivos e diretrizes apresentados, revisto periodicamente e publicada para o TIME SMARTERS

SMARTERS = AGENTE DE TRATAMENTO que pode ser CONTROLADOR ou OPERADOR e instrui o TIME SMARTERS por meio da POLÍTICA

TIME SMARTERS = membros do SMARTERS que lidam com DADOS PESSOAIS para cumprir suas funções e devem ter suas ações e iniciativas orientadas e reguladas pela POLÍTICA

DADO PESSOAL =  informação relacionada à pessoa natural identificada ou identificável

qualquer informação sobre alguém, como nome, CPF, endereço. Não são consideradas informações sobre empresas

DADO PESSOAL SENSÍVEL =  DADO PESSOAL sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou dado biométrico, quando vinculado a uma pessoa natural

qualquer informação sobre alguém que possa gerar discriminação, mesmo que positiva

CONSENTIMENTO =  manifestação livre, informada e inequívoca pela qual o TITULAR concorda com o TRATAMENTO de seus DADOS PESSOAIS para uma finalidade determinada

"autorização" clara e informada do TITULAR para tratarmos seus DADOS PESSOAIS

TITULAR =  pessoa natural a quem se referem os DADOS PESSOAIS que são objeto de TRATAMENTO

dono daquele nome, CPF, endereço...

TRATAMENTO =  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

absolutamente tudo e qualquer coisa que o SMARTERS e o TIME SMARTERS fizer com DADOS PESSOAIS - inclusive excluir

CONTROLADOR =  pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao TRATAMENTO

empresa que dita as regras sobre o TRATAMENTO

OPERADOR =  pessoa natural ou jurídica, de direito público ou privado, que realiza o TRATAMENTO em nome do CONTROLADOR

empresa que realiza o TRATAMENTO para o CONTROLADOR ou em nome dele

SUBOPERADOR = empresa contratada pelo OPERADOR para auxiliar no TRATAMENTO realizado em nome do CONTROLADOR

AGENTE DE TRATAMENTO = em conjunto ou isoladamente o CONTROLADOR, o OPERADOR e o SUBOPERADOR

ENCARREGADO =  pessoa indicada pelo CONTROLADOR e OPERADOR para atuar como canal de comunicação entre o CONTROLADOR, os TITULARES e a ANPD

pessoa escolhida pelo SMARTERS para atuar em proteção de DADOS PESSOAIS, com as obrigações descritas na POLÍTICA. Também chamado de DPO ("Data Protection Officer")

ANPD = Autoridade Nacional de Proteção de Dados, responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no Brasil

LGPD = Lei 13.709/18, Lei Geral de Proteção de Dados e, na POLÍTICA, todas as demais normas e regulamentos sobre a matéria

COMITÊ = Comitê de Proteção de Dados, grupo multidisciplinar composto por sócios, empregados e prestadores de serviços do SMARTERS, com várias funções, treinados nas melhores práticas e regulações para constante melhoria dos procedimentos com DADOS PESSOAIS, e que auxilia o ENCARREGADO nas suas funções

ROPA = sigla para o Registro de Tratamento de Dados Pessoais, em constante atualização, utilizado no SMARTERS para mapear atividades de TRATAMENTO, seus projetos, apps e APIs que tratam DADOS PESSOAIS

INCIDENTE DE SEGURANÇA DA INFORMAÇÃO =  qualquer evento adverso confirmado, relacionado à violação na segurança de DADOS PESSOAIS, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou TRATAMENTO inadequado ou ilícito que possa ocasionar risco para os direitos e liberdades do TITULAR

qualquer problema de segurança que envolva DADOS PESSOAIS e cause risco ou lesão aos direitos do TITULAR

ISO 27001 = norma de segurança da informação definida pela OIN que, quando integralmente cumprida pode gerar uma certificação

Princípios da LGPD



Finalidade: realização do TRATAMENTO para propósitos legítimos, específicos, explícitos e informados ao TITULAR, sem possibilidade de TRATAMENTO posterior de forma incompatível com essas finalidades.



O TIME SMARTERS nunca realizará nenhum TRATAMENTO sem uma finalidade legítima.

Adequação: compatibilidade do TRATAMENTO com as finalidades informadas ao TITULAR, de acordo com o contexto do TRATAMENTO.



O TIME SMARTERS não realizará TRATAMENTO com finalidade diferente da informada ao TITULAR e se o CONSENTIMENTO for para uma finalidade específica, outro CONSENTIMENTO será coletado para outras finalidades.

Necessidade: limitação do TRATAMENTO ao mínimo necessário para a realização de suas finalidades, com abrangência dos DADOS PESSOAIS pertinentes, proporcionais e não excessivos em relação às finalidades do TRATAMENTO de DADOS PESSOAIS.



O TIME SMARTERS sempre realizará o TRATAMENTO mínimo necessário para o cumprimento da finalidade.

Livre acesso: garantia, aos TITULARES, de consulta facilitada e gratuita sobre a forma e a duração do TRATAMENTO, bem como sobre a integralidade de seus DADOS PESSOAIS.



O SMARTERS atende os TITULARES, por meio do ENCARREGADO e do COMITÊ, pelo e-mail privacy@smarte.rs.

Qualidade dos dados: garantia, aos TITULARES, de exatidão, clareza, relevância e atualização dos DADOS PESSOAIS, de acordo com a necessidade e para o cumprimento da finalidade de seu TRATAMENTO.



O TIME SMARTERS manterá esforços para garantir que os DADOS PESSOAIS tratados estejam corretos, adequados e atualizados.

Transparência: garantia, aos TITULARES, de informações claras, precisas e facilmente acessíveis sobre a realização do TRATAMENTO e os respectivos AGENTES DE TRATAMENTO observados os segredos comercial e industrial.



O TIME SMARTERS realizará um TRATAMENTO transparente e o fornecimento de informações aos TITULARES poderá ter diversas formas de acordo com a hipótese, sempre com o objetivo de melhorar a experiência do TITULAR e garantir a entrega objetiva e clara da informação. São exemplos as políticas de privacidade, termos de consentimento e cláusulas contratuais.

Segurança: utilização de medidas técnicas e administrativas aptas a proteger os DADOS PESSOAIS de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.



O TIME SMARTERS adotará medidas de segurança proporcionais e adequadas para o TRATAMENTO, como o uso de senhas ou encriptação, sempre que necessário.

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do TRATAMENTO de DADOS PESSOAIS.



O TIME SMARTERS realizará o TRATAMENTO adotando alto nível de cautela com a segurança dos DADOS PESSOAIS para prevenir eventuais danos aos TITULARES e seus direitos.

Não discriminação: impossibilidade de realização do TRATAMENTO para fins discriminatórios, ilícitos ou abusivos.



O TIME SMARTERS, em hipótese alguma, realizará o TRATAMENTO com objetivo de discriminar o TITULAR.

Responsabilização e prestação de contas: demonstração, pelo AGENTE DE TRATAMENTO, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de DADOS PESSOAIS e, inclusive, da eficácia dessas medidas.



O membro do TIME SMARTERS que realizar o TRATAMENTO será responsável por ele e pelo cumprimento da POLÍTICA na execução de suas funções.

Organização interna

O programa de governança sobre proteção de DADOS PESSOAIS será implementado, revisado e mantido pelo ENCARREGADO, auxiliado pelo COMITÊ.



Encarregado

👉 É indicado pelo @board, por meio de ata de assembleia dos sócios.

✉️ Seu nome e e-mail para contato devem ser sempre divulgados publicamente, assim como de eventuais substitutos quando houver alteração no cargo.

O e-mail para contato sobre DADOS PESSOAIS para TITULARES, do TIME SMARTERS ou não, é privacy@smarte.rs

Suas atribuições são:

1. Criar um programa de privacidade estratégico e abrangente que define, mantém, desenvolve e implementa políticas e processos para práticas de privacidade eficazes, minimizando os riscos e garantindo a confidencialidade dos DADOS PESSOAIS.
2. Criar e implementar um plano de comunicação sobre proteção de DADOS PESSOAIS no SMARTERS e garantir a interação entre as áreas da empresa para promover a cultura de proteção dos DADOS PESSOAIS.
3. Coordenar o COMITÊ para deliberações de rotina ou emergência, criando e mantendo monitoramento periódico para instaurar a cultura de proteção de DADOS PESSOAIS.
4. Garantir a atualização do ROPA, das políticas e dos procedimentos de privacidade do SMARTERS quando necessário.
5. Realizar, supervisionar e manter procedimentos para rastrear, investigar, avaliar, analisar, mitigar, corrigir e documentar eventuais violações e episódios de risco de privacidade de DADOS PESSOAIS como INCIDENTES DE SEGURANÇA DA INFORMAÇÃO.
6. Assumir uma função de liderança para garantir que o SMARTERS colete e mantenha CONSENTIMENTOS de forma adequada e forneça avisos de acordo com os requisitos legais.
7. Supervisionar, desenvolver e oferecer treinamentos e conscientização sobre privacidade e proteção de DADOS PESSOAIS ao TIME SMARTERS, e sancionar de forma proporcional e em conjunto com o COMITÊ e o RH eventuais violações intencionais.
8. Receber comunicações da ANPD, adotar as providências exigidas e gerenciar todos os processos de notificação de violações exigidos.
9. Aceitar reclamações, comunicações e denúncias de TITULARES, respondê-las, realizar contato ativo com informações quando necessário, prestar esclarecimentos e adotar providências.
10. Estabelecer diretrizes para interações com CONTROLADORES e OPERADORES com os quais o SMARTERS compartilhe ou trate, de qualquer forma, DADOS PESSOAIS.
11. Elaborar relatórios de impacto e reportes de INCIDENTE DE SEGURANÇA DA INFORMAÇÃO quando necessário.

Organização interna



Comitê

 É autônomo em relação a suas orientações e à sua organização interna, como sua estrutura, frequência de reuniões e priorização.

 Também criado por iniciativa do @board, por ata de assembleia dos sócios, para dar assistência ao ENCARREGADO em suas atividades.

 Sua composição pode ser alterada a qualquer tempo, a depender da necessidade do SMARTERS ou dos membros do COMITÊ, sem necessidade de alteração da POLÍTICA, mas com obrigatoriedade de divulgação das alterações realizadas.

Formado por: **Pietro Buquera Bujaldon**, CEO do SMARTERS (pietro@smarters.ai) + **César Gneccchi**, CTO do SMARTERS (cesar@smarters.ai) + **Milla Cerqueira**, a ENCARREGADA (dpo.ext@smarte.rs) + **Felipe Aguiar**, engenheiro de software contratado pelo SMARTERS (felipe@smarters.ai) + **Bianca Isabelle Lourenço**, advogada do SMARTERS (bia@smarters.ai) + **Ana Peng**, diretora de RH (anapeng@smarters.ai)

São assuntos de deliberação do COMITÊ (dentre outros que possam ser relevantes):

1. O programa de privacidade a ser implementado pelo ENCARREGADO e quaisquer iniciativas que auxiliem na criação da cultura de privacidade e proteção de DADOS PESSOAIS no SMARTERS.
2. Solicitações, reclamações, comunicações e denúncias de TITULARES ou necessidade de contato para informar sobre seus DADOS PESSOAIS.
3. Notificações, solicitações ou necessidade de contato com a ANPD para notificar violações ou prestar informação.
4. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO, os procedimentos de prevenção e eventual rastreamento, investigação, avaliação, análise, mitigação, correção e documentação de violações.
5. Atualização das políticas e procedimentos do SMARTERS sobre DADOS PESSOAIS, aplicação de treinamentos ao TIME SMARTERS e eventuais sanções internas por violações intencionais.
6. Aprovação de relatórios de impacto e reportes de INCIDENTE DE SEGURANÇA DA INFORMAÇÃO elaborados pelo ENCARREGADO.



Treinamento, conscientização e engajamento



O SMARTERS promoverá treinamentos periódicos para o TIME SMARTERS e informará com antecedência quais são obrigatórios, garantindo a participação de todos.



Todas as regras e direcionamentos sobre o tema serão tratados de forma simplificada e acessível para gerar o engajamento do TIME SMARTERS e promover a cultura de privacidade na empresa.



O COMITÊ e o ENCARREGADO estarão sempre disponíveis para esclarecer dúvidas e suportar o TIME SMARTERS sobre o TRATAMENTO de DADOS PESSOAIS de clientes, fornecedores e quaisquer terceiros, bem como dos seus próprios DADOS PESSOAIS tratados pelo SMARTERS.



O ENCARREGADO e o COMITÊ participarão de projetos, desenvolvimento de novos negócios e reuniões internas ou com clientes sempre que solicitado por alguém do TIME SMARTERS que entenda ser necessária a avaliação de questões relacionadas à privacidade ou proteção de DADOS PESSOAIS.



Os membros do TIME SMARTERS serão, sempre, convidados a participar e trazer questões sobre o tema para esclarecimento e desenvolvimento da cultura de forma participativa e colaborativa.



O TIME SMARTERS é e será sempre instruído a priorizar o privacy by design, ou seja, a aplicação dos princípios e orientações sobre privacidade e proteção de DADOS PESSOAIS na concepção dos produtos e serviços desenvolvidos.



O TIME SMARTERS terá o conhecimento necessário sobre o plano de resposta de incidentes do SMARTERS e terá livre acesso ao COMITÊ e ao ENCARREGADO para reportar qualquer suspeita de infração ou incidente.



Direitos e obrigações do titular

→ Todos do TIME SMARTERS devem respeitar os direitos do TITULAR quando realizarem qualquer TRATAMENTO com DADOS PESSOAIS de outros

←...e todos do TIME SMARTERS devem ter seus direitos respeitados como TITULARES de seus DADOS PESSOAIS

! Assim, todos os direitos aqui descritos são também **obrigações e orientações!**



O TITULAR tem direito a:

1. Liberdade, intimidade e privacidade
2. Ser informado, de forma clara (sobre: seus direitos, a finalidade, a forma e a duração do TRATAMENTO, quem é o CONTROLADOR e quais são suas informações de contato e responsabilidades, quem é o OPERADOR, quando houver, e suas responsabilidades, se seus DADOS PESSOAIS são compartilhados, com quem e qual a finalidade do compartilhamento, o que é o CONSENTIMENTO, quais as consequências de fornecê-lo e de não fornecê-lo, quais critérios e procedimentos são utilizados para a tomada de decisões automatizadas, se houver)
3. Confirmar se existe TRATAMENTO
4. Acessar os próprios DADOS PESSOAIS
5. Corrigir ou solicitar a correção de dados incompletos, inexatos ou desatualizados
6. Solicitar a anonimização, bloqueio ou eliminação de seus DADOS PESSOAIS tratados sem conformidade com a LGPD
7. Receber seus DADOS PESSOAIS para que sejam portados a outro fornecedor
8. Revogar seu CONSENTIMENTO
9. Solicitar a eliminação dos DADOS PESSOAIS cujo CONSENTIMENTO tenha sido retirado
10. Opor-se a TRATAMENTOS que não estejam de acordo com a LGPD
11. Não ser discriminado a partir de seus DADOS PESSOAIS
12. Não ter seus DADOS PESSOAIS utilizados para fins ilícitos ou abusivos
13. Solicitar a revisão de decisões tomadas unicamente por TRATAMENTO automatizado quando elas afetarem seus interesses
14. Ser notificado sobre qualquer INCIDENTE DE SEGURANÇA DA INFORMAÇÃO que possa causar risco ou dano relevante
15. Peticionar à ANPD ou aos órgão de defesa do consumidor caso entenda que seus direitos foram violados

Deve ser solicitado ao ENCARREGADO ou ao COMITÊ pelo e-mail privacy@smarte.rs

✗ não é possível fazer pedidos em nomes de terceiros sem procuração específica

✗ não é possível excluir dados necessários para a execução de contratos em vigor ou tratados para cumprimento de obrigação legal ou regulatória

✗ a revogação do CONSENTIMENTO pode inviabilizar a continuidade do serviço que motiva o TRATAMENTO

🔒 o ENCARREGADO pode e irá exigir a confirmação de alguns DADOS PESSOAIS ou outra forma de confirmar a identidade do TITULAR antes de repassar qualquer informação para garantir a segurança dos dados

🔒 o TITULAR é responsável pela veracidade dos DADOS PESSOAIS e sua imprecisão pode gerar consequências civis (multas) e criminais

🔒 o TITULAR também é responsável por reparar eventuais danos causados intencionalmente ou por culpa, por ação ou omissão, ao SMARTERS, ao TIME SMARTERS e a qualquer outro TITULAR



Papel do smarterts

O SMARTERS será **CONTROLADOR** sempre que as decisões fundamentais sobre o TRATAMENTO e os DADOS PESSOAIS for de sua responsabilidade

Exs.: DADOS PESSOAIS dos membros do TIME SMARTERS, tratados para manutenção da relação de trabalho, DADOS PESSOAIS de empregados de parceiros para comunicações

O SMARTERS será **OPERADOR** sempre que decisões fundamentais sobre o TRATAMENTO e os DADOS PESSOAIS forem do cliente que contratou o SMARTERS para realizar o TRATAMENTO em seu nome

Exs.: DADOS PESSOAIS de usuários dos agentes que são tratados para fornecer informações aos clientes dos projetos

Na realização de qualquer TRATAMENTO, o SMARTERS tomará todas as iniciativas necessárias para:

1. Manter os DADOS PESSOAIS precisos e realizar sua segurança pelo ENCARREGADO e COMITÊ
2. Evitar perdas, danos, falsificação, vazamentos e acesso externo não autorizado
3. Gerenciar os DADOS PESSOAIS e cumprir as determinações de segurança da informação
4. Especificar a finalidade do TRATAMENTO
5. Coletar, armazenar e utilizar os DADOS PESSOAIS de forma adequada e apenas conforme a necessidade de seus negócios
6. Seguir os princípios determinados na LGPD e na POLÍTICA
7. Declarar a base legal que fundamenta aquele TRATAMENTO
8. Atender aos requisitos específicos sobre DADOS PESSOAIS SENSÍVEIS e DADOS PESSOAIS de crianças e adolescentes
9. Não trazer, de nenhuma forma, dano ou prejuízo financeiro ou à imagem do TITULAR
10. Respeitar o tempo adequado e necessário e, terminada a finalidade e qualquer obrigação legal ou contratual de mantê-los, excluir ou anonimizar os DADOS PESSOAIS
11. Evitar incidentes técnicos e aqueles ocasionados pela ação ou omissão humana
12. Manter os DADOS PESSOAIS confidenciais, sempre que possível, e o TRATAMENTO adequado à finalidade
13. Armazenar os DADOS PESSOAIS em ambiente seguro, independente de ser eletrônico ou físico
14. Respeitar os fundamentos da LGPD, como o respeito à privacidade, a liberdade de expressão, o desenvolvimento econômico e tecnológico, a livre iniciativa, a defesa do consumidor e os direitos humanos
15. Tratar os DADOS PESSOAIS apenas na medida do CONSENTIMENTO coletado quando essa for a base legal

Compartilhamento de dados (com parceiros, operadores e suboperadores)



Caso o SMARTERS compartilhe com outras empresas os DADOS PESSOAIS dos quais ele é CONTROLADOR (ex.: de membros do time SMARTERS) OU OPERADOR (ex.: de usuários de agentes conversacionais de projetos), O **SMARTERS**:

1. Prezará pela seleção de terceiros capazes de gerenciar adequadamente os DADOS PESSOAIS e cumprir todas as leis e regulamentos no mesmo padrão de qualidade e comprometimento do SMARTERS
2. Estabelecerá cláusulas contratuais visando o compartilhamento seguro de DADOS PESSOAIS com seus parceiros



O **responsável** do TIME SMARTERS por esse compartilhamento **deverá**:

1. Verificar a idoneidade do parceiro ou fornecedor
2. Garantir que ele tenha firmado com o SMARTERS um acordo de transferência de DADOS PESSOAIS ou contrato comercial que delimite a responsabilidade de cada um quanto o TRATAMENTO
3. Verificar se a finalidade do compartilhamento é legítima e se o TITULAR pode obter informações sobre o compartilhamento quando desejar
4. Informar o ENCARREGADO sobre a parceria ou contratação



Os DADOS PESSOAIS só **poderão** ser compartilhados com terceiros caso:

1. Haja CONSENTIMENTO específico do TITULAR
2. Os DADOS PESSOAIS estejam devidamente anonimizados
3. Seja necessário para cumprir contratos, incluindo o contrato de trabalho do TIME SMARTERS
4. Seja requerido em procedimento de arbitragem ou processos judiciais
5. Seja necessário para realização de auditoria
6. Seja exigido por lei e regulamento ou por um ente público, como um tribunal ou a polícia
7. Seja necessário para proteção à saúde, à vida ou à incolumidade física do TITULAR



ISO/IEC 27002:2013 extensão ISO/IEC 27701:2019 - Item 8.5.5 Atendimento a LGPD - Garantir que os DADOS PESSOAIS não serão divulgados para outros fins; e ISO/IEC 27002:2013 extensão ISO/IEC 27701:2019 - Item 8.5.3 Atendimento a LGPD - Garantir que o TRATAMENTO dos dados tenha nível de proteção e rastreabilidade.

Transferência internacional de dados

? É o envio, transferência, comunicação, difusão ou interconexão de DADOS PESSOAIS para AGENTES DE TRATAMENTO localizados em outro país

↳ exs.: agentes conversacionais do SMARTERS que interajam com o público brasileiro, coletando dados, e enviando para um cliente ou parceiro localizado em outro país.

👤 O membro do TIME SMARTERS responsável pela transferência deve informar o ENCARREGADO para que ele enquadre em uma das bases legais aplicáveis.



A transferência deve ser:

1. Para país com mesmo grau de proteção do Brasil
2. Baseada em cláusulas contratuais específicas
3. Baseada em cláusula padrão contratual
4. Baseada em normas corporativas globais
5. Para proteção da vida ou segurança do TITULAR
6. Com autorização da ANPD
7. Com CONSENTIMENTO específico
8. Para execução de um contrato
9. Para cumprimento de uma lei ou regulamento
10. Para exercício de direito em processo judicial

✗ Não será considerada transferência internacional de DADOS PESSOAIS as hipóteses em que o SMARTERS transferir, armazenar e processar DADOS PESSOAIS com provedores de serviços localizados em outros países (exs.: e-mail, armazenamento em nuvem e disponibilização de aplicativos)

✓ O SMARTERS buscará parceiros qualificados que possam oferecer o mesmo nível de segurança que os DADOS PESSOAIS recebem no Brasil



Consentimento para tratar dados

 O SMARTERS terá disponível nos agentes conversacionais de uso próprio (ex.: Pedro, Barbs), iniciativas programadas de forma padrão para coleta e revogação de CONSENTIMENTO.

 O SMARTERS será o responsável pela coleta, manutenção e guarda do CONSENTIMENTO somente quando for CONTROLADOR.



Quando o SMARTERS for CONTROLADOR devido à coleta de DADOS PESSOAIS em fluxos conversacionais de agentes de uso interno (ex.: Pedro, Barbs):

1. O SMARTERS terá disponível iniciativas programadas de forma padrão para coleta e revogação de CONSENTIMENTO, quando necessários.
2. O SMARTERS será o responsável pela coleta, manutenção e guarda do CONSENTIMENTO.
3. As intenções de término de conversa e revogação de CONSENTIMENTO serão constantemente atualizadas e seguirão o macrofluxo de opt-out indicado nesta POLÍTICA e suas atualizações.
4. Os fluxos conversacionais terão intenções de NLP programadas para esclarecer dúvidas básicas dos TITULARES, também conforme o descrito no macrofluxo de opt-out.



Quando o SMARTERS for OPERADOR devido à coleta de DADOS PESSOAIS em fluxos conversacionais de agentes licenciados:

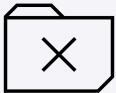
1. O CONTROLADOR é o responsável por instruir o SMARTERS sobre a coleta e a revogação do CONSENTIMENTO.
2. As iniciativas para coleta de CONSENTIMENTO devem ser instruídas, **necessariamente**, pelo CONTROLADOR, por disponibilização de termo ou política de privacidade ou, ainda, por intenção no fluxo conversacional que contenha, no mínimo, seu escopo, abrangência e prazo, caso seja determinado.
3. As iniciativas para revogação do CONSENTIMENTO, sua forma, abrangência e seus impactos devem ser instruídos pelo CONTROLADOR e, não havendo instrução, os fluxos com iniciativas padronizadas pelo SMARTERS serão aplicados, em conformidade com a LGPD e excluindo-se qualquer responsabilidade do SMARTERS sobre a adequação do conteúdo padronizado.

Deleção de dados pessoais



Os DADOS PESSOAIS serão armazenados pelo SMARTERS somente pelo período necessário para o cumprimento de suas finalidades

1. Os DADOS PESSOAIS serão armazenados pelo SMARTERS somente pelo período necessário para o cumprimento de suas finalidades
2. Identificado o termo da finalidade daquele TRATAMENTO, o membro do TIME SMARTERS responsável por aquele DADO PESSOAL deverá eliminá-lo
3. Caso a finalidade esteja atrelada a alguma obrigação legal ou regulatória, o SMARTERS manterá o DADO PESSOAL em conformidade com o prazo indicado na lei ou regulamento
4. Caso o SMARTERS opte por não excluir os DADOS PESSOAIS, ou por impossibilidade técnica, o DADO PESSOAL deverá ser devidamente anonimizado para que seja possível a sua retenção



O TITULAR poderá solicitar a deleção:

1. Apenas de seus DADOS PESSOAIS, ou de criança ou adolescente do qual seja responsável legal, ou apresentando procuração do TITULAR
2. A qualquer tempo, desde que o SMARTERS não tenha que armazená-los para cumprir uma obrigação legal ou regulatória
3. Pelos canais de comunicação com o ENCARREGADO e o COMITÊ
4. Revogando o CONSENTIMENTO caso essa seja a base legal que legitima o TRATAMENTO

 Caso o TITULAR solicite a exclusão de DADOS PESSOAIS necessários para a execução de um contrato ou oferecimento de produto ou serviço, o SMARTERS informará sobre a impossibilidade de prosseguir com aquela execução a partir da eliminação

 Recebida solicitação de exclusão por parte do TITULAR, o membro do TIME SMARTERS que a receber deverá informar o ENCARREGADO para avaliação dos impactos daquela deleção ou solicitação do TITULAR

Incidente de segurança da informação

? É o evento adverso confirmado de violação na segurança de DADOS PESSOAIS

↳ exs.: Acesso não autorizado, destruição, perda, alteração, vazamento e tudo que possa ocasionar risco para os direitos do TITULAR

Incidente técnico é relacionado à problema eletrônico, de hardware ou de software

Exs.: violação de firewall, vírus

Incidente por ação ou omissão humana é relacionado à ação tomada ou não por uma pessoa.

Exs.: DADOS PESSOAIS de usuários dos agentes que são tratados para fornecer informações aos clientes dos projetos



Havendo um INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

1. O Plano de Resposta à Incidentes do SMARTERS deve ser seguido
2. É obrigação de todos os membros do TIME SMARTERS informar imediatamente o ENCARREGADO e o COMITÊ ao descobrir ou suspeitar de um INCIDENTE DE SEGURANÇA DA INFORMAÇÃO com:
 - a. A natureza (exs.: invasão pela internet, roubo ou perda de equipamentos, vírus, dispersão não autorizada)
 - b. Os DADOS PESSOAIS impactados
 - c. A data, hora, local e duração do INCIDENTE DE SEGURANÇA DA INFORMAÇÃO
 - d. As pessoas envolvidas ou com conhecimento do ocorrido
3. O membro do TIME SMARTERS que identificar o INCIDENTE DE SEGURANÇA DA INFORMAÇÃO ou que tiver conhecimento dele deverá auxiliar o ENCARREGADO e o COMITÊ na identificação dos possíveis riscos, e não poderá divulgar, comunicar o alardear o ocorrido sem a devida autorização do ENCARREGADO ou do COMITÊ, sob pena de insubordinação
4. Se o ENCARREGADO e o COMITÊ identificarem dano ou risco de dano relevante aos direitos do TITULAR, o INCIDENTE DE SEGURANÇA DA INFORMAÇÃO deverá, obrigatoriamente, ser informado à ANPD, em 2 dias úteis, seguindo o Plano de Resposta a Incidentes
5. O SMARTERS e todos os membros do TIME SMARTERS deverão colaborar com qualquer investigação que ocorra a respeito
6. Caso o SMARTERS seja OPERADOR dos DADOS PESSOAIS envolvidos no INCIDENTE DE SEGURANÇA DA INFORMAÇÃO, o CONTROLADOR deverá ser avisado de forma imediata para orientar as atitudes preventivas e de reversão do incidente





Mudanças na Política

O SMARTERS, o TIME SMARTERS e as suas atividades estão em constante aprimoramento, assim como essa POLÍTICA. Dessa forma, sua versão mais atual estará sempre disponível na em meio digital e deve ser consultada regularmente.