Regras Corporativas Vinculantes do Grupo PROSEGUR

VERSÃO PÚBLICA

SETEMBRO DE 2023

PROSEGUR

www.prosegur.com

Índice

1. Proprietário

Diretoria de Conformidade do Grupo PROSEGUR.

2. Introdução

2.1. Sobre a Prosegur

- **Prosegur Compañía de Seguridad España, SA** (doravante denominada PROSEGUR): é a Empresa Matriz de um grupo líder mundial no setor de segurança privada. Com as nossas cinco linhas de negócios: alarmes, segurança, Logística de Valores e Gestão de Numerário, terceirização de processos de negócios (AVOS) e cibersegurança (Cipher), proporcionamos segurança confiável às empresas e famílias, com base nas soluções mais avançadas disponíveis no mercado.

- **Alarmes**: a Prosegur Alarmes tem uma ampla gama de produtos que ajudam a melhorar a segurança e a tranquilidade das famílias e empresas. Os alarmes Prosegur Triple Security oferecem os sistemas mais avançados do mercado. A linha da empresa inclui de sistemas de alarme com verificação por vídeo à automatização de áreas internas e externas, produtos sempre personalizados e que nos tornam referência mundial em segurança.

- **Segurança**: a Prosegur Security presta serviços integrais de segurança com alto valor agregado, combinando as mais recentes tecnologias e os melhores profissionais. A Empresa aposta permanentemente na inovação tecnológica, integrando-a na cadeia de valor em cada segmento de negócio.

  O negócio de segurança inclui guarda tripulada tradicional e serviços auxiliares, como segurança cibernética.

  Estes serviços são resultado da experiência e do conhecimento das áreas de risco dos clientes.

- **Logística de Valores e Gestão de Numerário**: o Prosegur Cash abrange todo o ciclo de caixa e processa mais de € 450 bilhões por ano. Esse negócio opera em mais de 500 centros em 15 países e administra mais de 100 mil caixas eletrônicos.

  O Prosegur Cash é líder global na prestação de serviços de logística e gerenciamento de caixa, bem como serviços terceirizados para instituições financeiras, lojas de varejo, agências governamentais e bancos centrais, casas da moeda, joalherias e outras atividades comerciais no mundo todo. Principalmente nos setores de banco e distribuição.

- **AVOS**: o Prosegur AVOS é o setor de atividade com foco em terceirizar soluções de negócios, projetar soluções inovadoras e utilizar novas capacidades tecnológicas.

  No Prosegur AVOS, ajudamos nossos parceiros a melhorar suas operações e ficar à frente do mercado, assumindo os processos mais complexos e melhorando a experiência do cliente. Desenvolvemos uma proposta de valor diferencial cujo objetivo principal é aproveitar o conhecimento adquirido ao longo dos anos e adaptá-lo às novas tendências em tecnologia e digitalização. Nosso objetivo na Prosegur AVOS é proporcionar aos nossos clientes a máxima agilidade, rastreabilidade e visibilidade em todas as tarefas executadas no local de trabalho.

- **Cibersegurança**: A Cipher é uma empresa global de segurança cibernética que presta uma ampla gama de serviços: Detecção e Resposta Gerenciadas (MDR, Managed Detection and

Response), Serviços Gerenciados de Segurança (MSS, Managed Security Services), Serviços de Inteligência Cibernética (CIS, Cyber Intelligence Services), Serviços da equipe vermelha (RTS, Serviços Red Team), Governança, Risco e Conformidade (GRC) e Integração de Tecnologia de Segurança Cibernética (CTI, Cybersecurity Technology Integration). Esses serviços contam com o suporte 24 horas do Cipher Labs, um laboratório de pesquisa e desenvolvimento de ameaças e inteligência cibernética de elite, e também por seis Centros de Operações de Segurança (SOC, Security Operations Centers).

- Operamos nos cinco continentes, onde o desafio é prestar serviços com maior valor agregado e ocupar uma posição de destaque no setor de segurança privada em cada mercado.

- Para isso, buscamos ter uma forte presença geográfica com base em um modelo de negócios consolidado. Além da nossa abordagem global, também atuamos localmente. Atuamos conforme as particularidades de cada mercado, pois o nosso setor é altamente regulamentado e varia de acordo com a legislação de cada país.

- Além de ser líder mundial em prestar serviços de segurança privada, o Grupo PROSEGUR tem um firme compromisso com a sociedade e com os mais desfavorecidos, motivo pelo qual temos uma organização sem fins lucrativos, a Fundação Prosegur, que representa o compromisso do Grupo PROSEGUR de contribuir com o progresso das regiões mais carentes em que atua. O grupo apoia a educação como uma força motriz indiscutível para a mudança, da deficiência intelectual e promove ações de voluntariado que canalizam a solidariedade dos profissionais da nossa empresa.

  Nossos projetos solidários desenvolvidos por meio da Fundação Prosegur nas áreas da educação, inclusão social, voluntariado empresarial e cultura, são implementados progressivamente nos diferentes países em que operamos, levando em conta critérios de sustentabilidade, transparência e replicação de práticas recomendadas.

- A natureza global deste grupo de empresas obriga o Grupo PROSEGUR a envidar todos os esforços para regularizar transferências internacionais de dados que possam ocorrer entre as diferentes entidades do grupo localizadas em várias regiões; Europa, América Latina, EUA e resto do mundo, adotando para esse fim as presentes Regras Corporativas Vinculantes, como definido abaixo.

2.2. Definições

Para fins deste documento, os termos a seguir têm os significados aqui atribuídos.

- “**Acordo de RCV**”: documento com o fim de estabelecer a estrutura jurídica comum para regular os IDTs que ocorram entre as entidades que se enquadrem no seu escopo de aplicação.

- “**Entidade RCV**”: entidade do Grupo PROSEGUR no escopo de aplicação do Acordo de RCV.

- **"Regras Corporativas Vinculantes** -**RCV**" ou "**RCVs**”: significa as políticas de proteção de dados pessoais aderidas por um Controlador ou Processador estabelecido no território de um Estado Membro para transferências ou um conjunto de transferências de Dados Pessoais a um Controlador ou Processador em um ou mais Terceiros Países em um grupo de empresas, ou grupo de empresas envolvidas em uma atividade econômica conjunta.

- **"Autoridade(s) de Supervisão Competente(s)"**: significa Autoridade(s) de Supervisão de Proteção de Dados da EEE competente(s) para os Exportadores de Dados.

- “**Controlador de dados**” ou “**Controlador**”: pessoa física ou jurídica, autoridade pública, agência ou outro órgão que sozinho ou em com outros determine os fins e os meios do Processamento de Dados Pessoais.

- “**Exportador de Dados**”: Entidade RCV estabelecida no Espaço Econômico Europeu.

- "**Importador de Dados**": Entidade RCV estabelecida ou localizada em um Terceiro País.

- "**Processador de dados**" ou "**Processador**": pessoa física ou jurídica, autoridade pública, agência ou outro órgão que processe Dados Pessoais em nome do Controlador.

- "**Avaliação do Impacto da Proteção de Dados**": análise detalhada de uma ou mais operações semelhantes de Processamento de Dados Pessoais, com o fim de identificar e avaliar os riscos associados ao Processamento e determinar as medidas a serem tomadas para evitá-los ou mitigá-los.

- "**Diretor de Proteção de Dados**": pessoa responsável por orientar os Controladores e Processadores sobre suas obrigações sob as leis de proteção de dados pertinentes, monitorar o cumprimento dessas obrigações e atuar como ponto de contato para as Autoridades de Supervisão.

- "**Divulgação**": divulgação por transmissão, disseminação ou disponibilização de outra forma.

- "**Lei Europeia de Proteção de Dados**": o RGPD e as leis de proteção de dados pertinentes dos Estados Membros.

- "**Espaço Econômica Europeu**" ou "**EEE**": os Estados Membros da União Europeia, juntamente com Liechtenstein, Islândia e Noruega.

- "**Leis Europeias**": o direito da União Europeia e dos seus Estados Membros.

- “**RGPD**” ou “**Regulamento Geral de Proteção de Dados**”: o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, sobre a proteção das pessoas físicas no que diz respeito ao processamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados).

- "**Transferências Internacionais de Dados**" ou "**IDTs**": Divulgação de Dados Pessoais de um Exportador de Dados para um Importador de Dados.

- "**Estado(s) Membro(s)**": o(s) Estado(s) Membro(s)s da União Europeia, juntamente com Liechtenstein, Islândia e Noruega.

- "**Transferência(s) Subsequente(s)**”: Divulgação de Dados Pessoais de um Importador de Dados a destinatários, que podem pertencer ou não ao Grupo PROSEGUR.

- “**Dados pessoais**” ou “**Dados**”: significa qualquer informação sobre a uma pessoa física identificada ou identificável ("**Titular dos dados**"); uma pessoa física identificável é aquela que pode ser identificada, de forma direta ou indireta, em particular por referência a um identificador como nome, número de identificação, dados de localização, identificador online ou a um ou mais fatores específicos do físico, identidade fisiológica, genética, mental, econômica, cultural ou social dessa pessoa física.

- "**Violação(ões) de dados pessoais**": violação da segurança levando à destruição, perda ou alteração, ou divulgação ou acesso acidental ou ilegal não autorizado a, Dados Pessoais transmitidos, armazenados ou processados de outra forma.

- "**Pessoal**": qualquer pessoa, seja em tempo inteiro ou temporário, interno ou externo, que preste serviços e/ou exerça uma atividade profissional no escopo de uma entidade do Grupo PROSEGUR.

- "**Processando**": qualquer operação ou conjunto de operações executadas nos Dados Pessoais ou nos conjuntos de Dados Pessoais, por meios automatizados ou não, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, eliminação ou destruição.

- "**PROSEGUR**": Prosegur Compañía de Seguridad España, S.A., empresa controladora do Grupo PROSEGUR.

- "**Grupo PROSEGUR**": todas as entidades que sejam parte do grupo de empresas PROSEGUR, estejam ou não no âmbito do Acordo de RCV.

- "**Destinatário**": pessoa física ou jurídica, autoridade pública, agência ou outro órgão a quem os Dados Pessoais sejam divulgados, seja terceiro ou não. Porém, as autoridades públicas que podem receber dados pessoais no âmbito de uma investigação específica segundo a legislação da União Europeia ou do Estado Membro não serão consideradas Destinatários; o processamento desses dados por tais autoridades públicas deve cumprir com as regras de proteção de dados pertinentes de acordo com as finalidades do Processamento;

- "**Categorias Especiais de Dados Pessoais**": Dados pessoais que revelem a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas ou filiação sindical, bem como os dados genéticos (relacionados às características genéticas herdadas ou adquiridas de uma pessoa física que forneçam informações exclusivas sobre a fisiologia ou a saúde dessa pessoa física e que resultem, nomeadamente, da análise de uma amostra biológica da pessoa física em questão), dados biométricos visando identificar de forma exclusiva uma pessoa física (resultantes de tratamentos técnicos específicos relacionados ao estado físico, fisiológico ou características comportamentais de uma pessoa física, que permitam ou confirmem a identificação exclusiva dessa pessoa singular, como imagens faciais ou dados dactiloscópicos), dados sobre a saúde (relacionados à saúde física ou mental de uma pessoa física, incluindo a prestação de cuidados de saúde, que revelam informações sobre seu estado de saúde) ou dados relacionados à vida sexual ou orientação sexual de uma pessoa física.

- "**Cláusulas contratuais padrão**": cláusulas padrão de proteção de dados adotadas pela Comissão Europeia de acordo com o procedimento de exame mencionado no Artigo 93 (2) do RGPD ou adotadas por uma Autoridade de Supervisão e aprovadas pela Comissão Europeia de acordo com o procedimento de exame mencionado no Artigo 93 (2) do RGPD;

- "**Autoridade de Supervisão**": uma autoridade pública independente, estabelecida por um Estado Membro para monitorar a aplicação do RGPD, a fim de proteger os direitos e liberdades fundamentais de pessoas físicas em relação ao Processamento e facilitar o livre fluxo de Dados Pessoais dentro da União Europeia.

- "**Terceiro(s) País(es)**": países fora do Espaço Econômico Europeu.

- “**Terceiro(s)**”: significa uma pessoa física ou jurídica, autoridade pública, agência ou órgão que não seja o Titular, o Controlador, o Processador dos Dados e as pessoas que, sob a autoridade direta do Controlador ou do Processador, tenham autorização para Processar Dados Pessoais.

3. Escopo

3.1. Escopo material

- Essas RCVs se aplicam a IDTs e ao Processamento feito por Importadores de Dados como resultado de tais IDTs. Aplicam-se também, doravante, às Transferências Contínuas a Entidades de RCV e ao Processamento realizado por eles como resultado de tais Transferências Subsequentes.

3.2. Âmbito Geográfico

3.2.1. Entidades e Pessoal sujeitos às RCVs

- Estas RCVs são vinculativas para todas as Entidades RCV e seu Pessoal. A lista atualizada das Entidades RCV está no Anexo 1.
- A estrutura do Grupo PROSEGUR é apresentada na URL https://www.prosegur.com/en/about.
- Os dados de contato das Entidades RCV são disponibilizados, por país, nas URLs https://www.prosegur.com/en/legal-notice e https://www.prosegur.com/en/privacy-policy.
- O descumprimento por parte do Pessoal de qualquer das obrigações contidas nestas RCVs é considerado violação das instruções da PROSEGUR e/ou das Entidades RCV na sua qualidade de empregador ou empresário. Neste caso, a PROSEGUR e/ou as Entidades RCV reservam-se o direito de exercer as ações judiciais cabíveis (incluindo, sem limitação, ações trabalhistas, civis, administrativas e/ou criminais), relacionadas aos danos causados como resultado de tal descumprimento, e de acordo com as disposições do acordo coletivo e/ou das cláusulas contratuais pertinentes.

3.2.2. Dados Pessoais e atividades de Processamento sujeitas às RCVs

- As atividades de Dados Pessoais, IDT e Processamento sujeitas às RCVs são detalhadas no Mapa Internacional de Transferência de Dados como Anexo 2 e resumidas abaixo:

PAÍSES As RCVs serão aplicáveis às transferências feitas entre as Entidades RCV estabelecidas nos seguintes países:	**ESPAÇO ECONÔMICO EUROPEU**	**FORA DO ESPAÇO ECONÔMICO EUROPEU**
	Espanha; Alemanha; Portugal	Argentina; Austrália; Brasil; Canadá, Chile; Colômbia; Costa Rica; Equador; El Salvador; Guatemala; Honduras; México; Nicarágua; Panamá; Paraguai; Peru; África do Sul; Uruguai; Reino Unido, Estados Unidos

CATEGORIAS DE TITULARES DE DADOS	CATEGORIAS DE DADOS	FINALIDADE(S)
Funcionários e seus beneficiários/familiares (incluindo menores de idade)	Dados de identificação (nome, sobrenomes, endereço, e-mail, fax, telefone, ID/passaporte, assinatura) Detalhes de características pessoais (estado civil, informações familiares, data de nascimento, local de nascimento, idade, sexo, nacionalidade, língua materna) Dados de saúde Detalhes das circunstâncias sociais (informações de moradia, propriedades, hobbies, associações a que pertence, licenças e autorizações) Dados acadêmicos e profissionais (currículo e experiência profissional, qualificações, detalhes do cargo) Detalhes econômicos/financeiros/de seguros (dados econômicos da folha de pagamento, rendimentos, dados bancários; informações fiscais, seguros, planos de aposentadoria) Dados de transação de bens e serviços (bens e serviços recebidos pelo Titular dos Dados, transações financeiras) Dados sobre infrações e infrações administrativas Dados sobre atas da diretoria da empresa, procurações e contratos	Prestação de serviços de informática entre as empresas do Grupo PROSEGUR: (i) suporte e manutenção de TI; (ii) ferramentas/sistemas digitais globais; (iii) gerenciamento de incidentes técnicos a diferentes áreas e negócios. Prestação de serviços de gerenciamento de relacionamento com funcionários e RH entre as empresas do Grupo PROSEGUR: (i) Gerenciamento de Folha de Pagamento; (ii) Prevenção de riscos ocupacionais Tarefas de gerenciamento de equipes realizadas pelos gerentes relacionadas a pessoas sob sua responsabilidade, como apoiar o recrutamento, a formação, a avaliação de desempenho e a promoção Página da web para encontrar informações da Prosegur sobre notícias, lista telefônica, dados organizacionais e informações da empresa Criação de um identificador exclusivo para acesso à rede Prosegur Administração de expatriados Auditoria (avaliação de controles internos) Administração de canal de denúncia Gerenciamento de frotas Processos contábeis, fiscais e financeiros Contratos e administração jurídica Gerenciamento de riscos Conformidade com obrigações legais (ex. solicitação da Autoridade Tributária para reter uma quantia em dinheiro de um funcionário para pagar uma multa de trânsito)

		Avaliar o custo contencioso ou trabalhista da empresa para vender Gerenciamento/conformidade de direitos e obrigações de proteção de dados (por exemplo, solicitações/reclamações do Titular dos Dados)
Candidatos	Dados de identificação e de contato, características pessoais, situação social, acadêmica e profissional, vínculo empregatício, dados econômicos e financeiros	Processos de recrutamento Prestação de serviços de informática entre as empresas do Grupo PROSEGUR:(i) suporte técnico; (ii) gerenciamento de incidentes técnicos de ferramentas/sistemas digitais globais. Gerenciamento/conformidade de direitos e obrigações de proteção de dados (por exemplo, solicitações/reclamações do Titular dos Dados)
Fornecedores e seus representantes ou pessoas de contato	Dados de identificação e contato, dados acadêmicos e profissionais, trabalhistas, econômicos e financeiros, transações de bens e serviços, infrações	Gestão de relacionamento com fornecedores, incluindo contabilidade/fiscal/legal Auditoria (avaliação de controles internos) Administração de canal de denúncia Prestação de serviços de informática entre as empresas do Grupo PROSEGUR: (i) suporte técnico; (ii) ferramentas/sistemas digitais globais; gerenciamento de incidentes técnicos para diferentes áreas e negócios. Conformidade com obrigações legais (ex. solicitação das Autoridades Fiscais) Gerenciamento de contratos Gerenciamento da cadeia de suprimentos e compras Criação de um identificador exclusivo para acesso à rede Prosegur e proteção da rede Prosegur Gerenciamento/conformidade de direitos e obrigações de proteção de dados (por exemplo, solicitações/reclamações do Titular dos Dados)

Usuários, clientes, clientes em potencial e representantes ou pessoas de contato de clientes e clientes em potencial	Dados de identificação e contato, profissionais, trabalhistas, econômicos e financeiros, transações de bens e serviços, infrações	Prestação de serviços de informática entre as empresas do Grupo PROSEGUR: (i) suporte técnico; (ii) ferramentas/sistemas digitais globais; gerenciamento de incidentes técnicos para diferentes áreas e negócios. Prestação de serviços comerciais entre as empresas do Grupo PROSEGUR, incluindo visitas comerciais, ações de fidelização, publicidade e prospecção comercial, atendimento ao cliente e administração de sinistros. Prestação de serviços entre as empresas do Grupo PROSEGUR para o negócio Gelt: prestação de serviços de análise de dados e administração de bancos de dados Gestão de relacionamento com o cliente, incluindo contabilidade/fiscal/legal Prestação de Serviços a Clientes Auditoria (avaliação de controles internos) Administração de canal de denúncia Prevenção à lavagem de dinheiro Conformidade com obrigações legais (ex. solicitação das Autoridades Fiscais) Gerenciamento de contratos Gerenciamento/conformidade de direitos e obrigações de proteção de dados (por exemplo, solicitações/reclamações do Titular dos Dados)
Inquilinos e proprietários	Dados de identificação e contato, acadêmicos e profissionais, dados trabalhistas, informações comerciais	Administração de propriedades Gerenciamento de contratos
Representantes das empresas-alvo, pessoas de contato e funcionários	Dados de identificação e contato, características pessoais, acadêmicas e profissionais, vínculo empregatício, dados econômicos e financeiros	Avaliar o custo contencioso ou trabalhista da empresa para comprar Administração de sinistros
Beneficiários (incluindo menores)	Dados de identificação e contato, características pessoais, dados de saúde, acadêmicos e profissionais, vínculo empregatício, dados econômicos e financeiros	Prestação de serviços de informática entre as empresas do Grupo PROSEGUR: (i) suporte técnico; (ii) ferramentas/sistemas digitais globais; gestão de

		incidentes técnicos para o sistema da Fundação.

4. Finalidade

- Na estrutura das relações comerciais entre as diversas entidades que integram o Grupo PROSEGUR, a PROSEGUR assume o firme compromisso de cumprir e respeitar as leis de privacidade e a proteção dos Dados Pessoais processados no âmbito das suas atividades, visando principalmente proteger os direitos e liberdades essenciais das pessoas físicas, em particular seu direito à privacidade e à confidencialidade.

- Para cumprir este compromisso e suas obrigações de proteção de dados, a PROSEGUR estabeleceu estas Regras Corporativas Vinculativas (doravante, as "RCVs") como parte integrante do Acordo RCV, que visa regular os IDTs que possam ocorrer nas entidades sob seu escopo e que estão especificados no Anexo 1 destas RCVs.

5. Versão pública

Este documento é a versão pública das RCVs a ser publicado nos sites das Entidades RCV e disponibilizado a qualquer pessoa que o solicite.

6. Implementação

6.1. Princípios de processamento de Dados Pessoais

6.1.1. Princípios aplicáveis ao Processamento de Dados Pessoais

- O Processamento de Dados Pessoais deve ser feito de acordo com os seguintes princípios:

6.1.1.1 Princípio da legalidade

- O processamento de Dados Pessoais deve ser lícito. O processamento só é lícito se e na medida em que pelo menos uma destas condições for aplicável:

  a) Os Titulares dos Dados consentirem com o Processamento dos seus Dados Pessoais para uma ou mais finalidades específicas.

  b) O processamento for necessário para executar um contrato do qual o Titular dos Dados faça parte, ou para diligências solicitadas pelo Titular dos Dados antes da celebração de um contrato;

  c) O processamento for necessário para cumprir uma obrigação legal a que o Controlador esteja sujeito.

  d) O processamento for necessário para proteger os interesses vitais do Titular dos Dados ou de outra pessoa física;

e) O processamento for necessário para desempenhar uma tarefa no interesse público ou no exercício da autoridade oficial investida no Controlador;

f) O processamento for necessário para efeitos dos interesses legítimos pretendidos pelo Controlador ou por um terceiro, exceto quando esses interesses forem substituídos pelos interesses ou direitos e liberdades essenciais do Titular dos Dados que exijam a Proteção de Dados Pessoais, particularmente quando o Titular dos Dados for uma criança.

6.1.1.2 Justiça e transparência

- O Processamento de Dados Pessoais deve ser feito de maneira justa e transparente para os Titulares dos Dados. Os Titulares dos Dados devem ser informados das circunstâncias relacionadas ao Processamento dos seus Dados Pessoais de forma acessível e compreensível, com linguagem clara e simples, de acordo com o disposto na Lei Europeia de Proteção de Dados.

6.1.1.3 Princípio da limitação da finalidade

- Os Dados Pessoais devem ser processados para fins especificados, explícitos e legítimos e jamais de forma incompatível com esses fins.

6.1.1.4 Princípio de minimização de dados

- Dados Pessoais que devem ser adequados, relevantes e limitados ao necessário para os fins para aos quais são coletados. A minimização de dados deve ser aplicada levando em conta a quantidade de dados coletados, o escopo do seu processamento e o seu período de retenção. O Acesso aos Dados também deve ser minimizado, de forma que somente o Pessoal ou Destinatários que precisam conhecê-los para cumprir suas obrigações possam acessá-los ("base de necessidade de conhecimento").

6.1.1.5 Princípio da precisão

- Os Dados Pessoais processados devem ser precisos e, caso necessário, atualizados. Serão tomadas todas as medidas razoáveis para garantir que os Dados Pessoais que sejam inexatos, levando em conta as finalidades para as quais foram processados, sejam apagados o mais rápido possível.

6.1.1.6 Princípio de limitação de armazenamento

- Os Dados Pessoais devem ser guardados de forma que permita a identificação dos Titulares dos Dados por um período não superior ao necessário para os fins para aos quais os Dados Pessoais são processados.

6.1.1.7 Princípio de integridade e confidencialidade

- Os Dados Pessoais devem ser processados de forma a garantir a segurança apropriada dos Dados Pessoais, incluindo proteção contra Processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, aplicando medidas técnicas ou organizacionais apropriadas.

6.1.1.8 Princípio de responsabilidade

- As Entidades RCV devem ser responsáveis e capazes de demonstrar o cumprimento de todos os princípios, direitos e obrigações previstos nestas RCVs. Elas também são responsáveis e capazes demonstrar o cumprimento desses princípios, direitos e obrigações.

6.1.1.9 Proteção de Dados desde a concepção e por padrão

- Tendo em conta a modernidade, o custo de implementação e a natureza, o escopo, o contexto e as finalidades do Processamento, bem como os riscos de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas físicas apresentados pelo Processamento, as Entidades RCV devem, tanto no momento de determinar os meios de Processamento quanto como no momento do Processamento em si, implementar medidas técnicas e organizacionais adequadas, como a pseudonimização, que visam implementar os princípios de Proteção de Dados, como a minimização de dados, de forma eficaz e para integrar as salvaguardas necessárias ao Processamento, a fim de cumprir os requisitos das Leis Europeias de Proteção de Dados e proteger os direitos dos Titulares dos Dados.

- O Processamento deve, desde o início, incorporar as medidas técnicas e organizacionais que permitam a aplicação efetiva dos princípios estabelecidos nas Leis Europeias de Proteção de Dados, o cumprimento dos seus requisitos e a proteção dos direitos dos Titulares dos Dados.

- Devem ser implementadas medidas para garantir que, por padrão, somente os Dados Pessoais necessários para cada fim específico da atividade de Processamento sejam efetivamente processados. A obrigação de implementar essas medidas aplica-se à quantidade de Dados Pessoais coletados, à extensão do seu Processamento, ao período do seu armazenamento e à sua acessibilidade. Especificamente, as medidas devem garantir que, por padrão, os Dados Pessoais não sejam acessíveis, sem a intervenção do indivíduo, a um número indefinido de pessoas.

- Ou seja, desde a concepção de um novo projeto, sistema, ferramenta ou processo em que esteja previsto o Processamento de Dados Pessoais, as Entidades RCV levarão em conta a Proteção dos Dados Pessoais, adotando decisões e implementando medidas que garantam a conformidade com as Leis Europeias de Proteção de Dados e restrinjam o Processamento de Dados Pessoais ao que for estritamente necessário.

6.1.2. Processamento de categorias especiais de Dados Pessoais

- O processamento de Categorias Especiais de Dados Pessoais é proibido, a menos que se aplique uma destas situações:

  a) O Titular dos Dados tenha consentido explicitamente com o Processamento desses Dados Pessoais para um ou mais fins específicos, exceto quando a Lei Europeia estabelecer que a proibição de Processamento desses Dados não possa ser levantada pelo Titular dos Dados;

  b) O processamento for necessário para cumprir obrigações e exercício de direitos específicos do Controlador ou do Titular dos Dados no campo da legislação trabalhista, previdenciária e de proteção social, conforme estabelecido na Lei Europeia ou em um

acordo coletivo conforme as Leis Europeias que preveem as devidas salvaguardas dos direitos fundamentais e dos interesses do Titular dos Dados;

c) O Processamento for necessário para proteger os interesses vitais do Titular dos Dados ou de outra pessoa física quando o Titular dos Dados estiver física ou legalmente incapaz de dar o seu consentimento;

d) O Processamento for feito no decurso das suas atividades legítimas com as devidas salvaguardas por uma fundação, associação ou qualquer outra organização sem fins lucrativos com objetivo político, filosófico, religioso ou sindical e na condição de o Processamento se referir exclusivamente aos membros atuais ou anteriores da organização ou a pessoas que tenham contato regular com a organização no âmbito das suas finalidades e que os Dados Pessoais não sejam divulgados fora dessa organização sem o consentimento dos Titulares dos Dados;

e) O Processamento for relacionado a Dados Pessoais que tenham sido tornados públicos manifestamente pelo Titular dos Dados;

f) O Processamento for necessário para a instauração, exercício ou defesa de ações e/ou reclamações legais ou sempre que os tribunais estejam atuando em sua capacidade judicial;

g) O Processamento for necessário por motivos de interesse público substancial, com base em leis europeias que devem ser proporcionais ao objetivo pretendido, respeitar a essência do direito à proteção dos dados e prever medidas adequadas e específicas para salvaguardar os direitos fundamentais e os interesses do Titular dos Dados;

h) O Processamento for necessário para fins de medicina preventiva ou ocupacional e/ou avaliação da capacidade de trabalho do funcionário, diagnóstico médico, prestação de assistência ou tratamento de saúde ou social ou administração de sistemas e serviços de saúde ou assistência social, com base em de Leis Europeias ou de acordo com um contrato com um profissional de saúde e quando os Dados Pessoais forem processados por ou sob a responsabilidade de um profissional ou por qualquer outra pessoa sujeita a sigilo profissional de acordo com a Lei Europeia ou normas estabelecidas pelas organizações nacionais competentes;

i) O Processamento for necessário por motivos de interesse público no campo da saúde pública, como proteção contra ameaças transfronteiriças graves à saúde ou garantia de altos padrões de qualidade e segurança de cuidados de saúde e de medicamentos ou dispositivos médicos, com base nas Leis Europeias que preveem medidas apropriadas e específicas para proteger os direitos e liberdades do Titular dos Dados, especialmente o sigilo profissional;

j) O Processamento for necessário para fins de arquivamento de interesse público, fins de pesquisa científica ou histórica ou fins estatísticos com base nas Leis Europeias que devem ser proporcionais ao objetivo pretendido, respeitar a essência do direito à Proteção de Dados e prever medidas adequadas e específicas para salvaguardar os direitos fundamentais e os interesses do Titular dos Dados.

6.1.3. Medidas para garantir a segurança dos dados

- As Entidades RCV implementarão e aplicarão as medidas técnicas e organizacionais adequadas para garantir um nível de segurança apropriado, levando em conta modernidade, os custos de implementação, a natureza, âmbito, contexto e finalidades do Processamento, bem como os riscos a que o Processamento está exposto e o possível impacto sobre os direitos e liberdades das pessoas físicas, seja decorrente da ação humana ou do ambiente físico ou natural.

- As medidas que devem ser implementadas incluem, sem limitação, as seguintes:

  a) pseudonimização e criptografia dos Dados Pessoais;

  b) capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços de Processamento;

  c) capacidade de restaurar a disponibilidade e o acesso aos Dados Pessoais rapidamente em caso de incidentes físicos ou técnicos;

  d) verificação regular, avaliação e análise da eficácia das medidas técnicas e organizacionais para garantir a segurança do Processamento.

- As Entidades RCV também devem tomar medidas para garantir que qualquer pessoa que atue sob sua responsabilidade que tenha acesso a Dados Pessoais só possa processar tais Dados Pessoais sob as instruções do Controlador, a menos que seja obrigada a fazê-lo ao abrigo das Leis Europeias.

- Ao avaliar o nível adequado de segurança, deve-se levar em consideração, especificamente, os riscos apresentados pelo Processamento, em particular de destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a Dados Pessoais Transmitidos, armazenados ou processados de outra forma.

- A Política de Segurança da Informação do Grupo PROSEGUR, constante do Anexo 3, constitui a estrutura para a definição, gerenciamento, administração e implementação dos mecanismos e procedimentos necessários para estabelecer níveis de segurança adequados para os ativos de informação do Grupo PROSEGUR e seus clientes.

6.1.4. Modelo de Conformidade e Governança de Proteção de Dados

- As Entidades RCV designarão um Diretor de Proteção de Dados quando: (i) suas atividades principais consistirem em operações de Processamento que, por sua natureza, âmbito e/ou finalidades, exijam um acompanhamento regular e sistemático dos Titulares dos Dados em grande escala; ou (ii) suas atividades principais consistirem no Processamento em grande escala de Categorias Especiais de Dados de acordo com a Cláusula 6.1.2 ou Dados Pessoais relacionados a condenações e infrações criminais.

- Os Diretores de Proteção de Dados terão, pelo menos, estas funções:

  a) para informar e orientar as Entidades RCV e o Pessoal que executam o Processamento de suas obrigações de acordo com estas RCVs e com as disposições de proteção de Dados da Lei Europeia ou do Estado Membro;

b) Para monitorar o cumprimento destas RCVs, com as disposições de proteção de Dados e com as políticas das Entidades da RCV sobre a proteção de Dados Pessoais, incluindo a atribuição de responsabilidades, conscientização e formação do Pessoal envolvido nas operações de Processamento e as auditorias relacionadas;

c) prestar orientações, sempre que solicitado, no que diz respeito à Avaliação de Impacto da Proteção de Dados e monitorar seu desempenho de acordo com a Cláusula 6.1.8;

d) cooperar com a Autoridade de Supervisão;

e) Para atuar como o ponto de contato para a Autoridade de Supervisão sobre questões relacionadas ao Processamento, incluindo a consulta prévia nos termos das Leis Europeias, e consultar, quando apropriado, sobre qualquer outro assunto.

- A PROSEGUR nomeou (i) um Diretor de Proteção de Dados corporativo ao nível do Grupo PROSEGUR ("Group Data Protection Officer") com a responsabilidade, entre outras, de fiscalizar o cumprimento das RCVs tendo o mais alto apoio da administração para realizar esta tarefa; e (ii) Diretores de Proteção de Dados locais nos países do Espaço Econômico Europeu em que o Grupo PROSEGUR está presente, bem como no Brasil e no Uruguai [“Local Data Protection Officers”]. Os Diretores de Proteção de Dados Locais e do Grupo responderão diretamente ao mais alto nível administrativo das Entidades RCV.

- A PROSEGUR também nomeou Diretores Locais de Conformidade nos países onde um Diretor Local de Proteção de Dados não é obrigatório de acordo com esta cláusula ou a lei local. Esses Diretores de Conformidade Local são responsáveis pela Proteção de Dados em nível local, atuam como contatos e gerentes para tratar de questões de Proteção de Dados (incluindo, sem limitação, reclamações relacionadas a RCVs) em nível local, respondendo às equipes de gerenciamento local e ao Diretor de Proteção de Dados do Grupo.

- Tanto os Diretores de Proteção de Dados quanto os Diretores de Conformidade Local fazem parte e recebem o apoio do (i) Comitê de Proteção de Dados Corporativos; (ii) Comitê de Privacidade (Executivo); (iii) Responsável pelo Processamento Funcional; e (iv) Testadores de Controle, conforme estabelecido no Modelo de Conformidade e Governança de Proteção de Dados.

- O Anexo 4 fornece informações sobre a estrutura do Modelo de Conformidade e Governança de Proteção de Dados no Grupo PROSEGUR, bem como as responsabilidades das equipes.

6.1.5. Processadores e Subprocessadores de Dados

- Quando uma Entidade RCV que atue como Controlador quiser terceirizar a prestação de serviços a um Processador (seja uma Entidade RCV ou não), ela deverá, em primeira instância, usar somente Processadores de Dados que forneçam garantias suficientes para implementar medidas técnicas e organizacionais apropriadas de forma que o Processamento cumpra os requisitos das RCVs e garanta a proteção dos direitos dos Titulares dos Dados. O mesmo se aplica quando uma Entidade RCV que atue como um Processador queira contratar um subprocessador, seja uma Entidade RCV ou não (doravante, "Subprocessador(es) de Dados" ou "Subprocessador(es)").

- Esse Processamento pelo Processador, em nome do Controlador, será regido por um contrato ou outro ato legal sob as Leis Europeias, que vincula o Processador ao Controlador e que define o assunto e a duração do Processamento, a natureza e a finalidade do Processamento, o tipo de Dados Pessoais e as categorias de Titulares dos Dados e as obrigações e direitos do Controlador ("Contrato do Processador de Dados"). O Acordo do Processador de Dados, que

pode ser baseado, no todo ou em parte, em Cláusulas Contratuais Padrão, estipulará, especificamente, que o Processador:

a) Processe os Dados Pessoais somente mediante instruções documentadas do Controlador, inclusive no que diz respeito a transferências de Dados Pessoais a um Terceiro País ou uma organização internacional, a menos que seja exigido por lei à qual o Processador esteja sujeito; nesse caso, o Processador informará o Controlador sobre esse requisito legal antes do Processamento, a menos que a lei proíba essas informações por motivos importantes de interesse público;

b) garanta que as pessoas autorizadas a processar os Dados Pessoais tenham se comprometido com a confidencialidade ou estejam sob uma obrigação legal apropriada de confidencialidade;

c) tome todas as providências exigidas nos termos da Cláusula 6.1.3;

d) respeite estas condições: (i) O Processador não deve contratar outro Processador sem autorização prévia escrita específica ou geral por parte do Controlador. No caso de uma autorização geral escrita, o Processador deve informar o Controlador sobre quaisquer alterações pretendidas relacionadas à adição ou substituição de outros Processadores, dando assim ao Controlador a oportunidade de se opor a tais alterações; e (ii) quando um Processador contratar outro Processador para executar atividades de processamento específicas em nome do Controlador, as mesmas obrigações de proteção de dados estabelecidas no Contrato do Processador de Dados entre o Controlador e o Processador serão impostas a esse outro Processador por meio de um contrato ou outro ato legal sob a lei, fornecendo especificamente garantias suficientes para aplicar medidas técnicas e organizacionais adequadas de forma que o Processamento cumpra os requisitos destas RCVs. Quando esse outro Processador não cumprir suas obrigações de Proteção de Dados, o Processador inicial permanecerá totalmente responsável perante o Controlador por cumprir as obrigações desse outro Processador.

e) tendo em conta a natureza do Processamento, auxilia o Controlador aplicando medidas técnicas e organizacionais adequadas, na medida do possível, para cumprir a obrigação do Controlador de responder a solicitações para exercitar os direitos do Titular dos Dados previstos na Cláusula 6.3;

f) auxilia o Controlador em cumprir as obrigações previstas nas Cláusulas 6.1.3. e 6.1.6 a 6.1.8. tendo em conta a natureza do Processamento e as informações disponíveis para o Processador;

g) à escolha do Controlador, exclui ou devolve todos os Dados Pessoais ao Controlador após o término da prestação de serviços relacionados ao Processamento e exclui as cópias existentes, a menos que a lei exija o armazenamento dos Dados Pessoais;

h) disponibiliza ao Controlador todas as informações necessárias para demonstrar conformidade com as obrigações previstas nesta Cláusula e permite e contribui para auditorias, inclusive inspeções, feitas pelo Controlador ou outro auditor por ele designado.

i) o Processador informará imediatamente o Controlador se, em sua opinião, uma instrução violar estas RCVs ou quaisquer disposições de Proteção de Dados das Leis Europeias.

- Caso uma Entidade RCV queira subcontratar ao Subprocessador a totalidade ou parte dos serviços que lhe foram contratados, a Entidade RCV deverá obter autorização prévia por escrito, específica ou geral, do Controlador de Dados. Quando for autorizado pelos representantes do Controlador de Dados a usar outro Processador de Dados, o Subprocessador estará contratualmente vinculado a, pelo menos, as mesmas obrigações estipuladas no Contrato do Processador de Dados, segundo as disposições destas RCVs.

- O Processador de Dados é responsável perante o Controlador de Dados e será responsável por cumprir efetivamente as obrigações de Proteção de Dados pelo Subprocessador.

- O Processador de Dados compromete-se a notificar o Controlador de Dados, com antecedência e por meios certificáveis, sobre possíveis alterações planejadas em termos de adição ou substituição de Processadores de Dados, dando ao Controlador de Dados a oportunidade de se opor a tais alterações.

- Para os efeitos anteriores, as Entidades RCV devem observar e cumprir a Política do Grupo PROSEGUR para Seleção e Avaliação de Fornecedores, constante do Anexo 5. As disposições da Cláusula 6.2 destas RCVs também devem ser observadas.

6.1.6. Violações de Dados Pessoais

- Caso ocorra, ou se suspeite que tenha ocorrido, uma violação de segurança que possa afetar os Dados Pessoais, a pessoa que a detectar isso deverá informar imediatamente o Diretor de Proteção de Dados Local/Diretor de Conformidade Local e este informará imediatamente a PROSEGUR (através do Diretor de Proteção de Dados do Grupo), de acordo com o Protocolo de Gerenciamento e Notificação de Violação de Dados Pessoais, constante como Anexo 6.

- Entre outras obrigações, deve haver um registro escrito documentando os fatos relacionados à Violação de Dados Pessoais, seus efeitos e as medidas corretivas tomadas de todas as Violações de Dados Pessoais e deve ser disponibilizado à(s) Autoridade(s) de Supervisão competentes, mediante solicitação.

- As Entidades RCVs que atuam como Controladoras de Dados devem notificar a Autoridade de Supervisão competente sobre quaisquer Violações de Dados Pessoais, a menos que seja improvável que tais violações representem risco aos direitos e liberdades dos Titulares dos Dados. A notificação deve ser feita sem atraso indevido e, se possível, dentro de 72 horas após o Controlador de Dados tomar conhecimento sobre a Violação de Dados Pessoais. Os Titulares dos Dados também devem ser informados, sem atraso indevido, quando for provável que a Violação de Dados Pessoais resulte em alto risco aos seus direitos e liberdades.

- Quando uma Entidade RCV que atue como Subcontratante estiver envolvida em uma Violação de Dados Pessoais, tal Entidade deverá informar imediatamente a PROSEGUR (por meio do Diretor da Proteção de Dados do Grupo), que é responsável por notificar a Entidade RCV na qualidade de Controlador de Dados, sem atraso indevido, para que sejam feitas as notificações exigidas pelas presentes RCV, se aplicável.

6.1.7. Registro das atividades de Processamento

- As Entidades RCVs que atuam como Controladores devem manter, por escrito (incluindo, sem limitação, um formulário eletrônico), um Registro das Atividades de Processamento (RoPA, Record of the Processing Activities) de Dados Pessoais realizados sob sua responsabilidade, e mantê-lo atualizado e ser fornecido às Autoridades de Supervisão, mediante solicitação. O RoPA deve conter estas informações:

a) O nome e detalhes de contato do Controlador, quando aplicável, o Controlador adjunto, o representante do Controlador e o Diretor de Proteção de Dados Local ou do Grupo;

b) as finalidades do Processamento;

c) uma descrição das categorias de Titulares dos Dados e as categorias de Dados Pessoais;

d) As categorias de Destinatários a quem os Dados Pessoais foram ou serão divulgados, incluindo Destinatários em Terceiros Países e organizações internacionais;

e) Quando aplicável, transferências de Dados Pessoais a um Terceiro País ou uma organização internacional, incluindo a identificação do Terceiro País ou organização internacional que seja o Destinatário dos Dados e, quando aplicável, a documentação das salvaguardas adequadas;

f) sempre que possível, os prazos previstos para a exclusão das diferentes categorias de Dados;

g) sempre que possível, uma descrição geral das medidas de segurança técnicas e organizacionais mencionadas na Cláusula 6.1.3 destas RCVs.

- As Entidades RCVs que atuam como Processadores e, quando aplicável, o representante do Processador devem manter um RoPA de todas as categorias de atividades de Processamento realizadas em nome de um Controlador, contendo:

a) o nome e detalhes de contato do Processador ou Processadores e de cada Controlador em nome do qual o Processador está atuando e, quando aplicável, do Controlador ou representante do Processador e do Diretor de Proteção de Dados Local ou do Grupo;

b) as categorias de Processamento executadas em nome de cada Controlador;

c) quando aplicável, transferências de Dados Pessoais para um Terceiro País ou uma organização internacional, incluindo a identificação desse Terceiro País ou organização internacional e, no caso de transferências mencionadas no segundo parágrafo da Cláusula 6.2.1 destas RCVs, a documentação de salvaguardas adequadas;

d) sempre que possível, uma descrição geral das medidas de segurança técnicas e organizacionais mencionadas na Cláusula 6.1.3 destas RCVs.

6.1.8. Avaliações do Impacto da Proteção de Dados

- As Entidades RCV devem fazer uma Avaliação do Impacto da Proteção de Dados (doravante, "DPIA" ou Data Protection Impact Assessment na sigla em inglês) antes de iniciar o

Processamento de Dados Pessoais, sempre que um determinado tipo de Processamento envolver um alto risco aos direitos e liberdades dos Titulares dos Dados.

- Essas avaliações serão elaboradas de acordo com a metodologia estabelecida pelo Grupo PROSEGUR, com a orientação do Grupo ou do Diretor Local de Proteção de Dados, quando nomeado. O objetivo é avaliar a necessidade e proporcionalidade do Processamento, identificar os riscos e estabelecer as medidas necessárias para mitigá-los.

- Para este fim, as Entidades RCV devem observar e cumprir o Protocolo de Gerenciamento de DPIA do Grupo PROSEGUR, constante no Anexo 7.

- Sempre que, após a realização de um DPIA, uma Entidade RCV identificar um alto risco que não possa ser mitigado, tal Entidade deve consultar a Autoridade de Supervisão relevante antes de realizar o Processamento pretendido.

6.2. Requisitos para divulgar Dados Pessoais

6.2.1. Transferências Internacionais de Dados

- Os Dados Pessoais não podem ser transferidos para fora do EEE se estes requisitos não forem cumpridos:

    a) o Importador de Dados estiver sujeito e puder cumprir essas RCVs. A título de esclarecimento, estas RCVs são apenas aplicáveis a IDTs entre entidades do Grupo PROSEGUR que a elas tenham aderido; e/ou

    b) a Comissão Europeia tiver decidido que o Terceiro País onde o Importador de Dados está localizado garante um nível adequado de proteção; ou

    c) se o país onde o Importador de Dados está localizado não tiver um nível adequado de proteção de acordo com uma decisão de adequação da Comissão Europeia, as Entidades RCV devem tomar as devidas salvaguardas, e na condição de que os direitos pertinentes dos Titulares dos Dados e recursos legais efetivos para os Titulares dos Dados estejam disponíveis. Serão consideradas salvaguardas adequadas os seguintes mecanismos:

        i. Cláusulas contratuais padrão

        ii. Código de conduta aprovado de acordo com o RGPD, juntamente com compromissos vinculativos e exequíveis do Controlador ou Processador no Terceiro País para aplicar as salvaguardas adequadas, inclusive no que diz respeito aos direitos dos Titulares dos Dados

        iii. Mecanismo de certificação aprovado de acordo com o RGPD, juntamente com compromissos vinculativos e exequíveis do Controlador ou Processador no Terceiro País para aplicar as salvaguardas adequadas, inclusive no que diz respeito aos direitos dos Titulares dos Dados

iv. Instrumento juridicamente vinculativo e executável entre as autoridades ou órgãos públicos.

- Se nenhum desses requisitos for cumprido, uma transferência ou um conjunto de transferências de Dados Pessoais fora do EEE ocorrerá somente em uma das seguintes condições:

a) a transferência foi autorizada previamente pela Autoridade de Supervisão competente com base na implementação de salvaguardas apropriadas por cláusulas contratuais entre o Controlador ou Processador e o Controlador, Processador ou Destinatário dos Dados Pessoais no Terceiro País ou organização internacional.

b) houver um julgamento de um tribunal ou uma decisão de uma autoridade administrativa de um Terceiro País exigindo que o Controlador ou o Processador transfira ou divulgue Dados Pessoais com base em um acordo internacional, como um tratado de assistência jurídica mútua, estabelecida entre o solicitante a um Terceiro País e à União Europeia ou a um Estado Membro;

c) o Titular dos Dados tenha consentido explicitamente com a transferência proposta, depois de ter sido informado dos possíveis riscos de tais transferências para o Titular dos Dados devido à ausência de uma decisão de adequação e salvaguardas adequadas;

d) a transferência for necessária (i) para executar um contrato entre o Titular dos Dados e o Controlador ou a implementação de medidas pré-contratuais tomadas mediante solicitação do Titular dos Dados; (ii) para celebrar ou executar um contrato celebrado no interesse do Titular dos Dados entre o Controlador e outra pessoa física ou coletiva; (iii) por motivos importantes de interesse público reconhecidos pela legislação da União Europeia ou de um Estado Membro; (iv) a declaração, exercício ou defesa de ações judiciais; ou (v) para proteger interesses vitais do Titular dos Dados ou de outras pessoas, quando o Titular dos Dados estiver física ou legalmente incapaz de dar o seu consentimento;

e) somente se a transferência (i) não for repetitiva, (ii) for relacionada somente a um número limitado de Titulares dos Dados, (iii) for necessária para efeitos de fazer cumprir interesses legítimos envidados pelo Controlador que não sejam anulados pelos interesses ou direitos e liberdades do Titular dos Dados, e (iv) o Controlador tiver avaliado todas as circunstâncias envolvendo a transferência de dados e, com base nessa avaliação, tiver fornecido salvaguardas adequadas em relação à proteção de Dados Pessoais. Neste caso, o Controlador deve informar a Autoridade de Supervisão da transferência. O Controlador deverá, para além da prestação das informações mencionadas na Cláusula 6.3.1, informar o Titular dos Dados sobre a transferência e os interesses legítimos irrefutáveis pretendidos.

6.2.2. Transferências subsequentes

6.2.2.1 Quando o Destinatário for uma Entidade RCV

Em geral, os requisitos estabelecidos na Cláusula **6**.**2**.1 acima devem ser cumpridos e observados. Em caso de dúvida, o Importador dos Dados deve informar o Exportador de Dados e obter sua autorização expressa.

6.2.2.2 Quando o Destinatário não for uma entidade RCV

O Importador de Dados deve informar o Exportador de Dados, verificar se qualquer um dos mecanismos e/ou derrogações contidos na seção 5.8.4 do Anexo 5 deste documento é aplicável à Transferência Subsequente e obter a autorização do Exportador de Dados.

6.2.3. Relacionamentos do Processador de Dados

Quando as divulgações de dados forem baseadas em um relacionamento do Processador de Dados, esse relacionamento deve ser executado por escrito, com base no Modelo de Contrato do Processador de Dados do Grupo PROSEGUR e levando em consideração a Política sobre Seleção e avaliação de fornecedores, constante como Anexo 5.

6.3. Direitos dos Titulares dos Dados

6.3.1. Informações:

- Os Controladores de Dados são obrigados a fornecer informações aos Titulares dos Dados, conforme aqui detalhado:

a) Quando os Dados Pessoais são coletados do Titular dos Dados, no momento da coleta dos Dados Pessoais, os Titulares dos Dados devem receber todas estas informações:

(i) a identidade e detalhes de contato do Controlador e, quando aplicável, do representante do Controlador;

(ii) os detalhes de contato do Diretor de Proteção de Dados, quando aplicável;

(iii) as finalidades do Processamento a que se destinam os Dados Pessoais, bem como a base legal do Processamento;

(iv) quando o Processamento for baseado em interesses legítimos, os interesses legítimos pretendidos pelo Controlador ou por um Terceiro;

(v) os Destinatários ou categorias de Destinatários dos Dados Pessoais, se houver;

(vi) quando pertinente, o fato de o Controlador pretender transferir os Dados Pessoais para um Terceiro País ou organização internacional e a existência ou ausência de decisão de adequação ou a referência às salvaguardas apropriadas ou salvaguardas adequadas e os meios para obter uma cópia dos mesmos ou onde tiverem sido disponibilizados.

Além das informações acima, o Controlador deverá, no momento da coleta dos Dados Pessoais, fornecer ao Titular dos Dados as seguintes informações adicionais necessárias para garantir um Processamento justo e transparente:

(i) o período durante o qual os Dados Pessoais serão armazenados, ou se isso não for possível, os critérios usados para determinar esse período;

(ii) a existência do direito de solicitar ao Controlador o acesso e retificação ou a exclusão dos Dados Pessoais ou restrição do Processamento em relação ao Titular dos Dados ou de se opor ao Processamento, bem como o direito à portabilidade dos dados;

(iii) quando o Processamento tiver como base o consentimento do Titular dos Dados, a existência do direito de retirar o consentimento a qualquer momento, sem prejuízo da licitude do Processamento baseado no consentimento anterior à sua retirada;

(iv) o direito de registrar reclamação a uma Autoridade de Supervisão;

(v) se o fornecimento de Dados Pessoais for um requisito legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o Titular dos Dados tiver obrigação de fornecer os Dados Pessoais e as possíveis consequências de não fornecer tais Dados Pessoais;

(vi) quando pertinente, a existência de tomada de decisão automatizada, incluindo a criação de perfis e, pelo menos nesses casos, informações significativas sobre a lógica envolvida, bem como o significado e as consequências esperadas de tal Processamento para o Titular dos Dados.

Quando o Controlador pretender processar os Dados Pessoais para uma finalidade diferente daquela para a qual os Dados Pessoais foram coletados, o Controlador deve fornecer ao Titular dos Dados, antes desse processamento adicional, informações sobre essa outra finalidade e outras informações relevantes conforme mencionado acima.

b) Quando os Dados Pessoais não tiverem sido obtidos do Titular dos Dados, o Controlador fornecerá ao Titular dos Dados estas informações:

(i) a identidade e os detalhes de contato do Controlador e, quando aplicável, do representante do Controlador;

(ii) os detalhes de contato do Diretor de Proteção de Dados, quando aplicável;

(iii) as finalidades do Processamento a que se destinam os Dados Pessoais, bem como a base legal do Processamento;

(iv) as categorias dos Dados Pessoais em questão;

(v) os Destinatários ou categorias de Destinatários dos Dados Pessoais, se houver;

(vi) quando pertinente, o fato de o Controlador pretender transferir os Dados Pessoais para um Terceiro País ou organização internacional e a existência ou ausência de decisão de adequação ou a referência às salvaguardas apropriadas ou salvaguardas adequadas e os meios para obter uma cópia dos mesmos ou onde tiverem sido disponibilizados.

Além das informações acima, o Controlador deverá, no momento da coleta dos Dados Pessoais, fornecer ao Titular dos Dados as seguintes informações adicionais necessárias para garantir um Processamento justo e transparente:

(i) o período durante o qual os Dados Pessoais serão armazenados, ou se isso não for possível, os critérios usados para determinar esse período;

(ii) quando o Processamento se basear no interesse legítimo do Controlador, nos interesses legítimos pretendidos pelo Controlador ou por um Terceiro;

(iii) a existência do direito de solicitar ao Controlador o acesso e retificação ou a exclusão dos Dados Pessoais ou restrição do Processamento em relação ao Titular dos Dados ou de se opor ao Processamento, bem como o direito à portabilidade dos dados;

(iv) quando o Processamento tiver como base o consentimento do Titular dos Dados, a existência do direito de retirar o consentimento a qualquer momento, sem prejuízo da licitude do Processamento baseado no consentimento anterior à sua retirada;

(v) o direito de registrar reclamação a uma Autoridade de Supervisão;

(vi) de qual fonte os Dados Pessoais se originam e, se pertinente, se eles se originam de fontes disponíveis publicamente;

(vii) a existência de tomada de decisão automatizada, incluindo a criação de perfis e, pelo menos nesses casos, informações significativas sobre a lógica envolvida, bem como o significado e as consequências esperadas de tal Processamento para o Titular dos Dados.

O Controlador deve fornecer as informações mencionadas nos parágrafos acima: (a) dentro de um período razoável após a obtenção dos Dados Pessoais, mas o mais tardar dentro de um mês, levando em conta as circunstâncias específicas em que os Dados Pessoais são processados; (b) se os Dados Pessoais forem usados para comunicação com o Titular dos Dados, o mais tardar no momento da primeira comunicação com esse Titular dos Dados; ou (c) se estiver prevista uma divulgação a outro destinatário, o mais tardar quando os Dados Pessoais forem divulgados pela primeira vez.

Quando o Controlador pretender processar os Dados Pessoais para uma finalidade diferente daquela para a qual os Dados Pessoais foram obtidos, o Controlador deve fornecer ao Titular dos Dados, antes desse processamento adicional, informações sobre essa outra finalidade e outras informações relevantes conforme mencionado no Parágrafo 2 da Cláusula 6.3.1(b).

Os parágrafos anteriores desta Cláusula 6.3.1(b) não se aplicam quando e na medida em que:

(i) o Titular dos Dados já tiver as informações;

(ii) o fornecimento dessas informações se mostrar impossível ou implicar um esforço desproporcional, em particular para Processamento para fins de arquivamento de interesse público, fins de pesquisa científica ou histórica ou fins estatísticos ou na medida em que a obrigação mencionada no primeiro parágrafo desta seção (b) for susceptível de impossibilitar ou prejudicar seriamente a realização dos propósitos de tal Processamento. Nesses casos, o Controlador tomará as medidas adequadas para proteger os direitos e liberdades e interesses legítimos do Titular dos Dados, incluindo a disponibilização pública das informações;

(iii) a coleta ou divulgação estiver expressamente prevista na Legislação Europeia ou dos Estados Membros, a que o Controlador estiver sujeito e que preveja medidas adequadas para proteger os legítimos interesses do Titular dos Dados; ou

(iv) onde os Dados Pessoais devam permanecer confidenciais sujeitos a uma obrigação de sigilo profissional regulamentada pelas Leis Europeias ou dos Estados Membros, incluindo uma obrigação estatutária de sigilo.

6.3.2. Outros direitos

- Os Titulares dos Dados podem exercer estes direitos:

(i) **Acesso**: confirmar se os Dados Pessoais que lhes digam respeito estão ou não sendo processados, e solicitar informações sobre quais Dados Pessoais específicos estão sendo processados e, se for o caso, o acesso aos Dados Pessoais e às seguintes informações:

a) as finalidades do Processamento;
b) as categorias dos Dados Pessoais em questão;
c) os Destinatários ou categorias de Destinatários a quem os Dados Pessoais foram ou serão divulgados, em particular Destinatários em Terceiros Países ou organizações internacionais. Quando os Dados Pessoais forem transferidos a um Terceiro País ou a uma organização internacional, o Titular dos Dados terá o direito de ser informado sobre as salvaguardas apropriadas nos termos da Cláusula 6.2.1. sobre a transferência.
d) quando possível, o período previsto durante o qual os Dados Pessoais serão armazenados, ou, se não for possível, os critérios usados para determinar esse período;
e) A existência do direito de solicitar ao Controlador a retificação ou exclusão dos Dados Pessoais ou a restrição do Processamento dos Dados Pessoais relacionados ao Titular dos Dados ou de se opor a tal Processamento;
f) o direito de registrar reclamação a uma Autoridade de Supervisão;
g) onde os Dados Pessoais não são coletados do Titular dos Dados, qualquer informação disponível sobre a sua fonte;
h) a existência de tomada de decisão automatizada, incluindo a criação de perfis e, pelo menos nesses casos, informações significativas sobre a lógica envolvida, bem como o significado e as consequências previstas de tal Processamento para o Titular dos Dados.

O Controlador deverá fornecer uma cópia dos Dados Pessoais em Processamento. Para quaisquer outras cópias solicitadas pelo Titular dos Dados, o Controlador pode cobrar uma taxa razoável com base nos custos administrativos. Quando o Titular dos Dados solicitar por meio eletrônico, e salvo solicitação em contrário do Titular dos Dados, as informações serão fornecidas em um formulário eletrônico de uso comum.

O direito de adquirir uma cópia não deve prejudicar os direitos e liberdades de terceiros.

(ii) **Retificação**: obter do Controlador, sem demora indevida, a retificação dos Dados Pessoais inexatos que lhes digam respeito. Tendo em conta as finalidades do Processamento, o Titular dos Dados terá direito a que os Dados Pessoais incompletos sejam completados, inclusive mediante a prestação de declaração complementar.

(iii) **Apagamento (direito de ser esquecido)**: O Titular dos Dados terá o direito de obter do Controlador a exclusão dos Dados Pessoais que lhe digam respeito, sem demora indevida, e o Controlador terá a obrigação de excluir os Dados Pessoais, sem demora indevida, quando se aplicar um dos seguintes motivos:

a) os Dados Pessoais não forem mais necessários em relação às finalidades para os quais foram coletados ou Processados de outra forma;
b) o Titular dos Dados retirar o consentimento no qual o Processamento se baseia de acordo com a Cláusula 6.1.1.1., ou Cláusula 6.1.2., e quando não houver outra base legal para o Processamento;
c) o Titular dos Dados se opor ao Processamento nos termos do ponto (vi);
d) os Dados Pessoais foram processados ilicitamente;
e) os Dados Pessoais devem ser excluídos para cumprir uma obrigação legal nas Leis Europeias a que o Controlador esteja sujeito;
f) os Dados Pessoais tenham sido coletados em relação à oferta de serviços da sociedade da informação diretamente a uma criança.

Quando o Controlador tiver tornado os Dados Pessoais públicos e for obrigado a excluí-los, o Controlador, levando em conta a tecnologia disponível e o custo de implementação, deve tomar medidas razoáveis, incluindo medidas técnicas, para informar os Controladores que estão processando os Dados Pessoais que o Titular dos Dados solicitou a exclusão por parte de tais Controladores de quaisquer links, ou cópia ou replicação desses Dados Pessoais.

O direito à exclusão não se aplica na medida em que o Processamento seja necessário:

a) para exercitar o direito de liberdade de expressão e informação;
b) para cumprir uma obrigação legal que exija o Processamento por Leis Europeias a que o Controlador esteja sujeito ou para o desempenho de uma tarefa executada no interesse público ou no exercício de autoridade pública investida no Controlador;
c) por motivos de interesse público na área de saúde pública de acordo com os termos da Cláusula 6.1.2.
d) para fins de arquivamento de interesse público, fins de pesquisa científica ou histórica ou fins estatísticos de acordo com as Leis Europeias, na medida em que

esse direito possa impossibilitar ou prejudicar seriamente a realização dos objetivos desse processamento; ou

e) para o estabelecimento, exercício ou defesa de reivindicações legais.

(iv) **Restrição de Processamento**: O Titular dos Dados terá o direito de adquirir do Controlador a restrição de Processamento quando uma das seguintes situações se aplicar:

a) a exatidão dos Dados Pessoais for contestada pelo Titular dos Dados, por um período que permita ao Controlador verificar a exatidão dos Dados Pessoais;
b) O Processamento for ilícito e o Titular dos Dados se opor à exclusão dos Dados Pessoais e solicitar a restrição da sua utilização;
c) O Controlador não precisar mais dos Dados Pessoais para fins do Processamento, mas eles forem solicitados pelo Titular dos Dados para o estabelecimento, exercício ou defesa de ações judiciais;
d) o Titular dos Dados se opor ao Processamento enquanto aguarda a verificação se os fundamentos legítimos do Controlador prevalecem sobre os do Titular dos Dados.

Nos casos em que o Processamento tiver sido restringido, tais Dados Pessoais, com exceção do armazenamento, somente serão processados com o consentimento do Titular dos Dados ou para a declaração, exercício ou defesa de ações judiciais ou para a proteção dos direitos de outra pessoa singular ou coletiva ou por motivos de interesse público importante da União Europeia ou de um Estado Membro.

Um Titular dos Dados que obtiver a restrição de Processamento deve ser informado pelo Controlador antes que a restrição de Processamento seja levantada.

(v) **Portabilidade de dados**: Os Titulares dos Dados terão o direito de receber os Dados Pessoais que lhes digam respeito, que tenham fornecido a um Controlador, em formato estruturado, de uso comum e legível por máquina e têm o direito de transmitir esses Dados a outro Controlador sem impedimento do Controlador a quem os Dados Pessoais foram fornecidos, onde: a) o Processamento for baseado no consentimento ou em um contrato de acordo com as Cláusulas 6.1.1.1. e 6.1.2.; e b) o Processamento for realizado por meios automatizados.

Ao exercer o seu direito à portabilidade dos dados, os Titulares dos Dados terão o direito de que os Dados Pessoais sejam transmitidos diretamente de um Controlador a outro, sempre que tecnicamente possível.

O exercício do direito à portabilidade dos dados (a) não prejudica o direito à exclusão. Esse direito não se aplica ao Processamento necessário para executar uma tarefa realizada no interesse público ou no exercício da autoridade oficial investida no Controlador; e (b) não afetar adversamente os direitos e liberdades de outras pessoas.

(vi) **Direito de contestar**: Os Titulares dos Dados terão o direito de se opor, por motivos relacionados à sua situação específica, a qualquer momento ao Processamento dos Dados Pessoais que lhes digam respeito com base nos pontos (e) ou (f) da Cláusula 6.1.1.1., incluindo a definição de perfis com base nessas disposições. O Controlador não processará mais dos Dados Pessoais, a menos que o Controlador demonstre motivos legítimos

irrefutáveis para o Processamento que se sobreponham aos interesses, direitos e liberdades do Titular dos Dados ou para o estabelecimento, exercício ou defesa de reivindicações legais.

Quando os Dados Pessoais forem processados com fins de marketing direto, o Titular dos Dados terá o direito de se opor a qualquer momento ao Processamento de Dados Pessoais que lhes digam respeito para esse marketing, o que inclui a criação de perfis na medida em que esteja relacionado a esse marketing direto.

Quando o Titular dos Dados se opuser ao Processamento para fins de marketing direto, os Dados Pessoais não serão mais Processados para esses fins.

O mais tardar no momento da primeira comunicação com o Titular dos Dados, esse direito será explicitamente levado ao conhecimento do Titular dos Dados e apresentado de forma clara e separada de qualquer outra informação.

No contexto da utilização dos serviços da sociedade da informação, o Titular dos Dados pode exercer o seu direito de oposição por meios automatizados usando especificações técnicas. Quando Dados Pessoais forem processados para fins de pesquisa científica ou histórica ou para fins estatísticos, o Titular dos Dados, por motivos relacionados com a sua situação particular, terá o direito de se opor ao Processamento de Dados Pessoais que lhe digam respeito, a menos que o Processamento seja necessário para executar uma tarefa por motivos de interesse público.

- O Controlador deverá comunicar qualquer retificação ou apagamento de Dados Pessoais ou restrição de Processamento realizado de acordo com esta Cláusula a cada Destinatário a quem os Dados Pessoais foram divulgados, a menos que isso se mostre impossível ou envolva esforço desproporcional. O Controlador deve informar o Titular dos Dados sobre esses Destinatários se o Titular dos Dados solicitar.

6.3.3. Direito de contestar uma decisão individual automatizada

- Os Titulares dos Dados têm o direito de não ficarem sujeitos a uma decisão baseada somente no Processamento automatizado dos seus Dados Pessoais, como a definição de perfis, que tenha efeitos jurídicos sobre eles ou os afete significativamente de forma similar ("decisões individuais automatizadas"), a menos que qualquer uma das seguintes exceções se aplique: (i) a decisão seja necessária para celebrar ou executar um contrato entre o Titular dos Dados e um Controlador; (ii) a decisão seja autorizada pelas Leis Europeias a que o Controlador esteja sujeito e que também preveja medidas adequadas para salvaguardar os direitos e liberdades e interesses legítimos do Titular dos Dados; ou (iii) a decisão se basear no consentimento explícito do Titular dos Dados.

- Nas exceções mencionadas nos pontos (i) e (iii) acima, o Controlador deverá implementar as medidas adequadas para salvaguardar os direitos e liberdades e interesses legítimos do Titular dos Dados, pelo menos o direito de obter intervenção humana do Controlador, de expressar seu ponto de vista e contestar a decisão.

- Além disso, as decisões sob exceções (i) a (iii) não devem ser baseadas em Categorias Especiais de Dados Pessoais, a menos que as condições da Cláusula 6.1.2 se apliquem e haja medidas apropriadas para salvaguardar os direitos e liberdades e interesses legítimos do Titular dos Dados.

6.3.4. Direito de registrar reclamação

- Os Titulares dos Dados têm o direito de registrar uma reclamação junto à Autoridade de Supervisão Competente, caso considerem que o Processamento dos seus Dados Pessoais viole estas RCVs. Em particular com a Autoridade de Supervisão (i) no Estado Membro da sua residência habitual; (ii) no Estado Membro onde tem um local de trabalho; ou (iii) no Estado Membro onde ocorreu a alegada infração.

6.3.5. Direito a um recurso judicial efetivo

- Os Titulares dos Dados têm direito a um recurso judicial efetivo em relação aos Processadores de Dados ou Controladores de Dados onde os Titulares dos Dados considerem que seus direitos sob essas RCVs foram violados como resultado do Processamento de seus Dados Pessoais e não obstante qualquer recurso administrativo ou extrajudicial disponível. As ações contra o Controlador ou Subcontratante serão instauradas, à escolha do Titular dos Dados, perante os tribunais do Estado Membro onde o Controlador ou o Subcontratante tenham um estabelecimento ou perante os tribunais do Estado Membro onde o Titular dos Dados tenha sua residência habitual.

- Quando a infração tiver sido causada por uma Entidade RCV estabelecida fora do EEE, a Cláusula 6.7. será aplicada.

6.3.6. Procedimento para o exercício dos direitos do Titular dos Dados

- Os Titulares dos Dados podem exercer os direitos previstos nos parágrafos 6.3.2 e 6.3.3 ou registrar uma reclamação enviando uma solicitação por escrito ao endereço postal da Entidade RCV que atua na qualidade de Controlador, para os endereços de e-mail indicados nas Políticas de Privacidade das Entidades RCV ou ao seguinte endereço de e-mail oficina.privacidad@prosegur.com. Se a Entidade RCV tiver dúvidas razoáveis quanto à identidade do Titular dos Dados que fez a solicitação, a Entidade RCV poderá solicitar tal informação adicional necessária para confirmar a identidade do Titular dos Dados.

- Os Titulares dos Dados devem receber uma resposta sobre os direitos que estão exercendo sem demoras e em todos os casos, dentro de um (1) mês do recebimento da solicitação. Esse prazo poderá ser prorrogado por mais 2 (dois) meses, quando necessário, dependendo da complexidade e quantidade de solicitações recebidas. O Titular dos Dados deverá ser informado sobre tal prorrogação dentro de 1 (um) mês do recebimento da solicitação, indicando os motivos pelo atraso.

- Será fornecida uma resposta aos Titulares dos Dados, aceitando ou rejeitando a solicitação/reclamação. Os Titulares dos Dados serão também informados de que, caso não fiquem satisfeitos com a resposta recebida, terão o direito de registrar reclamação junto à Autoridade de Supervisão Competente, bem como buscar o efetivo recurso judicial, nos termos das Cláusulas 6.3.4 e 6.3.5 acima.

6.4. Direitos de terceiros beneficiários

- As Entidades RCV concordam e aceitam expressamente que os Titulares dos Dados têm o direito de fazer cumprir esta cláusula e as cláusulas 6.1.1, 6.1.2, 6.1.3, 6.1.6, 6.2, 6.3, 6.4, 6.5, 6.6.6, 6.7 e 6.8 destas RCV como terceiros beneficiários.

6.5. Reivindicações/reclamações

- Não obstante o disposto na Cláusula 7 destas RCVs, os Titulares dos Dados podem exercer seus direitos ou registrar uma reclamação sobre o Processamento dos seus Dados pelas Entidades RCV e sua aplicação de RCVs seguindo o procedimento indicado na Cláusula 6.3.6.

- As Entidades RCV devem cumprir o disposto na Cláusula 6.3.6 e no Protocolo de Tratamento de Reclamações e Reclamações de RCV, constante como Anexo 8.

6.6. Ações para implementar RCVs

6.6.1. Treinamento de pessoal

- No âmbito do compromisso do Grupo PROSEGUR com a privacidade e cumprimento da proteção de Dados, são realizados treinamentos e cursos de conscientização anualmente.

- As Entidades RCV e os Diretores Locais de Proteção de Dados/Conformidade, com o apoio do Diretor de Proteção de Dados do Grupo, são responsáveis por definir o formato dos cursos de formação e sensibilização (presencial ou online), bem como a frequência dos treinamentos.

- Mais especificamente, são realizadas anualmente as seguintes ações de treinamento e conscientização: (i) uma sessão geral sobre questões de privacidade e proteção de Dados; e (ii) uma sessão específica sobre RCVs.

  A sessão geral sobre questões de privacidade aborda, entre outros, o impacto da privacidade na atividade do Grupo PROSEGUR e do seu Pessoal e as políticas e normas adotadas no Grupo PROSEGUR.

  A sessão específica sobre questões de RCV abrange o conteúdo desta RCV, incluindo os anexos relevantes.

- As sessões de treinamento e conscientização são realizadas pela Plataforma Online da Universidade Prosegur, acessível na Intranet do Grupo PROSEGUR. Os conteúdos das sessões de treinamento e conscientização são um misto de teoria e prática, incluindo um questionário de avaliação que deve ser aprovado (isto é, 7 em 10 respostas corretas) para considerar o curso “frequentado e concluído”. A Universidade Prosegur usa a plataforma online para gerenciar as solicitações ao Pessoal para que frequentem o curso, lembretes, participantes e quem concluiu cada curso.

- O Pessoal também terá acesso às políticas internas do Grupo PROSEGUR sobre a Proteção de Dados Pessoais e segurança da informação, bem como ao conteúdo dessas RCVs. As informações estarão incluídas nos materiais entregues ao Pessoal no momento da incorporação, publicados na intranet do Grupo PROSEGUR e das Entidades RCV e promovidas por meio de notificações.

6.6.2. Monitoramento de conformidade com RCV

- O Diretor de Proteção de Dados do Grupo e o Comitê de Proteção de Dados Corporativos são responsáveis por supervisionar a implementação destas RCVs, com o apoio dos Diretores Locais de Proteção de Dados/Conformidade e dos órgãos de gerenciamento das Entidades RCV.

- O Diretor de Conformidade/Proteção de Dados Local designado terá, entre outras, as seguintes funções:

  (i) Informar e aconselhar as Entidades RCV e o pessoal que realiza o Processamento sobre as suas obrigações ao abrigo da RCV e das Leis Europeias de Proteção de Dados. O Diretor de Conformidade/Proteção de Dados Local se reporta diretamente ao nível mais alto da hierarquia da Entidade RCV.

  (ii) monitorar o cumprimento do disposto na RCV e da Lei Europeia de Proteção de Dados, e das políticas da PROSEGUR, incluindo a atribuição de responsabilidades, conscientização e treinamento do pessoal envolvido nas operações de Processamento.

  (iii) atuar como ponto de contato com as autoridades de supervisão em questões relacionadas a operações de Processamento de Dados e implementação de RCV, bem como cooperar com as investigações conduzidas por tais autoridades.

  (iv) revisar os relatórios de auditoria de proteção de dados e monitorar a implementação das medidas corretivas neles propostas.

  (v) lidar com solicitações e reclamações feitas por Titulares de Dados.

- O Diretor de Proteção de Dados do Grupo é responsável por manter esta RCV atualizada e por relatar atualizações à(s) Autoridade(s) de Supervisão(s) relevante(s), bem como por informar anualmente o status da implementação da RCV. Os Diretores Locais de Proteção de Dados/Diretores Locais de Conformidade devem reportar trimestralmente ao Diretor de Proteção de Dados do Grupo sobre as medidas de proteção de Dados tomadas a nível local.

6.6.3. Verificação de conformidade RCV

- O Grupo PROSEGUR tem também um Programa de Auditorias, descrito no Anexo 9, para verificar o cumprimento das Entidades RCV com esta RCV. Esse programa estabelece a frequência e os períodos das revisões e auditorias, seu escopo, ações envolvidas e meios, entre outros aspectos.

- Os resultados das avaliações e auditorias devem ser comunicados ao Diretor de Proteção de Dados do Grupo, ao Diretor de Proteção de Dados/Diretor de Conformidade Local, ao Comitê de Proteção de Dados Corporativos e à Diretoria da Entidade RCV em causa.

- Os resultados das auditorias também devem ser comunicados à Diretoria da PROSEGUR.

- Em caso de descumprimento da RCV, os relatórios incluem recomendações e medidas corretivas a implementar pela Entidade RCV em causa, dentro de um prazo específico. Caso as recomendações e medidas corretivas não sejam devidamente implementadas, o fato é comunicado à Diretoria da PROSEGUR, para as devidas decisões; incluindo, entre outros, a exclusão da Entidade RCV do escopo da RCV.

- As Autoridades de Supervisão podem exigir acesso a relatórios de auditoria e podem executar auditorias de proteção de dados de qualquer Entidade RCV.

- As auditorias também serão feitas mediante solicitação específica do Diretor de Proteção de Dados do Grupo ou do Diretor de Proteção de Dados/Diretor de Conformidade Local e em caso de alterações ou fatos que afetem significativamente as RCVs.

6.6.4. Atualizações de RCV

- As RCVs são revisadas e atualizadas, em caso de alterações, seja na Lei Europeia de Proteção de Dados ou em qualquer conteúdo das RCVs (incluindo seus Anexos). O Diretor de Proteção de Dados do Grupo é o responsável por revisar regularmente as RCVs e alterar conforme necessário para mantê-las atualizadas e, para isso, deve fazer o seguinte:

  (i) Manter um registo atualizado das Entidades RCV e atualizações de RCV, bem como exibir tais detalhes nas RCVs;

  (ii) monitorar as mudanças regulatórias, registrando-as e adicionando-as à RCV;

  (iii) fornecer as informações necessárias aos Titulares dos Dados e/ou autoridades de supervisão, conforme necessário.

- Alterações nas RCVs (que incluam, entre outros, a lista de Entidades RCV) são comunicadas a todas as Entidades RCV sem demora indevido.

- As alterações nas RCVs ou na lista de Entidades RCV são comunicadas às Autoridades de Supervisão, por meio da Autoridade de Supervisão principal, uma vez por ano juntamente com uma explicação dos motivos. Quando as alterações nas RCVs puderem afetar o nível de proteção oferecido pelas RCVs ou afetar significativamente as RCVs, essas alterações devem ser notificadas com antecedência às Autoridades de Supervisão Competentes, por meio da Autoridade de Supervisão líder, com uma breve explicação dos motivos da atualização. Neste caso, as Autoridades de Supervisão também avaliarão se as alterações feitas exigem uma nova aprovação.

- Nenhuma transferência deve ser feita a uma nova Entidade RCV até que a nova Entidade RCV esteja efetivamente vinculada às RCVs e possa cumpri-las.

6.6.5. Não conformidade de RCV

- As Entidades RCV informarão imediatamente o Exportador de Dados se não puderem cumprir a RCV, por qualquer motivo, incluindo as situações descritas na Cláusula 6.8.2.

- Caso o Importador de Dados (ou qualquer outra Entidade RCV que seja destinatária em uma Transferência Subsequente) viole as RCVs ou seja incapaz de cumprir as RCVs, o Exportador de Dados suspenderá o IDT.

- As Entidades RCV devem, à escolha do Exportador de Dados, devolver ou excluir imediatamente os Dados Pessoais que foram transferidos sob a RCV em sua totalidade quando:

  (i) o Exportador de Dados tiver suspendido o IDT e a conformidade com estas RCV não for restaurada dentro de um prazo razoável e, em qualquer caso, dentro de um mês após a suspensão; ou

  (ii) a Entidade RCV estiver em violação substancial ou persistente das obrigações da RCV; ou

  (iii) A Entidade RCV não cumprir uma decisão vinculativa de um tribunal competente ou Autoridade de Supervisão sobre suas obrigações ao abrigo da RCV.

- O mesmo se aplica a quaisquer cópias dos Dados e Transferências Subsequentes. As Entidades RCV certificarão a exclusão dos Dados ao Exportador de Dados. Até que os Dados sejam excluídos ou devolvidos, as Entidades RCV continuarão garantindo a conformidade com a RCV. No caso de leis locais pertinentes às Entidades RCV que proíbam a devolução ou exclusão dos Dados Pessoais transferidos, as Entidades RCV garantem que continuarão assegurando a conformidade com a RCV e somente processarão os Dados na medida e pelo tempo exigido pela lei local.

6.6.6. Informações aos Titulares dos Dados

- Os Titulares dos Dados serão informados das RCVs pelos seguintes meios:

  (i) publicação nos sites oficiais da PROSEGUR e das Entidades RCV;

  (ii) publicação na intranet da PROSEGUR e Entidades RCV;

  (iii) inclusão de referências a RCVs em cláusulas informativas de Proteção de Dados em relação a contratos, formulários, políticas, manuais e avisos.

  A informação prestada aos Titulares dos Dados consta do Anexo 0 - Versão pública das RCVs.

- Adicionalmente, os Titulares dos Dados podem solicitar por escrito uma cópia das RCVs, enviando-a ao seguinte endereço: oficina.privacidad@prosegur.com.

6.7. Responsabilidade Legal

- A PROSEGUR será responsável e concorda em tomar as medidas necessárias para remediar os atos das Entidades RCV localizadas fora do EEE e pagar uma indemnização por quaisquer danos materiais ou imateriais resultantes da violação das RCVs por essas Entidades RCV fora do EEE.

- A PROSEGUR ficará isenta, no todo ou em parte, dessa responsabilidade desde que prove que o evento que originou o dano não é, de forma alguma, da responsabilidade do Importador de Dados ou de outras Entidades RCV no caso de uma Transferência Subsequente. Caberá à PROSEGUR o ônus de provar que as RCV não foram violadas ou que o evento gerador do dano não é, de forma alguma, da responsabilidade da Entidade ou Entidades RCV em causa.

- Nos casos em que a violação destas RCVs tenha sido cometida por uma Entidade RCV estabelecida em um Terceiro País, a jurisdição será estabelecida nos tribunais ou outras autoridades competentes da União Europeia, e o Titular dos Dados terá direitos e recursos adequados contra a PROSEGUR como se a violação tivesse ocorrido no Estado Membro em que a PROSEGUR está sediada e não no país do Importador de Dados ou Entidade RCV fora da EEE.

  Neste caso, o processo contra a PROSEGUR será instaurado, à escolha do Titular dos Dados, perante os tribunais de Espanha ou perante os tribunais do Estado Membro onde o Titular dos Dados tenha sua residência habitual.

6.8. Relacionamento com regulamentos e autoridades

6.8.1. Comunicação e cooperação com as Autoridades de Supervisão

- As Entidades RCV comprometem-se a cooperar com as Autoridades de Supervisão Competentes em todos os assuntos relacionados à implementação destas RCVs e, em particular, a:

  (i) fornecer todas as informações exigidas pelas Autoridades de Supervisão no que diz respeito às RCVs e ao Processamento por elas regido;

  (ii) permitir sua auditoria por parte das Autoridades de Supervisão;

  (iii) implementar as recomendações feitas pelas Autoridades de Supervisão;

  (iv) fornecer os relatórios de verificação/auditorias de conformidade da RCV exigidos pelas Autoridades de Supervisão;

  (v) comunicar alterações às RCVs à Autoridades de Supervisão.

6.8.2. Relacionamento com as leis locais

6.8.2.1 Compatibilidade com as leis locais

- Os Dados Pessoais devem ser processados pelas Entidades RCV de acordo com as leis que lhes sejam pertinentes. Na ausência de uma lei local de Proteção de Dados, ou onde tal lei estabeleça um nível de proteção inferior ao previsto nestas RCVs, os direitos e obrigações estipulados nas RCVs prevalecerão. Onde a lei local exigir um nível mais alto de Proteção de Dados Pessoais, ela prevalecerá sobre as RCVs.

- As Entidades RCVs garantem que não têm motivos para acreditar que as leis e práticas nos Terceiros Países de destino previstos aplicáveis ao Processamento de Dados Pessoais pelos Importadores de Dados relevantes, incluindo quaisquer requisitos para divulgar Dados Pessoais ou medidas que autorizem o acesso por parte de autoridades públicas, impedir que os importadores de dados cumpram suas obrigações sob estas RCVs.

- A BCR baseia-se no entendimento de que as leis e práticas que respeitam a essência dos direitos e liberdades fundamentais e não excedam o necessário e proporcional em uma sociedade democrática para salvaguardar um dos objetivos abaixo enumerados, não estejam em contradição com esta RCV:

  a) segurança nacional;

  b) defesa;

  c) segurança pública;

  d) a prevenção, investigação, detecção ou repressão de infrações penais ou a execução de sanções penais, incluindo a proteção e prevenção de ameaças à segurança pública;

  e) outros objetivos importantes de interesse público geral da União Europeia ou de um Estado membro, nomeadamente um interesse econômico ou financeiro importante da

União Europeia ou de um Estado membro, incluindo questões monetárias, orçamentais e fiscais, saúde pública e segurança social;

f) a proteção da independência judicial e dos processos judiciais;

g) a prevenção, investigação, detecção e repressão das infrações à ética das profissões regulamentadas;

h) uma função de monitoramento, inspeção ou regulamentação conectada, mesmo ocasionalmente, com o exercício da autoridade pública nos casos mencionados nos pontos a) a e) e g);

i) a proteção do Titular dos Dados ou dos direitos e liberdades de terceiros;

j) a execução de ações cíveis.

- Ao avaliar as leis e práticas do Terceiro País que possam afetar o cumprimento dos compromissos contidos na RCV, as Entidades da RCV devem ter em conta, nomeadamente, os seguintes elementos:

  (i) as circunstâncias específicas do IDT ou conjunto de IDTs e de quaisquer Transferências Subsequentes previstas no mesmo Terceiro País ou para outro Terceiro País, incluindo:

    - finalidades para as quais os Dados Pessoais são transferidos e processados (por exemplo, marketing, RH, armazenamento, suporte de TI, etc.);
    - tipos de entidades envolvidas no Processamento (o importador de dados e qualquer outro destinatário de qualquer Transferência Subsequente);
    - setor em que ocorre o IDT ou conjunto de IDTs;
    - categorias e formato dos Dados Pessoais transferidos;
    - localização do Processamento, incluindo armazenamento;
    - canais de transmissão utilizados.

  (ii) As leis e práticas do Terceiro País de destino que sejam relevantes à luz das circunstâncias da transferência, incluindo aquelas que exijam a divulgação de dados a autoridades públicas ou que autorizam o acesso de tais autoridades, incluindo aquelas que dão acesso a esses dados durante o trânsito entre o país do Exportador de Dados e país do Importador de Dados, bem como as limitações e salvaguardas aplicáveis;

  (iii) Quaisquer salvaguardas contratuais, técnicas ou organizacionais relevantes implementadas para complementar as salvaguardas sob as RCVs, incluindo medidas aplicadas durante a transmissão e o Processamento dos Dados Pessoais no país de destino.

- As Entidades RCV comprometem-se a que, sempre que devam ser implementadas quaisquer salvaguardas para além das previstas na RCV, a PROSEGUR, o Diretor de Proteção de Dados do Grupo ou do Diretor de Proteção de Dados/Diretor de Conformidade Local serão informados e envolvidos na avaliação.

- As Entidades RCV devem documentar adequadamente essa avaliação, bem como as medidas complementares selecionadas e implementadas e devem disponibilizar essa documentação à Autoridade de Supervisão Competente, mediante solicitação.

- Os Exportadores de Dados devem monitorar, de forma contínua e, quando apropriado, em colaboração com Importadores e Destinatários de Dados, desenvolvimentos nos países terceiros para os quais os exportadores de dados transferiram dados pessoais que possam afetar a avaliação inicial do nível de proteção e as decisões tomadas adequadamente nessas transferências.

6.8.2.2 Incompatibilidade com as leis locais

- Qualquer Entidade RCV atuando como Importador ou Destinatário de Dados deve notificar imediatamente o Exportador de Dados se, ao usar esta RCV como uma ferramenta para IDT e durante sua associação à RCV, tiver motivos para acreditar que está ou se tornou sujeito às leis ou práticas que o impediriam de cumprir suas obrigações de acordo com as RCV, inclusive após uma alteração nas leis do Terceiro País ou uma medida (como uma solicitação de divulgação). Esta informação deverá também ser levada à PROSEGUR e ao Diretor de Proteção de Dados do Grupo.

- Após verificar tal notificação, a Entidade RCV que atua como Exportadora de Dados, juntamente com a PROSEGUR, o Diretor de Proteção de Dados do Grupo e o Diretor Local de Proteção de Dados/Conformidade, comprometem-se a identificar prontamente as medidas adequadas (por exemplo, medidas técnicas ou organizacionais de modo a garantir a segurança e confidencialidade) a serem adotadas pela Entidade RCV que atua como Exportadora de Dados e/ou pela Entidade RCV que atua como Importadora de Dados para permitir que cumpram suas obrigações sob a RCV. O mesmo se aplica caso uma Entidade RCV que atua como Exportadora de Dados tiver motivos para acreditar que uma Entidade RCV que atua como Importadora de Dados ou Destinatária de uma Transferência Subsequente não possa mais cumprir suas obrigações sob esta RCV.

- Quando a Entidade RCV atuando como Exportador de Dados, juntamente com a PROSEGUR, o Diretor de Proteção de Dados do Grupo e o Diretor de Proteção de Dados/Diretor de Conformidade relevante avaliar que nenhuma salvaguarda adequada para o IDT ou conjunto de IDTs pode ser garantida ou se instruído pela(s) Autoridade(s) de Supervisão Competente(s), compromete-se a suspender o IDT ou conjunto de IDT em causa, bem como todas as transferências de dados para as quais a mesma avaliação e raciocínio levariam a uma consequência semelhante.

- A PROSEGUR, o Diretor de Proteção de Dados do Grupo e o Diretor de Conformidade/Proteção de Dados Local relevantes e competentes informarão todas as outras Entidades RCV sobre a avaliação realizada e seus resultados para que sejam aplicadas as medidas suplementares identificadas caso o mesmo tipo de transferências efetuadas por quaisquer outras Entidades RCV ou, caso não possam ser aplicadas medidas complementares eficazes, o IDT em causa será suspenso ou encerrado.

- Após essa suspensão, a Entidade RCV que atua como Exportadora de Dados pode escolher encerrar o IDT ou conjunto de IDTs. Nesse sentido, os Dados Pessoais que tiverem sido transferidos antes da suspensão, e possíveis cópias dos mesmos, caso queira a Entidade RCV que atua como Exportadora de Dados, deverão ser devolvidas a ela ou inteiramente destruídas.

- Sempre que houver alguma incompatibilidade com a legislação local que possa resultar em efeitos adversos substanciais na aplicação das garantias prestadas pela RCV, a PROSEGUR notificará as Autoridades de Supervisão Competentes, incluindo quaisquer solicitações ou

requisições juridicamente vinculativas para a divulgação de Dados Pessoais por uma autoridade ou órgão de segurança do estado do país em questão. As Autoridades de Supervisão Competentes devem ser claramente informadas sobre a solicitação, nomeadamente sobre os Dados solicitados, a entidade requerente e a base legal da divulgação, salvo proibição legal que impeça tal notificação.

- Se, em casos específicos, for proibida a suspensão e/ou notificação, as Entidades RCV solicitadas envidarão todos os esforços para obter o direito de renunciar esta proibição de divulgação às Autoridades de Supervisão Competentes do máximo de informações possível, com a maior brevidade possível, e poder demonstrar isso. Sempre que, em tais casos, apesar dos melhores esforços, as Entidades RCV não conseguirem notificar as Autoridades de Supervisão Competentes, as Entidades RCV comprometem-se a fornecer anualmente às Autoridades de Supervisão Competentes um relatório geral sobre as solicitações recebidas, incluindo o número de solicitações de divulgação, os tipos de Dados solicitados e as autoridades ou órgãos solicitantes, quando possível.

- Em qualquer caso, as divulgações de Dados Pessoais por uma Entidade RCV a autoridades públicas não devem ser massivas, desproporcionais ou indiscriminadas, de modo a limitar-se ao que é necessário em uma sociedade democrática para proteger interesses específicos importantes, incluindo a segurança pública e a prevenção, investigação, detecção e repressão de infrações criminais ou execução de penalidades criminais, incluindo a proteção e prevenção de ameaças à segurança pública.

6.9. Duração

- As RCVs entrarão em vigor no dia da sua adoção e permanecerão válidas por tempo indeterminado.

ANEXOS

7. Anexos

7.1. Anexo 1 - Entidades RCV

A lista de entidades do Grupo PROSEGUR que estão aderidas a estas RCV está disponível no seguinte link: Política de Privacidad: Normas Corporativas Vinculantes | Prosegur.com.

7.2. Anexo 2 - Mapa de Transferências de Dados Internacionais

Um resumo da Transferência Internacional de Dados esperada ou executada atualmente está incluído na **Cláusula 3.2.2.** das RCV.

Ali, você pode encontrar as informações relevantes sobre os países de onde os Dados Pessoais são ou serão exportados, os Terceiros Países de destino atuais ou esperados, os grupos de Titulares de Dados afetados e os tipos dos Dados que serão transferidos, bem como as finalidades do seu Processamento.

7.3. Anexo 3 - Política de Segurança da Informação

A Política de Segurança da Informação do Grupo PROSEGUR é interna e confidencial. Na **Cláusula 6.1.3** das RCVs, você pode encontrar as informações públicas e relevantes sobre as medidas de segurança implementadas no Grupo PROSEGUR.

7.4. Anexo 4 - Modelo de Governança para Conformidade em assuntos de Proteção de Dados

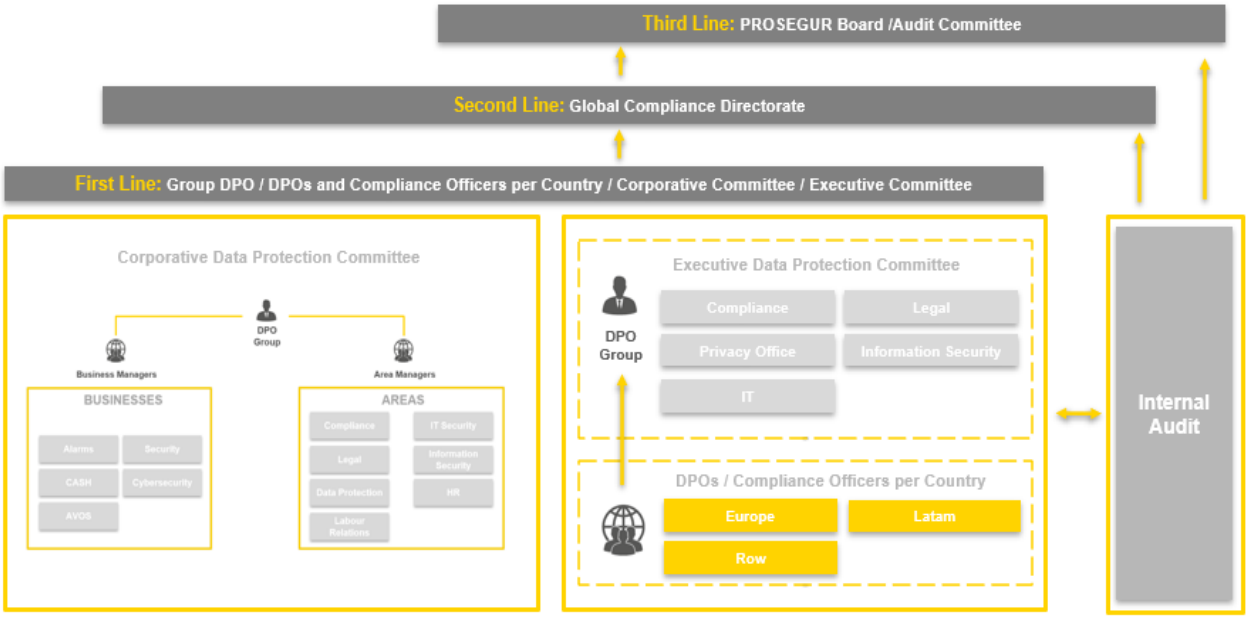
O Modelo de Governança para Conformidade em assuntos de Proteção de Dados é uma política interna e confidencial por meio da qual o Grupo PROSEGUR estabelece as bases do seu sistema interno de Proteção de Dados Pessoais e as respectivas políticas e procedimentos associados. Esta Política declara:

i. Os Princípios de Proteção de Dados que devem ser respeitados por todas as entidades participantes do Grupo PROSEGUR e seu Pessoal. Esses princípios são indicados na **Cláusula 6.1.1.** das RCVs.

ii. As funções e responsabilidades das principais áreas e de todo o Pessoal do Grupo PROSEGUR para proteção dos Dados Pessoais, que incluem as relacionadas com a aplicação das RCVs.

iii. As funções e responsabilidades dos Diretores de Proteção de Dados Globais e Locais e Diretores de Conformidade Locais estão resumidas na **Cláusula 6.1.4** das RCVs.

iv. A composição dos órgãos corporativos de Proteção de Dados Pessoais, suas funções e responsabilidades, a quem respondem e com que frequência, bem como seu posicionamento como linhas de defesa da Privacidade e Proteção de Dados. Veja um resumo abaixo:



- **Comitê de Proteção de Dados Corporativos**

  O Comitê de Proteção de Dados Corporativos, liderado e presidido pelo DPO do Grupo, se reunirá semestralmente e consistirá de um membro das principais áreas e negócios da PROSEGUR, denominado Gerente de Processamento Funcional, a quem caberá acompanhar as ações que foram definidas para garantir a conformidade no campo da Proteção de Dados em seu campo de competência, e devem responder ao Diretores de Conformidade/DPO Local e/ou do Grupo sobre o nível de conformidade com as ações implementadas. Esse Comitê tem as seguintes funções:

  - Informar sobre as ações desenvolvidas por cada uma das áreas/departamentos e negócios no campo da Proteção de Dados, bem como sobre qualquer assunto que considere apropriado no domínio da Proteção de Dados.
  - Informar sobre possíveis riscos na área de Proteção de Dados.
  - Denunciar Violações de Dados Pessoais e/ou incidentes identificados.
  - Reportar novas iniciativas que envolvam o Processamento de Dados Pessoais.
  - Informar sobre os resultados das avaliações objetivas dos riscos, bem como das novas atividades de Processamento identificadas no âmbito da sua competência, (negócio/área/departamento), incorporando as novas atividades de Processamento implementadas.
  - Informar sobre o acesso aos Dados do Grupo PROSEGUR por parte de novos terceiros.
  - Identificar as novas Transferências Internacionais de Dados executadas.
  - Informar as novas necessidades detectadas no campo da Proteção de Dados.
  - Preparar materiais para cursos e sessões de treinamento sobre Processamento de Dados Pessoais e definir o formato dos cursos de treinamento e sua frequência.

- **Comitê Executivo de Proteção de Dados**

- O Comitê Executivo de Proteção de Dados é representada pelo DPO do Grupo e pelos responsáveis pelas áreas de Conformidade, Jurídico, Proteção de Dados, Segurança Informática e Segurança da Informação, tendo como principal objetivo tratar de questões de maior relevância no campo da Proteção de Dados, de acordo com os critérios de prioridade, criticidade e urgência.

7.5. Anexo 5 - Política de Seleção e Avaliação de Fornecedores

A Seleção e Avaliação de Fornecedores é uma política interna e confidencial pela qual o Grupo PROSEGUR estabelece os requisitos para contratar um Processador de Dados. Esta Política afirma, em resumo, que:

- As Entidades RCV só podem contratar Processadores que ofereçam garantias suficientes para implementar as medidas técnicas e organizacionais adequadas, de forma a garantir que a atividade que envolva o Processamento de Dados Pessoais seja realizada de acordo com os requisitos estabelecidos pelas RCVs a este respeito e garantindo a proteção dos direitos dos Titulares dos Dados. O mesmo se aplica quando uma Entidade RCV atuando como Processador deseja contratar um subprocessador, seja uma Entidade RCV ou não.

- Essas garantias estão contidas, entre outros elementos, na competência, confiabilidade e recursos, visando implementar as medidas técnicas e organizacionais correspondentes ao cumprimento dos requisitos das RCV, incluindo a segurança do Processamento. Nesse sentido, a adesão do Processador a um código de conduta aprovado ou a um mecanismo de certificação aprovado pode ser usada como forma de demonstrar a existência de garantias suficientes quanto ao cumprimento das suas obrigações de Proteção de Dados.

- O processo de seleção de um Fornecedor que atue como Processador de Dados inicia-se com o envio de um questionário de avaliação do fornecedor, o qual deve ser preenchido antes de efetivar a contratação. O questionário e as respostas devem ser acompanhados de evidências relevantes. O questionário inclui também perguntas questões sobre medidas técnicas de segurança, às quais o Fornecedor deve responder de forma a avaliar o nível de conformidade e determinar se as medidas de segurança implementadas são adequadas ao nível de risco identificado. Se os resultados do processo de avaliação não forem satisfatórios após a conclusão do processo de avaliação, o Fornecedor relevante não poderá ser contratado, a menos que ele remedie as deficiências identificadas na avaliação e certifique a correção apresentado as evidências pertinentes.

- As Entidades RCV também têm o direito de auditar as instalações e sistemas do Processador de Dados e solicitar o acesso a determinada documentação que comprove a conformidade com as RCVs, como seus Registros de Atividades de Processamento, compromissos de confidencialidade assinados com seus funcionários e colaboradores, certificados de treinamento em Proteção de Dados, certificados de ter sido avisado sobre o assunto ou ter sido auditado, etc.

- A relação com o Processador será regida por um contrato ou outro ato jurídico de acordo com as Leis Europeias, que vincula o Processador ao Controlador. Os requisitos mínimos deste contrato estão descritos na **Cláusula 6.1.5.** das RCVs.

7.6. Anexo 6 – Protocolo de Gerenciamento e Notificação sobre Violação de Dados Pessoais

O Protocolo de Gerenciamento e Notificação sobre Violação de Dados Pessoais da PROSEGUR é interno e confidencial. Na **Cláusula 6.1.6** das RCVs pode encontrar as informações relevantes e públicas sobre o procedimento de violação de dados pessoais no Grupo PROSEGUR.

7.7. Anexo 7 - Protocolo de Gerenciamento de DPIA

A Avaliação do Impacto da Proteção de Dados (doravante, "DPIA" ou Data Protection Impact Assessment na sigla em inglês) é um protocolo interno e confidencial através do qual o Grupo PROSEGUR estabelece os requisitos para contratar um Processador de Dados. Este protocolo afirma, em resumo, que:

- A DPIA é uma análise detalhada de uma ou mais operações similares de Processamento de Dados Pessoais que visa identificar e avaliar os riscos associados ao Processamento e especificar as medidas a serem tomadas para preveni-los ou mitigá-los.

- Este processo de avaliação deve ser realizado antes do início de qualquer operação de Processamento de Dados Pessoais, para que os meios necessários para garantir que a conformidade dos princípios, direitos e obrigações estabelecidos pela legislação de Proteção de Dados Pessoais sejam determinados e aplicados desde o início da operação. No entanto, nada impede que uma DPIA seja feita para um Processamento que já esteja em pleno funcionamento.

- As Entidades de RCV devem fazer uma DPIA quando for provável que a natureza, escopo, contexto ou finalidades de um tipo de Processamento, especialmente se com o uso de novas tecnologias, envolva alto risco para os direitos e liberdades das pessoas singulares.

- A DPIA deve incluir pelo menos:

    - uma descrição sistemática das operações de Processamento previstas e das finalidades do Processamento, incluindo, quando pertinente, o interesse legítimo das Entidades RCV;

    - uma avaliação da necessidade e proporcionalidade das operações de processamento em relação à sua finalidade;

    - uma avaliação dos riscos para os direitos e liberdades dos Titulares dos Dados; e

    - as medidas previstas para enfrentar os riscos, incluindo salvaguardas, medidas de segurança e mecanismos para garantir a Proteção dos Dados Pessoais e para demonstrar cumprimento das leis, tendo em conta os direitos e interesses legítimos dos Titulares dos Dados e outras pessoas físicas afetadas.

7.8. Anexo 8 - Protocolo de Tratamento de Reclamações e Reclamações de RCV

O Protocolo de Tratamento de Reclamações e Reclamações de RCV PROSEGUR é um protocolo interno e confidencial. Na **Cláusula 6.3.6** das RCVs você pode encontrar as informações relevantes e públicas a respeito.

7.9. Anexo 9 – Programa de Auditoria

O Programa de Auditoria é um protocolo interno e confidencial pelo qual o Grupo PROSEGUR estabelece a frequência e os períodos das avaliações e auditorias, seu escopo, ações envolvidas e meios, entre outros aspectos, com o objetivo de verificar a conformidade das Entidades RCV com as RCVs.

O programa de auditoria afirma, em resumo, que:

- A conformidade das Entidades RCV com as leis locais de Proteção de Dados e as políticas e códigos internos do Grupo PROSEGUR é constantemente avaliada pelo Diretor de Proteção de Dados do Grupo por meio de relatórios do sistema de Proteção de Dados, que contém toda a informação sobre Proteção de Dados a nível local (ou seja, registros de atividades de processamento, sistemas associados, reclamações e solicitações recebidas, etc.) bem como o nível de cumprimento dos controles de Proteção de Dados do Grupo PROSEGUR. Além disso, os DPOs/Diretores de Conformidade Locais devem se reportar trimestralmente ao Diretor de Proteção de Dados do Grupo e o Diretor de Proteção de Dados do Grupo deve se reportar à Diretoria da PROSEGUR, que é o nível mais alto de gerenciamento do grupo.

- Além dessas análises gerais de Conformidade de Proteção de Dados, o Grupo PROSEGUR criou um programa de auditoria para verificar especificamente a conformidade das Entidades RCV com as RCVs, que consiste em:

    - **Avalições anuais**: Anualmente, cada Entidade RCV responderá a um questionário sobre o cumprimento das RCVs. Estes questionários medirão o nível de implementação da Entidade RCV e o seu grau de eficácia. Com base nas informações fornecidas, será elaborado um relatório pela Auditoria Interna, que será enviado ao Diretor de Proteção de Dados do Grupo e para os Diretores Locais de Proteção/Conformidade de Dados do país relevante, para que seja enviado por sua vez ao Comitê de Proteção de Dados Corporativos. Serão propostas recomendações e medidas corretivas para eventuais descumprimentos ou deficiências identificadas.

    - **Auditorias trienais:** Trienalmente, a Auditoria Interna fará uma auditoria onde serão avaliadas as respostas ao questionário da última revisão anual e seu relatório e coletadas evidências sobre o cumprimento dos requisitos das RCVs. Será elaborado um relatório pela Auditoria Interna, que será enviado ao Diretor de Proteção de Dados do Grupo e para os Diretores Locais de Proteção/Conformidade de Dados do país relevante, para que seja enviado por sua vez ao Comitê de Proteção de Dados Corporativos. Os relatórios de auditoria resultantes serão também comunicados ao órgão de administração e gerenciamento da Entidade RCV em causa e à Diretoria da PROSEGUR.

      Em caso de descumprimento da RCV, os relatórios incluirão recomendações e medidas corretivas a implementar pela Entidade RCV em causa, dentro de um prazo específico. Caso as recomendações e medidas corretivas não sejam devidamente implementadas, o fato é comunicado à Diretoria da PROSEGUR, para as devidas decisões; incluindo, entre outros, a exclusão da Entidade RCV do escopo da RCV.

    - **Auditorias solicitadas:** As Autoridades de Supervisão podem exigir acesso a relatórios de auditoria e podem executar auditorias de Proteção de Dados de qualquer Entidade RCV. Também serão realizadas auditorias de Proteção de Dados mediante solicitação específica do Diretor de Proteção de Dados do Grupo ou do Diretor de Proteção de Dados/Diretor de Conformidade Local, sempre que considerarem necessário. As auditorias também serão necessárias em caso de (i) mudanças na estrutura/políticas da Entidade RCV e/ou nas leis locais de Proteção de Dados; ou (ii) qualquer fato reportado ou detectado, que afete significativamente as RCVs e/ou que ponha em causa a capacidade da Entidade RCV cumprir as RCVs.

PROSEGUR