Regras Corporativas Vinculantes Aplicáveis ao Grupo PROSEGUR

VERSÃO PÚBLICA

SETEMBRO DE 2023

www.prosegur.com

PROSEGUR

Índice

1. Origem

Direção Corporativa de Conformidade

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 que atua no setor de atividade da segurança privada, com cinco atividades económicas (negócios): alarmes, segurança, gestão de tesouraria, terceirização de processos de negócios (AVOS) e cibersegurança (Cipher), proporciona segurança confiável às empresas e famílias, com base nas soluções mais avançadas e *best practices* disponíveis no mercado.

- **Alarmes**: a Prosegur Alarmes dispõe de uma vasta gama de produtos que ajudam a melhorar a segurança e a tranquilidade de famílias e empresas. Os alarmes Prosegur Triple Security oferecem os sistemas mais avançados do mercado. A linha empresarial inclui de sistemas de alarme com verificação por vídeo, automatização de áreas internas e externas, produtos sempre personalizados (customizados ao cliente) e que a tornam referência mundial em segurança.

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

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

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

- ***Cash***: a Prosegur Cash abrange todo o ciclo de vida do dinheiro, tratando mais de € 450 mil milhões por ano. Este negócio é operado em mais de 500 centros logísticos, em 15 países e gere mais de 100 mil caixas eletrónicas.

  A Prosegur Cash é líder global na prestação de serviços de logística e gestão de tesouraria, bem como de serviços terceirizados para instituições financeiras, distribuidores, agências publicas, bancos centrais, casas da moeda, joalherias e outras atividades comerciais pelo mundo fora, atuando principalmente nos setores de atividade bancária e da distribuição.

- **AVOS**: a Prosegur AVOS atua no setor de atividade de terceirização de soluções de negócios, projetando soluções inovadoras utilizando para o efeito as novas soluções tecnológicas.

  Na Prosegur AVOS, ajudamos nossos parceiros a melhorar suas operações permitindo ficar na vanguarda do mercado, assumindo os processos mais complexos e melhorando a experiência do cliente, desenvolvendo uma proposta de valor diferenciadora cujo objetivo principal se foca em aproveitar o conhecimento adquirido ao longo dos anos e adaptá-lo às novas tendências tecnológicas e digitais. O objetivo da Prosegur AVOS visa proporcionar aos seus clientes a máxima agilidade, rastreabilidade e visibilidade em todas as tarefas executadas na sua atividade.

- **Cibersegurança**: a Cipher é uma empresa global de segurança cibernética que presta uma vasta gama de serviços: v.g. 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 Avaliação de Segurança Detalhada (RTS, Red Team Services), Governança, Risco e Conformidade (GRC) e Integração de Tecnologias de Segurança Cibernética (CTI, Cybersecurity Technology Integration). Estes serviços contam com o suporte 24 horas do Cipher Labs, um laboratório de pesquisa e desenvolvimento de ameaças e inteligência cibernética de elite, assim como seis (6) Centros de Operações de Segurança (SOC, Security Operations Centers).

- Opera nos cinco continentes, visando o desafio de prestar serviços com maior valor acrescentado, ocupando uma posição de destaque no setor de segurança privada no mercado.

- Ademais, procura possuir uma forte presença geográfica com base em um modelo de negócios consolidado. Além da abordagem global, também atua localmente, em conformidade com as especificidades de cada mercado, dado que este setor de atividade é altamente regulamentado e varia de em conformidade com a legislação de cada país.

- Para além de ser líder mundial na prestação serviços de segurança privada, o Grupo PROSEGUR tem um firme compromisso com a sociedade civil em particular com os mais desfavorecidos, motivo pelo qual detém uma organização sem fins lucrativos, *in caso* a Fundação Prosegur, representando o compromisso do Grupo PROSEGUR em contribuir para o progresso das regiões mais carentes nos locais onde atua. O Grupo apoia a educação como um pilar axiomático para a mudança, do déficit no funcionamento cognitivo, promovendo ações de voluntariado que conduzam à solidariedade dos profissionais do Grupo PROSEGUR.

  Os projetos solidários desenvolvidos pela Fundação Prosegur nas áreas da educação, inclusão social, voluntariado empresarial e cultura, são implementados progressivamente nos diferentes países em que opera, levando em conta critérios de sustentabilidade, transparência e replicação de *best practices* recomendadas.

- A natureza global do 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 do globo; v.g. Europa, América Latina, EUA e resto do mundo, adotando para esse fim as presentes Regras Vinculativas Aplicáveis às Empresas, como definido infra.

2.1. Definições

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

- “**Acordo BCR**”: 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 BCR**”: entidade do Grupo PROSEGUR no alvo de aplicação do Acordo de BCR.

- **"Regras Vinculativas Aplicáveis às Empresas - BCR**" ou "**BCRs**”: significa as políticas de proteção de dados pessoais aderidas por um Responsável pelo Tratamento ou Subcontratante estabelecido no território de um Estado Membro para transferências ou um conjunto de transferências de Dados Pessoais para um Responsável pelo Tratamento ou Subcontratante estabelecido num ou mais Terceiros Países de um grupo de empresas ou de um grupo de empresas envolvidas em uma atividade econômica conjunta.

- **"Autoridade(s) de Controlo Competente(s)"**: significa Autoridade(s) de controlo de Proteção de Dados do EEE competente(s) para os Exportadores de Dados.

- "**Responsável pelo Tratamento**" ou "**Responsável**": pessoa física ou jurídica, autoridade pública, agência ou outro órgão que sozinho ou com outros determine os fins e os meios do Tratamento de Dados Pessoais.

- "**Exportador de Dados**": Entidade BCR estabelecida no Espaço Económico Europeu.

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

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

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

- "**Encarregado da Proteção de Dados**": pessoa responsável por orientar os Responsáveis e Subcontratantes sobre as suas obrigações, sob as leis de proteção de dados, monitorizar 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 execução da proteção de dados de cada Estado Membro.

- "**Espaço Económica 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 tratamento 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 autorizada de Dados Pessoais transmitidos, armazenados ou tratados 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.

- "**Tratamento**": qualquer operação ou conjunto de operações executadas nos Dados Pessoais ou nos conjuntos de Dados Pessoais, por meios automatizados ou não, como a coleta, registo, 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 Responsável do Grupo PROSEGUR.

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

- "**Destinatário**": pessoa física ou jurídica, autoridade pública, agência ou outro órgão a quem os Dados Pessoais sejam divulgados, seja terceiro ou não. No entanto, 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 tratamento desses dados por tais autoridades públicas deve cumprir com as regras de proteção de dados pertinentes de acordo com as finalidades do Tratamento;

- "**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**": cláusula padrão de proteção de dados adotadas pela Comissão Europeia de acordo com o procedimento de exame mencionado no artigo 93º nº 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 93º nº2 do RGPD;

- "**Autoridade de Supervisão**": uma autoridade pública independente, estabelecida num Estado Membro para monitorizar a aplicação do RGPD, com a finalidade de proteger os direitos e liberdades fundamentais de pessoas físicas em relação ao Tratamento de Dados e promover a livre circulação de Dados Pessoais dentro da União Europeia.

- " **País(es) Terceiro(s)**": países exteriores ao Espaço Económico Europeu.

- "**Terceiro(s)**": significa uma pessoa física ou jurídica, autoridade pública, agência ou órgão que não seja o Titular, o Responsável, o Subcontratante dos Dados ou pessoas que sob a autoridade direta do Responsável ou do Subcontratante, tenham autorização para Tratar Dados Pessoais.

3. Finalidade

3.1. Finalidade material

- Estas BCRs se aplicam a IDTs e ao Tratamento feito por Importadores de Dados como resultado de tais IDTs. Aplicam-se também, doravante, às Transferências Contínuas a Entidades de BCR e ao Tratamento realizado por estes como resultado das Transferências Subsequentes.

3.2. Âmbito Geográfico

3.2.1. Entidades e Pessoal sujeitos às BCRs

- Estas BCRs são vinculativas para todas as Entidades BCR e seu Pessoal. A lista atualizada das Entidades BCR consta no Anexo 1.

- A estrutura do Grupo PROSEGUR é apresentada na URL https://www.prosegur.com/en/about.

- Os dados de contato das Entidades BCR são disponibilizados, por país, nas URLs https://www.prosegur.com/en/legal-notice e https://www.prosegur.com/en/privacy-policy.

- O incumprimento por parte do Pessoal de qualquer das obrigações contidas nestas BCRs é considerado uma violação das instruções da PROSEGUR e/ou das Entidades BCR na sua qualidade de empregador ou empresário. Neste caso, a PROSEGUR e/ou as Entidades BCR reservam-se o direito de exercer as ações judiciais respetivas (incluindo, sem limitação, ações de Direito do Trabalho, Cíveis, Administrativas e/ou Penais), relacionadas aos danos causados como resultado de tal incumprimento, e de acordo com as disposições do acordo coletivo e/ou das cláusulas contratuais respetivas.

3.2.2. Dados Pessoais e atividades de Tratamento sujeitas às BCRs

- As atividades de Dados Pessoais, IDT e Tratamento sujeitas às BCRs são detalhadas no Mapa Internacional de Transferência de Dados como Anexo 2 e resumidas infra:

PAÍSES As BCRs serão aplicáveis às transferências feitas entre as Entidades BCR estabelecidas nos seguintes países:	**ESPAÇO ECONÓMICO EUROPEU**	**FORA DO ESPAÇO ECONÓMICO 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)
Trabalhadores/colaboradores/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 morada, propriedades, hobbies, associações a que pertence, licenças e autorizações) Dados académicos e profissionais (currículo e experiência profissional, qualificações, detalhes do cargo) Detalhes Económicos/financeiros/de seguros (dados Económicos da folha de pagamento, rendimentos, dados bancários; informações fiscais, seguros, planos de aposentação) 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) gestão de incidentes técnicos a diferentes áreas e negócios. Prestação de serviços de gestão de relacionamento com funcionários e RH entre as empresas do Grupo PROSEGUR: (i) Gestão de Folha de Pagamento; (ii) Prevenção de riscos ocupacionais Tarefas de gestão de equipas 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 telefónica, dados organizacionais e informações da empresa Criação de um identificador exclusivo para acesso à rede Prosegur Administração de expatriados Auditoria (avaliação de controlos internos) Administração de canal de denúncia Gestão de frotas Processos contabilísticos, fiscais e financeiros Contratos e administração jurídica Gestão de riscos Conformidade com obrigações legais (v.g. solicitação por parte 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 Gestão/conformidade de direitos e obrigações de proteção de dados (v.g., solicitações/reclamações do Titular dos Dados)
Candidatos	Dados de identificação e de contato, características pessoais, situação social, académica e profissional, vínculo laboral, dados Económicos e financeiros	Processos de recrutamento Prestação de serviços de informática entre as empresas do Grupo PROSEGUR:(i) suporte técnico; (ii) gestão de incidentes técnicos de ferramentas/sistemas digitais globais. Gestão/conformidade de direitos e obrigações de proteção de dados (v.g., solicitações/reclamações do Titular dos Dados)
Fornecedores e seus representantes ou pessoas de contato	Dados de identificação e contato, dados académicos e profissionais, laborais, económicos e financeiros, transações de bens e serviços, infrações	Gestão de relacionamento com fornecedores, incluindo contabilidade/fiscal/jurídico/legal Auditoria (avaliação de controlos internos) Administração do canal de denúncia Prestação de serviços de informática entre as empresas do Grupo PROSEGUR: (i) suporte técnico; (ii) ferramentas/sistemas digitais globais; gestão de incidentes técnicos para diferentes áreas e negócios. Conformidade com obrigações legais (v.g. solicitação das Autoridades Fiscais) Gestão de contratos Gestão da cadeia de fornecedores e compras Criação de um identificador exclusivo para acesso à rede Prosegur e proteção da rede Prosegur Gestão/conformidade de direitos e obrigações de proteção de dados (v.g., solicitações/reclamações do Titular dos Dados)

Utilizadores, clientes, potenciais clientes e representantes ou pessoas de contato de clientes e de potenciais clientes	Dados de identificação e contato, profissionais, laborais, económicos 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; gestão 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 prospeção 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 bases de dados Gestão do relacionamento com o cliente, incluindo contabilidade/fiscal/jurídico/legal Prestação de Serviços a Clientes Auditoria (avaliação de controlos internos) Administração do canal de denúncia Prevenção ao branqueamento de capitais e financiamento do terrorismo Conformidade com as obrigações legais (v.g. solicitação das Autoridades Fiscais) Gestão de contratos Gestão/conformidade de direitos e obrigações de proteção de dados (v.g., solicitações/reclamações do Titular dos Dados)
Inquilinos e proprietários	Dados de identificação e contato, académicos e profissionais, dados laborais, informações comerciais	Administração de propriedades Gestão de contratos
Representantes das empresas-alvo, pessoas de contato e funcionários	Dados de identificação e contato, características pessoais, académicas e profissionais, vínculo laboral, dados Económicos e financeiros	Avaliar o custo contencioso ou laboral da empresa para comprar Administração de sinistros
Beneficiários (incluindo menores)	Dados de identificação e contato, características pessoais, dados de saúde,	Prestação de serviços de informática entre as empresas do Grupo PROSEGUR: (i) suporte

	académicos e profissionais, vínculo laboral, dados Económicos e financeiros	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 tratados 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 "BCRs") como parte integrante do Acordo BCR, que visa regular os IDTs que possam ocorrer nas entidades sob seu escopo e que estão especificados no Anexo 1 destas BCRs.

5. Versão pública

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

6. Implementação

6.1. Princípios de tratamento de Dados Pessoais

6.1.1. Princípios aplicáveis ao Tratamento de Dados Pessoais

- O Tratamento de Dados Pessoais deve ser feito em conformidade com os seguintes princípios:

6.1.1.1 Princípio da legalidade

- O tratamento de Dados Pessoais deve ser lícito. O tratamento só é lícito na medida em que é aplicável pelo menos uma das seguintes condições; se:

  a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;

  b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

  c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;

f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

6.1.1.2 Justiça e transparência

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

6.1.1.3 Princípio da limitação da finalidade

- Os Dados Pessoais devem ser tratados para fins especificados, explícitos e legítimos e jamais de forma incompatível com essas finalidades.

6.1.1.4 Princípio de minimização de dados

- • Dados Pessoais que devem ser adequados, relevantes e limitados ao necessário para as finalidades para as quais são recolhidos. A minimização de dados deve ser aplicada tendo em conta a quantidade de dados recolhidos, a finalidade do seu tratamento e o prazo de conservação. O Acesso aos Dados também deve ser minimizado, de forma que somente o Pessoal ou Destinatários que objetivamente necessitem, possam aceder a estes para o cumprimento de uma obrigação ("*need-to-know*").

6.1.1.5 Princípio da precisão

- Os Dados Pessoais tratados devem ser precisos e encontrarem-se atualizados. Serão tomadas todas as medidas razoáveis para garantir que os Dados Pessoais que sejam inexatos – tendo em conta as finalidades para as quais são tratados - sejam apagados o mais celeremente possível.

6.1.1.6 Princípio de limitação da conservação

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

6.1.1.7 Princípio de integridade e confidencialidade

- Os Dados Pessoais devem ser tratados de forma a garantir a segurança apropriada dos Dados Pessoais, incluindo proteção contra tratamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, aplicando-se as medidas técnicas e/ou organizativas apropriadas.

6.1.1.8 Princípio de responsabilidade

- As Entidades BCR devem ser responsáveis e capazes de demonstrar o cumprimento de todos os princípios, direitos e obrigações previstos nestas BCRs. Elas também têm o ónus de demonstrar o cumprimento destes princípios, direitos e obrigações.

6.1.1.9 Proteção de Dados desde a conceção e por defeito

- Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente RGPD e proteja os direitos dos titulares dos dados.

- O Tratamento deve, desde o início, incorporar as medidas técnicas e organizativas que permitam a aplicação efetiva dos princípios estabelecidos nas Legislações Europeias da 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 *default* somente os Dados Pessoais necessários para cada finalidade da atividade de Tratamento sejam efetivamente tratados. A obrigação de implementar essas medidas aplica-se à quantidade de Dados Pessoais tratados, à extensão do seu Tratamento, ao período de conservação 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 conceção de um novo projeto, sistema, ferramenta ou processo em que esteja previsto o Tratamento de Dados Pessoais, as Entidades BCR levarão em conta a Proteção dos Dados Pessoais, adotando decisões e implementando medidas que garantam a conformidade com as Legislações Europeias de Proteção de Dados e restrinjam o Tratamento de Dados Pessoais ao que for estritamente necessário.

6.1.2. Tratamento de categorias especiais de Dados Pessoais

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

  a) O titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição de Tratamento desses Dados não possa ser levantada pelo Titular dos Dados:

b) O tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dado;

c) O tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento;

d) O tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contatos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares;

e) O tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;

f) O tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional;

g) O tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;

h) O Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde;

i) O tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;

j) O tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a

essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.

6.1.3. Medidas para garantir a segurança dos dados

- As Entidades BCR implementarão e aplicarão as medidas técnicas e organizativas adequadas para garantir um nível de segurança apropriado, tendo em consideração as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, 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 cifragem dos Dados Pessoais;

  b) capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;

  c) capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;

  d) verificação regular, e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

- As Entidades BCR devem tomar medidas para garantir que qualquer pessoa que atue sob sua responsabilidade e que tenha acesso a Dados Pessoais só o possa tratar sob as instruções do Responsável, a menos que seja obrigada a fazê-lo pelo direito da União ou de um Estado-Membro.

- Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

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

6.1.4. Modelo de Conformidade e Governança de Proteção de Dados

- As Entidades BCR designam um Encarregado da Proteção de Dados quando: (i) atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou (ii) atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos da Cláusula 6.1.2 ou Dados Pessoais relacionados a condenações e infrações criminais.

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

a) suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;

b) Monitorizar o cumprimento destas BCRs, com as disposições de proteção de Dados e com as políticas das Entidades da BCR sobre a proteção de Dados Pessoais, incluindo a atribuição de responsabilidades, conscientização e formação do pessoal envolvido nas operações de tratamento e auditorias relacionadas;

c) Sempre que solicitado, prestar orientações, no que respeita à Avaliação de Impacto da Proteção de Dados e monitorizar seu desempenho de acordo com a Cláusula 6.1.8;

d) Cooperar com a Autoridade de Controlo;

e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento incluindo a consulta prévia nos termos das Legislações Europeias, e consultar, quando apropriado, sobre qualquer outro assunto.

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

- A PROSEGUR também nomeou Encarregados Locais de Conformidade nos países onde um Encarregado de Proteção de Dados não é obrigatório de acordo com esta cláusula ou a legislação local. Esses Encarregados 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 BCRs) ao nível local, respondendo às equipas de gestão local e ao Encarregado da Proteção de Dados do Grupo.

- Tanto os Encarregados de Proteção de Dados quanto os Encarregados de Conformidade Local fazem parte e recebem o apoio do (i) Comité de Proteção de Dados Corporativo; (ii) Comité de Privacidade (Executivo); (iii) Responsável pelo Tratamento Funcional; e (iv) Controladores de teste, 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. Subcontratante e Subcontratantes ulteriores de Dados

serviços a um Subcontratante ulterior (seja uma Entidade BCR ou não), ela deverá, em primeira instância, usar somente Subcontratante ulterior que forneça as garantias suficientes para implementar medidas técnicas e organizativas apropriadas de forma que o tratamento cumpra os requisitos das BCRs e garanta a proteção dos direitos dos Titulares dos Dados. O mesmo se aplica quando uma Entidade BCR que atue como um Subcontratante queira contratar um Subcontratante ulterior, seja uma Entidade BCR ou não (doravante, "Subcontratante ulterior(es) de Dados" ou "Subcontratante ulterior(es)").

- O tratamento pelo Subcontratante ulterior, em nome do Responsável, será regido por um contrato ou outro ato normativo ("Contrato do Subcontratante de dados") ao abrigo do direito da União ou dos Estados-Membros que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de

dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento. Esse contrato ou outro ato normativo estipulam, designadamente, que o subcontratante:

a) trata os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso o responsável pelo tratamento desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;

b) assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;

c) adota todas as medidas exigidas nos termos da Cláusula 6.1.3;

d) respeite estas condições: (i) O Subcontratante não deve contratar Subcontratante ulterior sem autorização prévia escrita específica ou geral por parte do Responsável. No caso de uma autorização escrita, o Subcontratante deve informar o Responsável sobre quaisquer alterações pretendidas relacionadas à adição ou substituição de outros Subcontratantes ulteriores, dando assim ao Responsável a oportunidade de se opor a tais alterações; e (ii) quando um Subcontratante contratar outro Subcontratante ulterior para executar atividades de tratamento em nome do Responsável, as mesmas obrigações de proteção de dados estabelecidas no Contrato entre o Subcontratante e o Responsável serão estas impostas a esse Subcontratante ulterior com recurso a um contrato ou outro ato normativo, que dê garantias suficientes para aplicar medidas técnicas e organizativas adequadas de forma que o tratamento cumpra os requisitos destas BCRs. Quando esse Subcontratante ulterior não cumprir suas obrigações de Proteção de Dados, o Subcontratante inicial permanecerá totalmente responsável perante o Responsável por cumprir as obrigações desse Subcontratante ulterior.

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

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

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

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

i) o Subcontratante informará imediatamente o Responsável se, em sua opinião, uma instrução violar estas BCRs ou quaisquer disposições de Proteção de Dados do direito da União ou do Estado-Membro respetivo.

- Caso uma Entidade BCR queira subcontratar ao Subcontratante ulterior a totalidade ou parte dos serviços que lhe foram adjudicados, a Entidade BCR deverá obter prévia autorização - por escrito - específica ou geral, do Responsável pelo Tratamento. Quando for autorizado pelos representantes do Responsável pelo Tratamento a recorrer a um Subcontratante ulterior, o Subcontratante ulterior estará contratualmente vinculado a, pelo menos, as mesmas obrigações estipuladas no Contrato do Subcontratante, segundo as disposições destas BCRs.

- O Subcontratante é responsável perante o Responsável pelo Tratamento e será responsável por cumprir efetivamente as obrigações de Proteção de Dados pelo Subcontratante ulterior.

- O Subcontratante compromete-se a notificar o Responsável pelo Tratamento, com antecedência e por meios rastreáveis, sobre possíveis alterações planeadas em termos de adição ou substituição de Subcontratante ulterior(es), dando ao Responsável pelo Tratamento a oportunidade de se opor a tais alterações.

- Para os efeitos supramencionados, as Entidades BCR 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 BCRs também devem ser observadas.

6.1.6. Violações de Dados Pessoais

- Em caso de ocorrência, ou se suspeite que tenha ocorrido, uma violação de segurança que possa afetar os Dados Pessoais, a pessoa que a detetar deverá informar de imediato e sem demora o Encarregado da Proteção de Dados Local/Encarregado de Conformidade Local o qual informará de imediato a PROSEGUR (através do Encarregado da Proteção de Dados do Grupo), de acordo com o Protocolo de Gestão e Notificação de Violação de Dados Pessoais, constante como Anexo 6.

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

- As Entidades BCRs que atuam como Responsável devem notificar a Autoridade de Controlo 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 setenta e duas (72) horas após o Responsável pelo Tratamento 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 num alto risco para os seus direitos e liberdades.

- Quando uma Entidade BCR que atue como Subcontratante tiver conhecimento de uma Violação de Dados Pessoais, essa Entidade deverá informar imediatamente a PROSEGUR (ao Encarregado da Proteção de Dados do Grupo), o qual é responsável por notificar - sem atraso indevido - a Entidade BCR na qualidade de Responsável pelo Tratamento, a fim de - se aplicável - serem executadas as notificações exigidas pelas presentes BCR.

6.1.7. Registo das atividades de Tratamento

- As Entidades BCRs que atuam como Responsáveis devem manter um Registo das Atividades de Tratamento (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 os contatos do responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados ou do Grupo;

b) as s finalidades do tratamento dos dados;

c) uma descrição das categorias de titulares de dados e das categorias de dados pessoais;

d) As s categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais;

e) Quando aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais que seja o Destinatário dos Dados e, quando aplicável, a documentação das salvaguardas adequadas

f) sempre que possível, os prazos previstos para o apagamento das diferentes categorias de dados;

g) sempre que possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas na Cláusula 6.1.3 destas BCRs.

- As Entidades BCRs que atuam como Subcontratante, quando aplicável, o representante do Subcontratante devem manter um ROPA de todas as categorias de atividades de Tratamento realizadas em nome de um Responsável, contendo:

a) o nome e detalhes de contato do Subcontratante(es) e de cada Responsável em nome do qual o Subcontratante está a atuar e, se aplicável, do Responsável ou representante do Subcontratante e do Encarregado da Proteção de Dados Local ou do Grupo;

b) as categorias de Tratamento tratadas em nome de cada Responsável;

c) se 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 BCRs, a documentação de salvaguardas adequadas;

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

6.1.8. Avaliações do Impacto da Proteção de Dados

- As Entidades BCR devem fazer uma Avaliação do Impacto sobre a Proteção de Dados (doravante, "DPIA" ou "*Data Protection Impact Assessment*") antes de iniciar o Tratamento de Dados Pessoais, sempre que um determinado tipo de tratamento envolver um alto risco para os direitos e liberdades dos Titulares dos Dados.

- Essas avaliações serão elaboradas de acordo com a metodologia estabelecida pelo Grupo PROSEGUR, com a orientação do Encarregado de Proteção de dados do Grupo ou do Encarregado Local de Proteção de Dados. O objetivo é avaliar a necessidade e proporcionalidade do tratamento, identificar os riscos e estabelecer as medidas necessárias para os mitigar.

- Para esta finalidade, as Entidades BCR devem observar e cumprir o Protocolo de Gestão de DPIA do Grupo PROSEGUR, constante no Anexo 7.

- Sempre que, após a realização de um DPIA, uma Entidade BCR identificar um alto risco que não possa ser mitigado, tal Entidade deve consultar a Autoridade de Controlo relevante antes de realizar o Tratamento 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 estiverem cumpridos os seguintes requisitos:

    a) o Importador de Dados está vinculado e poder cumprir essas BCRs. A título de esclarecimento, estas BCRs 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 BCR devem tomar as devidas salvaguardas, e na condição de que os direitos que assistem aos Titulares dos Dados e respetivos recursos legais 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 Responsável ou Subcontratante 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 Responsável ou Subcontratante 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 numa das seguintes condições:

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

b) houver uma decisão de um tribunal ou uma decisão vinculativa de uma autoridade administrativa de um Terceiro País exigindo que o Responsável ou o Subcontratante 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 a execução de um contrato entre o Titular dos Dados e o Responsável ou para 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 Responsável e outra pessoa física ou coletiva; (iii) por motivos 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 Responsável que não sejam anulados pelos interesses ou direitos e liberdades do Titular dos Dados, e (iv) o Responsável 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 Responsável deve informar a Autoridade de Controlo da transferência. O Responsável 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 BCR

Em geral, os requisitos estabelecidos na Cláusula 6.2.1 supra devem ser cumpridos e observados. Em caso de dúvida, o Importador dos Dados deve informar o Exportador e obter sua autorização expressa.

6.2.2.2 Quando o Destinatário não for uma entidade BCR

O Importador 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 Subcontratante

Quando as divulgações de dados forem baseadas num relacionamento do Subcontratante, esse relacionamento deve ser executado por escrito, com base no Modelo de Contrato do Subcontratante 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 Responsáveis são obrigados a proporcionar informações aos Titulares dos Dados, conforme infra especificado:

a) Quando os Dados Pessoais são recolhidos junto do titular, no momento da recolha dos Dados Pessoais, os Titulares dos Dados devem receber as seguintes informações:

(i) a identidade e os contatos do responsável pelo tratamento e, se for caso disso, do seu representante;

(ii) os contatos do encarregado da proteção de dados, se for caso disso;

(iii) as finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;

(iv) se o tratamento dos dados se basear nos interesses legítimos do responsável pelo tratamento ou de um terceiro;

(v) os destinatários ou categorias de destinatários dos dados pessoais, se os houver;

(vi) se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação, ou a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.

Além das informações supra, o Responsável deverá, no momento da coleta dos Dados Pessoais, proporcionar ao Titular dos Dados as seguintes informações adicionais necessárias para garantir um tratamento justo e transparente:

(i) o de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;

(ii) a existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;

(iii) se o Tratamento 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 Tratamento baseado no consentimento anterior à sua retirada;

(iv) o direito de registar reclamação a uma Autoridade de Controlo;

(v) se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;

(vi) quando exequível, 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 Tratamento para o Titular dos Dados.

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

b) Quando os Dados Pessoais não tiverem sido recolhidos junto do Titular dos Dados, o Responsável transmitirá ao Titular dos Dados as seguintes informações:

(i) a identidade e os contatos do responsável pelo tratamento e, se for caso disso, do seu representante;

(ii) os contatos do encarregado da proteção de dados, se for caso disso;

(iii) as s finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;

(iv) as categorias dos dados pessoais em questão;

(v) os destinatários ou categorias de destinatários dos dados pessoais, se os houver;

(vi) se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação, ou a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.

Além das informações supra, o Responsável deverá, no momento da coleta dos Dados Pessoais, proporcionar ao Titular dos Dados as seguintes informações adicionais necessárias para garantir um tratamento justo e transparente:

(i) o prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo;

(ii) Se o tratamento dos dados se basear nos interesses legítimos do responsável pelo tratamento ou de um terceiro;

(iii) a existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, e a retificação ou o apagamento, ou a limitação do tratamento no que disser respeito ao titular dos dados, e do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;

(iv) quando o Tratamento 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 Tratamento baseado no consentimento anterior à sua retirada;

(v) o direito de registar reclamação a uma Autoridade de Controlo;

(vi) a origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público;

(vii) a existência de decisões automatizadas, incluindo a definição de perfis e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

O Responsável deve comunicar as informações supramencionadas; (a) num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados; (b) se e os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados; ou (c) se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados.

Quando o responsável pelo tratamento tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados pessoais tenham sido obtidos, antes desse tratamento o responsável fornece ao titular dos dados informações

sobre esse fim e quaisquer outras informações pertinentes referidas 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 tenha conhecimento das informações;

(ii) Se comprove a impossibilidade de disponibilizar a informação, ou que o esforço envolvido seja desproporcionado, nomeadamente para o tratamento para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, sob reserva das condições, e na medida em que a obrigação seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento. Nesses casos, o responsável pelo tratamento toma as medidas adequadas para defender os direitos, liberdades e interesses legítimos do titular dos dados, inclusive através da divulgação da informação ao público;

(iii) a obtenção ou divulgação dos dados esteja expressamente prevista no direito da União ou do Estado-Membro ao qual o responsável pelo tratamento estiver sujeito, prevendo medidas adequadas para proteger os legítimos interesses do titular dos dados; ou

(iv) onde dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada pelo direito da União ou de um Estado-Membro, inclusive uma obrigação legal de confidencialidade.

6.3.2. Outros direitos

- Os Titulares dos Dados podem exercer estes direitos:

(i) **Acesso**: o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:

a) as finalidades do tratamento dos dados;
b) as categorias dos dados pessoais em questão;
c) os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais.
d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;
e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;
f) o direito de apresentar reclamação a uma autoridade de controlo;
g) se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;

h) a existência de decisões automatizadas, incluindo a definição de perfis, e pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

O responsável pelo tratamento fornece uma cópia dos dados pessoais em fase de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrónico de uso corrente.

O direito de obter uma cópia não prejudica os direitos e as liberdades de terceiros.

(ii) **Retificação**: obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.

(iii) **Apagamento ("direito de ser esquecido")**: O Titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:

a) os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
b) o retira o consentimento em que se baseia o tratamento dos dados nos termos da Cláusula 6.1.1.1., ou Cláusula 6.1.2., e se não existir outro fundamento jurídico para o referido tratamento;
c) o titular opõe-se ao tratamento nos termos do ponto (vi);
d) os Dados Pessoais foram Tratados ilicitamente;
e) os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;
f) os Dados Pessoais tenham sido recolhidos numa relação de oferta de serviços da sociedade da informação diretamente a uma criança.

Quando o Responsável tiver tornado públicos os dados pessoais e for obrigado a apagá-los, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.

O direito ao apagamento não se aplica na medida em que o tratamento se revele necessário:

O direito ao apagamento não se aplica na medida em que o tratamento se revele necessário:

a) ao exercício da liberdade de expressão e de informação;

b) ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado- -Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;
c) por motivos de interesse público no domínio da saúde pública, nos termos 6.1.2.
d) para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, de acordo o direito da União ou do Estado, medida em que o direito seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou
e) para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

iv) **Limitação do tratamento**: O Titular dos Dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma das seguintes situações:

a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão;
b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;
c) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;
d) tiver oposto ao tratamento até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

Quando o tratamento tiver sido limitado, os dados pessoais só podem, à exceção da conservação, ser objeto de tratamento com o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos ponderosos de interesse público da União ou de um Estado-Membro

O titular que tiver obtido a limitação do tratamento deve ser informado pelo responsável pelo tratamento antes de ser anulada a limitação ao referido tratamento.

(v) **Portabilidade de dados**: O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se: a) o tratamento se basear no consentimento dado nos termos das Cláusulas 6.1.1.1. e 6.1.2.; e b) o tratamento for realizado por meios automatizados.

Ao exercer o seu direito de portabilidade dos dados nos termos do n.º 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.

O exercício do direito à portabilidade dos dados (a) esse direito não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade

pública de que está investido o responsável pelo tratamento; e (b não prejudica os direitos e as liberdades de terceiros.

(vi) **Direito de oposição**: O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe 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 responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.

O mais tardar no momento da primeira comunicação ao titular dos dados, o direito é explicitamente levado à atenção do titular dos dados e é apresentado de modo claro e distinto de quaisquer outras informações

No contexto da utilização dos serviços da sociedade da informação, o titular dos dados pode exercer o seu direito de oposição por meios automatizados, utilizando especificações técnicas.

Quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, o titular dos dados tem o direito de se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, salvo se o tratamento for necessário para a prossecução de atribuições de interesse público.

- O Responsável deverá comunicar qualquer retificação ou apagamento de Dados Pessoais ou restrição de tratamento realizado de acordo com esta Cláusula a cada Destinatário a quem os Dados Pessoais foram divulgados, a menos que isso se mostre inexequível ou envolva esforço desproporcional. O Responsável 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

- O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar ("decisões individuais automatizadas"), a menos que seja aplicável uma das seguintes exceções: (i) a decisão seja necessária para celebrar ou execução de um contrato entre o titular dos dados e um responsável pelo tratamento; (ii) a autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou (iii) a decisão baseada no consentimento explícito do titular dos dados.

- Nas exceções mencionadas nos pontos (i) e (iii) supra, o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão.

- Ademais, 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 sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

6.3.4. Direito de apresentar reclamação

- Os titulares de dados têm direito a apresentar reclamação a uma autoridade de controlo, caso considerem que o tratamento dos seus Dados Pessoais viole estas BCRs, em especial à autoridade de controlo (i) no Estado-Membro da sua residência habitual; (ii) no Estado Membro do seu local de trabalho ou do loca; ou (iii) no Estado Membro onde foi alegadamente praticada a infração.

6.3.5. Direito à ação judicial

- Os Titulares dos Dados têm direito à ação judicial em relação ao Subcontratante ou Responsável se estes considerarem que os seus direitos sob essas BCRs foram violados em resultado do tratamento de seus Dados Pessoais, não obstante a qualquer recurso administrativo ou extrajudicial. As ações contra o Responsável ou Subcontratante são propostos nos tribunais do Estado Membro em que tenham estabelecimento ou em alternativa nos tribunais do Estado- -Membro em que o titular dos dados tenha a sua residência habitual.

- Quando a infração tiver sido causada por uma Entidade BCR 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 apresentar uma reclamação remetendo para o efeito uma solicitação por escrito para o endereço postal da Entidade BCR que atua na qualidade de Responsável, para os endereços de correio eletrónico indicados nas Políticas de Privacidade das Entidades BCR ou ao seguinte endereço de correio eletrónico oficina.privacidad@prosegur.com. Se a Entidade BCR tiver dúvidas razoáveis quanto à identidade do Titular dos Dados que fez a solicitação, a Entidade BCR poderá solicitar tal informação adicional necessária para confirmar a identidade do Titular dos Dados.

- Os Titulares dos Dados devem receber, sem demoras uma resposta sobre o exercício dos seus direitos e em todos o caso dentro de um (1) mês da receção do pedido. Esse prazo poderá – quando necessário - ser prorrogado por mais 2 (dois) meses. Para os devidos efeitos depende da complexidade e quantidade de solicitações recebidas. O Titular dos Dados deverá ser informado sobre tal prorrogação dentro de 1 (um) mês contado do momento da receção do pedido, com a justificação do(s) motivo(s) desse atraso.

- Será enviada uma resposta aos Titulares dos Dados, aceitando ou rejeitando a solicitação/reclamação. Os Titulares dos Dados serão também informados, caso não

fiquem satisfeitos com a resposta recebida, que terão o direito de apresenta uma reclamação junto à autoridade de controlo competente, assim como poder interpor recurso judicial, nos termos das Cláusulas 6.3.4 e 6.3.5 supra.

6.4. Direitos de terceiros beneficiários

- As Entidades BCR 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 BCR como terceiros beneficiários.

6.5. Reclamações

- Não obstante o disposto na Cláusula 7 destas BCRs, os Titulares dos Dados podem exercer todo os direitos que lhes assistam ou apresentar uma reclamação sobre o Tratamento dos seus Dados pelas Entidades BCR e sua aplicação de BCRs seguindo o procedimento indicado na Cláusula 6.3.6.

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

6.6. Ações para implementar BCRs

6.6.1. Formação do pessoal

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

- As Entidades BCR e os Encarregados Locais de Proteção de Dados/Conformidade, com o apoio do Encarregado da Proteção de Dados do Grupo, são responsáveis por definir o formato dos cursos de formação e sensibilização (presencial ou online), bem como a frequência das formações.

- Distintivamente são realizadas anualmente as seguintes ações de formação e conscientização: (i) uma sessão geral sobre questões de privacidade e Proteção de Dados; e (ii) uma sessão específica sobre BCRs.

- A sessão geral sobre questões de privacidade aborda, entre outras temáticas, o impacto da privacidade na atividade do Grupo PROSEGUR e dos seus trabalhadores/colaboradores e as políticas e normas adotadas no Grupo PROSEGUR. Todo o Pessoal da Prosegur deverá frequentar estas sessões de formação.

- A sessão específica sobre questões de BCR abrange o conteúdo desta BCR, incluindo os anexos relevantes e deverá contar com a presença de todo o Pessoal que tenha acesso permanente ou regular a Dados Pessoais, que esteja envolvido na recolha de Dados ou no desenvolvimento das ferramentas que tratam os Dados Pessoais.

- As sessões de formação e conscientização são realizadas pela Plataforma Online da Universidade Prosegur (Universidade PROSEGUR – UP), acessível através da Intranet do Grupo PROSEGUR. Os conteúdos das sessões de formação e conscientização são um misto de teoria e prática, incluindo um questionário de avaliação que deve ser aprovado (i.e., 7 em 10 respostas corretas) para considerar o curso “frequentado e concluído”. A Universidade Prosegur

utiliza a plataforma online para gerir 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 BCRs. As informações estão incluídas nos materiais entregues ao Pessoal no momento da incorporação (*on boarding*), publicados na intranet do Grupo PROSEGUR e das Entidades BCR e promovidas por meio de notificações.

6.6.2. Monitorização da conformidade com a BCR

- O Encarregado da Proteção de Dados do Grupo e o Comitê de Proteção de Dados Corporativos, com o apoio dos Encarregados Locais de Proteção de Dados/Conformidade e dos órgãos de gestão das Entidades BCR, são responsáveis por supervisionar a implementação destas BCRs

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

  (i) Informar e aconselhar as Entidades BCR e o pessoal que realiza o tratamento sobre as suas obrigações ao abrigo da BCR e pela legislação de Proteção de Dados da União Europeia. O Encarregado de Conformidade/Proteção de Dados Local reporta diretamente ao nível mais alto da hierarquia da Entidade BCR.

  (ii) monitorizar o cumprimento do disposto na BCR e da Legislação Europeia de Proteção de Dados, e das políticas da PROSEGUR, incluindo a atribuição de responsabilidades, conscientização e formação do pessoal envolvido nas operações de tratamento.

  (iii) atuar como ponto de contato com as autoridades de controlo em questões relacionadas a operações de Tratamento de Dados e implementação de BCR, bem como cooperar com as investigações conduzidas por estas autoridades.

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

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

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

6.6.3. Verificação de conformidade BCR

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

- Os resultados das avaliações e auditorias devem ser comunicados ao Encarregado da Proteção de Dados do Grupo, ao Encarregado da Proteção de Dados/ Encarregado de Conformidade Local, ao Comité de Proteção de Dados Corporativos e à Direção da Entidade BCR em causa.

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

- Em caso de incumprimento da BCR, os relatórios incluem recomendações e medidas corretivas a implementar pela Entidade BCR 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 BCR do escopo da BCR.

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

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

6.6.4. Atualizações de BCR

- As BCRs são revistas e atualizadas, em caso de alterações, seja na Legislação Europeia de Proteção de Dados ou em qualquer conteúdo das BCRs (incluindo seus Anexos). O Encarregado da Proteção de Dados do Grupo é o responsável por revier regularmente as BCRs e alterar conforme necessário para mantê-las atualizadas, devendo proceder da seguinte forma:

  (i) manter um registo atualizado das Entidades BCR e atualizações de BCR, bem como exibir tais detalhes nas BCRs;

  (ii) monitorizar as mudanças regulatórias, registrando-as e adicionando-as à BCR;

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

- Alterações nas BCRs (que incluam, entre outros, a lista de Entidades BCR) são comunicadas a todas as Entidades BCR sem demora indevida.

- As alterações nas BCRs ou na lista de Entidades BCR são comunicadas às autoridades de controlo, por meio da autoridade de controlo principal, uma vez por ano juntamente com uma explicação dos motivos. Quando as alterações nas BCRs puderem afetar o nível de proteção oferecido pelas BCRs ou afetar significativamente as BCRs, essas alterações devem ser notificadas com antecedência às autoridades de controlo competentes, por meio da autoridade de controlo 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 BCR até que a nova Entidade BCR esteja efetivamente vinculada às BCRs e possa cumpri-las.

6.6.5. Não conformidade da BCR

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

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

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

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

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

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

- O mesmo se aplica a quaisquer cópias dos Dados e Transferências Subsequentes. As Entidades BCR certificarão a exclusão dos Dados ao Exportador de Dados. Até que os Dados sejam excluídos ou devolvidos, as Entidades BCR continuarão garantindo a conformidade com a BCR. No caso de leis locais aplicáveis às Entidades BCR que proíbam a devolução ou exclusão dos Dados Pessoais transferidos, as Entidades BCR garantem que continuarão assegurando a conformidade com a BCR 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 BCRs pelos seguintes meios:

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

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

  (iii) inclusão de referências a BCRs 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 BCRs.

- Adicionalmente, os Titulares dos Dados podem solicitar por escrito uma cópia das BCRs, 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 corrigir os atos das Entidades BCR localizadas fora do EEE e pagar uma indemnização por quaisquer danos materiais ou imateriais resultantes da violação das BCRs por essas Entidades BCR 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 BCR no caso de uma Transferência Subsequente. Caberá à PROSEGUR o ónus de provar que as BCR não foram violadas ou que o evento gerador do dano não é, de forma alguma, da responsabilidade da Entidade ou Entidades BCR em causa.

- Nos casos em que a violação destas BCRs tenha sido cometida por uma Entidade BCR 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 BCR 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 Controlo

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

  (i) fornecer todas as informações exigidas pelas Autoridades de Controlo no que diz respeito às BCRs e ao tratamento exigido;

  (ii) permitir sua auditoria por parte das autoridades de controlo;

  (iii) implementar as recomendações feitas pelas autoridades de controlo;

  (iv) remeter os relatórios de verificação/auditorias de conformidade da BCR exigidos pelas autoridades de controlo;

  (v) comunicar alterações às BCRs às autoridades de controlo.

6.8.2. Relacionamento com as legislações locais

6.8.2.1 Compatibilidade com as legislações locais

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

- As Entidades BCRs garantem que não têm motivos para acreditar que as leis e práticas nos Terceiros Países de destino previstos aplicáveis ao Tratamento 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 BCRs.

- 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 BCR:

  a) segurança nacional;

b) defesa;

c) segurança pública;

d) a prevenção, investigação, deteção 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 da União Europeia ou de um Estado Membro, nomeadamente um interesse económico 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, deteção e repressão das infrações à ética das profissões regulamentadas;

h) uma função de monitorização, 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 País Terceiro que possam afetar o cumprimento dos compromissos contidos na BCR, as Entidades da BCR 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 País Terceiro ou para outro País Terceiro, incluindo:

    - finalidades para as quais os Dados Pessoais são transferidos e tratados (por exemplo, marketing, RH, armazenamento, suporte de TI, etc.);
    - tipos de entidades envolvidas no tratamento (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 tratamento, incluindo armazenamento;
    - canais de transmissão utilizados.

  (i) As leis e práticas do País Terceiro 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;

  (ii) Quaisquer salvaguardas contratuais, técnicas ou organizativas relevantes implementadas para complementar as salvaguardas sob as BCRs, incluindo medidas aplicadas durante a transmissão e o Tratamento dos Dados Pessoais no país de destino.

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

- As Entidades BCR 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 monitorizar, 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 legislações locais

- Qualquer Entidade BCR atuando como Importador ou Destinatário de Dados deve notificar imediatamente o Exportador de Dados se, ao usar esta BCR como uma ferramenta para IDT e durante sua associação à BCR, 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 BCR, inclusive após uma alteração nas leis do País Terceiro ou uma medida (como uma solicitação de divulgação). Esta informação deverá também ser levada à PROSEGUR e ao Encarregado da Proteção de Dados do Grupo.

- Após verificar tal notificação, a Entidade BCR que atua como Exportadora de Dados, juntamente com a PROSEGUR, o Encarregado da Proteção de Dados do Grupo e o Encarregado 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 BCR que atua como Exportadora de Dados e/ou pela Entidade BCR que atua como Importadora de Dados para permitir que cumpram suas obrigações sob a BCR. O mesmo se aplica caso uma Entidade BCR que atua como Exportadora de Dados tiver motivos para acreditar que uma Entidade BCR que atua como Importadora de Dados ou Destinatária de uma Transferência Subsequente não possa mais cumprir suas obrigações sob esta BCR.

- Quando a Entidade BCR na qualidade de Exportador de Dados, juntamente com a PROSEGUR, o Encarregado da Proteção de Dados do Grupo e o Encarregado da Proteção de Dados/Encarregado de Conformidade relevante avaliar que nenhuma salvaguarda adequada para o IDT ou conjunto de IDTs pode ser garantida ou se instruída pela(s) autoridade(s) de controlo 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 Encarregado da Proteção de Dados do Grupo e o Encarregado de Conformidade/Proteção de Dados Local relevantes e competentes informarão todas as outras Entidades BCR 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 BCR ou, caso não possam ser aplicadas medidas complementares eficazes, o IDT em causa será suspenso ou encerrado.

- Após essa suspensão, a Entidade BCR 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 BCR 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 BCR, a PROSEGUR notificará as autoridades de controlo 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 controlo 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 BCR solicitadas envidarão todos os esforços para obter o direito de renunciar esta proibição de divulgação às autoridades de controlo 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 BCR não conseguirem notificar as autoridades de controlo competentes, as Entidades BCR comprometem-se a fornecer anualmente às autoridades de controlo 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 BCR a autoridades públicas não devem ser massivas, desproporcionais ou indiscriminadas, de modo a limitar-se ao que é necessário numa sociedade democrática para proteger interesses específicos importantes, incluindo a segurança pública e a prevenção, investigação, deteção e repressão de infrações criminais ou execução de penalidades criminais, incluindo a proteção e prevenção de ameaças à segurança pública.

6.9. Duração

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

ANEXOS

7. Anexos

7.1. Anexo 1 - Entidades BCRs

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

7.2. Anexo 2 - Quadro de Transferências de Dados Internacionais

Um resumo da Transferência Internacional de Dados expectada ou executada atualmente está incluída na **Cláusula 3.2.2.** das BCRs.

Nessa cláusula poderá obter as informações relevantes sobre os países de onde os Dados Pessoais são ou serão exportados, os Terceiros Países de destino atuais ou expectados, os grupos de Titulares de Dados afetados e os tipos dos Dados que serão transferidos, bem como as finalidades do seu tratamento.

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 BCRs, poderá 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

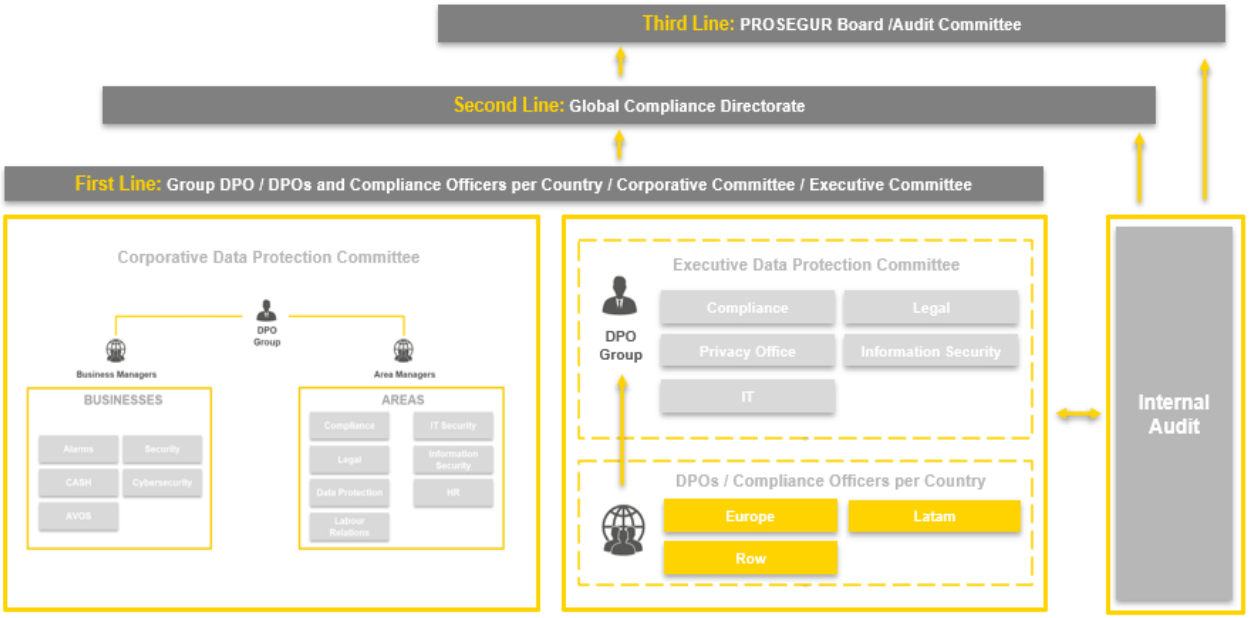
O Modelo de Governança para Conformidade em assuntos de Proteção de Dados é uma política interna e confidencial pela qual o Grupo PROSEGUR estabelece as bases do seu sistema interno de Proteção de Dados Pessoais. as políticas e procedimentos associados. Esta Política declara:

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 BCRs.

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 BCRs.

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

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:



- **Comité de Proteção de Dados Corporativos**

  O Comité de Proteção de Dados Corporativos, liderado e presidido pelo DPO do Grupo, reúne-se semestralmente e é constituído por de um membro das principais áreas e negócios da PROSEGUR, denominado Gerente de Tratamento Funcional, a quem caberá acompanhar as ações que foram definidas para garantir a conformidade no campo da Proteção de Dados na sua área de competência, respondendo ao Encarregado de Conformidade/DPO Local e/ou do Grupo informando sobre o nível de conformidade com as ações implementadas. Esse Comité 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 tratamento de Dados Pessoais.
  - Informar sobre os resultados das avaliações objetivas dos riscos, bem como das novas atividades de Tratamento identificadas no âmbito da sua competência, (negócio/área/departamento), incorporando as novas atividades de tratamento 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 tratamento de Dados Pessoais e definir o formato dos cursos de formação e a sua frequência.

- **Comité Executivo de Proteção de Dados**

- O Comité Executivo de Proteção de Dados é representado 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 fornecedor que trate dados pessoais. Esta Política resume, que:

- As Entidades BCR só podem contratar fornecedores que ofereçam garantias suficientes para implementar as medidas técnicas e organizativas adequadas, por forma a garantir que a atividade que envolva o tratamento de Dados Pessoais seja realizada de acordo com os requisitos estabelecidos pelas BCRs a esse respeito e garantindo a proteção dos direitos dos titulares dos dados. Ademais se aplica quando uma Entidade BCR atuando como Subcontratante deseja contratar um Subcontratante Ulterior, seja esta uma Entidade BCR ou não.

- Essas garantias estão contidas, entre outros elementos, na competência, confiabilidade e recursos, visando implementar as medidas técnicas e organizativas correspondentes ao cumprimento dos requisitos das BCRs, incluindo a segurança do tratamento. Nesse sentido, a adesão do Subcontratante 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 fornecedor que trata dados pessoais inicia-se com o envio de um questionário de avaliação do fornecedor, o qual deve ser preenchido antes de ser efetuada a contratação. O questionário assim como 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 seu nível de conformidade e determinar se as medidas de segurança implementadas são adequadas e satisfatórias 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 corrija as deficiências identificadas na avaliação e certifique a correção apresentado as evidências apropriadas.

- As Entidades BCR também têm o direito de auditar as instalações e sistemas do fornecedor que trate dados pessoais e solicitar o acesso a determinada documentação que comprove a conformidade com as BCRs, como seus Registos de Atividades de Tratamento, compromissos de confidencialidade assinados com seus funcionários e colaboradores, certificados de formação em Proteção de Dados, certificados de ter sido avisado sobre o assunto ou ter sido auditado etc.

- A relação com o fornecedor será regida por um contrato ou outro ato normativo de acordo com as Legislações Europeias, que vincule o Subcontratante ao Responsável pelo Tratamento. Os requisitos mínimos deste contrato estão descritos na **Cláusula 6.1.5.** das BCRs.

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

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

7.7. Anexo 7 - Protocolo de Gestão de DPIA

A Avaliação do Impacto sobre a 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 fornecedor que trate dados pessoais. Este protocolo resume, que:

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

- Este processo de avaliação deve ser realizado antes do início de qualquer operação de tratamento 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. Porém, nada impede que uma DPIA seja feita para um fornecedor já esteja em pleno atividade.

- As Entidades de BCR devem fazer uma DPIA quando for provável que a natureza, finalidade, ou contexto de um tipo de tratamento, 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 tratamento previstas e das finalidades do tratamento, incluindo, quando sempre que oportuno, o interesse legítimo das Entidades BCR;

    - uma avaliação da necessidade e proporcionalidade das operações de tratamento 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 legislações, tendo em consideração os direitos e interesses legítimos dos Titulares dos Dados e outras de pessoas físicas afetadas.

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

O Protocolo de Tratamento de Reclamações e Reclamações BCR PROSEGUR é um protocolo interno e confidencial. Na **Cláusula 6.3.6** das BCRs poderá encontrar as informações relevantes e públicas sobre este tema.

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, a sua finalidade, ações envolvidas e meios, entre outros aspectos, com o objetivo de verificar a conformidade das Entidades BCR com as BCRs.

O programa de auditoria resume, que:

- A conformidade das Entidades BCR com as legislações locais de Proteção de Dados e as políticas e códigos internos do Grupo PROSEGUR é constantemente avaliada pelo Encarregado 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, registos de Atividades de Tratamento, sistemas associados, reclamações e solicitações recebidas, etc.) bem como o nível de cumprimento dos controlos de Proteção de Dados do Grupo PROSEGUR. Ademais os DPOs/Encarregados de Conformidade Locais devem se reportar trimestralmente ao Encarregado de Proteção de Dados do Grupo e o Encarregado de Proteção de Dados do Grupo reporta à Direção da PROSEGUR, a qual representa o nível mais alto de gestão do Grupo.

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

    - **Avalições anuais**: Anualmente, cada Entidade BCR responderá a um questionário sobre o cumprimento das BCRs. Estes questionários medirão o nível de implementação da Entidade BCR e o seu grau de eficácia. Com base nas informações fornecidas, será elaborado um relatório pelo Departamento de Auditoria Interna, o qual será enviado ao Encarregado de Proteção de Dados do Grupo assim como para os Encarregados Locais de Proteção/Encarregados de Dados do país relevante, para que seja enviado por sua vez ao Comité 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 BCRs. Será elaborado um relatório pela Auditoria Interna, que será enviado ao Encarregado de Proteção de Dados do Grupo e para os Encarregados Locais de Proteção/Conformidade de Dados do país relevante, para que seja enviado por sua vez ao Comité de Proteção de Dados Corporativos. Os relatórios de auditoria resultantes serão também comunicados ao órgão de administração e gerenciamento da Entidade BCR em causa e à Direção da PROSEGUR.

      Em caso de incumprimento da BCR, os relatórios incluirão recomendações e medidas corretivas a implementar pela Entidade BCT em causa, dentro de um prazo especificado. Caso as recomendações e medidas corretivas não sejam devidamente implementadas, o fato é comunicado à Direção da PROSEGUR, para as devidas decisões; incluindo, entre outros, a exclusão da Entidade BCR do objetivo da BCR.

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

PROSEGUR