REGRAS **CORPORATIVAS** VINCULANTES DA CAPGEMINI

Atividades do controlador

Versão interna

COMPANY CONFIDENTIAL · SEC 1 · Capgemini Document

Índice

Histórico de versões

Histórico de versões		
Versão	Data	Comentários
1.0	2016	Versão inicial comunicada à CNIL e aprovada pela CNIL por ofício.
2.0	2018	Reescrita completa das Regras Corporativas Vinculativas
3.0	2023	Atualizado após a decisão Schrems II
4.0	2024-2025	Atualização e reformulação das Regras Corporativas Vinculativas, separadas em versões de Controlador e Operador para cumprir os requisitos do Conselho Europeu de Proteção de Dados (EDPB) e garantir melhor legibilidade.
Autores e colaboradores		
Papel	Atividade	Comentários
Nathalie Laneret	DPO do Grupo	
Luísa Achache	Consultor Jurídico Sênior de Proteção de Dados	
Distribuição de documentos		
Papel	Localização	Ação/Informação
CNIL	Paris, França	Para revisão e aprovação oficial, quando relevante.
Conselhos Gerais de Grupo e Locais, Diretor Executivo do Grupo	Paris, França	Para informações oficiais de gerenciamento e endosso.
Todos os funcionários	Todos os locais da Capgemini	Informações fornecidas conforme exigido por lei, tanto no momento da contratação quanto ao longo de todo o período de vínculo empregatício
Documento revisado e aprovado por		
Papel	Responsabilidade	Comentários
DPO do Grupo, Emmanuelle Bartoli	Aprovador interno	
CNIL, Autoridade Francesa de Proteção de Dados	Revisor Oficial & Aprovador	Aprovado por ofício em 2016, Revisado e confirmada versões mais recentes de acordo com o processo de autoridade oficial.

Introdução

Como líder global em consultoria, serviços de tecnologia e transformação digital, a Capgemini está na vanguarda da inovação, aproveitando nuvem, dados, conectividade de IA, software, engenharia digital e plataformas para atender a toda a amplitude das necessidades de nossos clientes. Desde o avanço da experiência digital do consumidor até a aceleração da indústria inteligente e a transformação da eficiência empresarial, ajudamos nossos clientes a definir o caminho certo para um futuro melhor.

A Capgemini está comprometida em proteger todos os dados pessoais que lhe são confiados como parte de suas atividades. Como um grupo internacional com entidades localizadas em mais de 40 países, é essencial para a Capgemini que as informações fluam livremente e com segurança. Fornecer um forte nível de proteção aos dados pessoais transferidos dentro do grupo é uma das razões pelas quais a Capgemini optou por implementar essas Regras Corporativas Vinculativas (BCR), que foram aprovadas pela primeira vez pela autoridade francesa de proteção de dados, a CNIL, em março de 2016 e posteriormente alteradas em 2019 e 2023 para cumprir o Regulamento Geral de Proteção de Dados (GDPR) e o Conselho Europeu de Proteção de Dados atualizou os requisitos além dos chamados *Schrems II* decisão.

Mais do que um mero mecanismo de transferência de dados, as BCR da Capgemini são nossa política global de proteção de dados, uma estrutura abrangente que define toda a nossa abordagem de responsabilidade para o tratamento de dados pessoais. As BCR da Capgemini não apenas definem os princípios que devem ser cumpridos ao processar Dados Pessoais, mas também especificam os procedimentos implementados para cumprir as leis de proteção de dados aplicáveis e, em particular, o Regulamento Geral de Proteção de Dados 2016/679.

Definições

Os termos usados neste documento são definidos da seguinte forma:

"**Decisão de Adequação**" significa uma decisão pela qual a Comissão Europeia determina que um país oferece um nível adequado de proteção de dados, permitindo que os dados pessoais sejam transferidos livremente para esse país em conformidade com o GDPR.

"**Lei de DP Aplicável**" significa qualquer regulamento de proteção de dados que possa ser aplicado e, em particular, (1) o Regulamento Europeu n°2016/679 relativo ao tratamento de Dados Pessoais (**GDPR)**, (2) quaisquer leis e regulamentos locais aplicáveis relacionados ao tratamento de Dados Pessoais.

"**Regras Corporativas Vinculativas**" ou "**BCR**" significa políticas de proteção de dados pessoais que são seguidas por um Controlador ou Operador estabelecido no território de um Estado-Membro para transferências ou um conjunto de transferências de Dados Pessoais para um Controlador ou Operador em um ou mais países terceiros dentro de um grupo de empresas ou grupo de empresas envolvidas em uma atividade econômica conjunta.

"**Regras Corporativas Vinculantes para Atividades de Controlador**" ou "**BCR-C**" significa as BCR aplicáveis às atividades da Capgemini como Controlador de Dados e, em particular, quando uma Empresa da Capgemini atuando como Controladora transfere Dados Pessoais para outra Empresa da Capgemini atuando como Controladora ou Operadora.

"**Regras Corporativas Vinculantes para Atividades de** Operadores" ou "**BCR-P**" significa as BCR aplicáveis às atividades da Capgemini como Operador de Dados.

"**Blue Book**" significa o livro de políticas e diretrizes da Capgemini que especifica uma série de princípios, valores, políticas e processos comumente adotados.

"**Capgemini**" ou "**Grupo**" significa todas as entidades pertencentes e/ou controladas direta ou indiretamente pela Capgemini SE.

"**Contato Comercial da Capgemini**" significa um fornecedor, subcontratado, acionista, cliente ou parceiro da Capgemini.

"**Cliente Capgemini**" significa qualquer pessoa física ou jurídica para a qual a Capgemini presta serviços de acordo com um contrato.

"**Empresa(s) Capgemini"** significa qualquer entidade que faça parte do Grupo e que esteja vinculada às BCR da Capgemini.

"**Funcionário da Capgemini**" significa todos os funcionários atuais, antigos ou potenciais funcionários da Capgemini, incluindo funcionários de agências e estagiários.

"**Autoridade Supervisora Competente**" significa a Autoridade Supervisora do país onde o Titular de Dados tem sua residência habitual, local de trabalho ou local da suposta violação, ou a Autoridade Supervisora do país onde o Controlador de Dados está estabelecido.

"**Organização de Segurança Cibernética**" significa a função global da Capgemini de criar e gerenciar políticas de segurança globais e monitorar a conformidade das Unidades de Negócios e Linhas de Negócios Globais. A Organização de Segurança Cibernética é composta por uma rede de Diretores de Segurança Cibernética nomeados para cada Unidade de Negócios.

"**Controlador de Dados**" ou "**Controlador**" significa a pessoa física ou jurídica, autoridade pública, agência ou outro órgão que, sozinho ou em conjunto com outros, determina as finalidades e os meios de tratamento de Dados Pessoais.

"**Exportador de dados**" ou "**Exportador**" significa a entidade que transfere os dados pessoais.

"**Importador de Dados**" ou "**Importador**" significa o destinatário de uma transferência de dados.

"**Operador de Dados**" ou "**Operador**" significa uma pessoa física ou jurídica, autoridade pública, agência ou outro órgão que processa dados pessoais em nome do Controlador.

"**Avaliação de Impacto à Proteção de Dados**" ou "**DPIA"** significa um processo para avaliar, em particular, a origem, natureza, particularidade e gravidade de um risco associado a um tratamento de Dados Pessoais. O objetivo de um DPIA é avaliar e mitigar o risco associado a um tratamento ou conjunto de tratamento de Dados Pessoais.

"**Diretor de Proteção de Dados**" ou "**DPO"** significa os Funcionários designados da Capgemini devidamente nomeados perante a autoridade de proteção de dados competente, quando necessário, e que possuem conhecimento especializado das leis e práticas de proteção de dados, aconselhando, informando e monitorando a conformidade com a Lei de DP Aplicável, e que fazem parte da Organização de Proteção de Dados descrita na Seção 8 deste documento.

"**Titular de Dados**" significa qualquer pessoa física identificada ou identificável cujos Dados Pessoais são processados.

"**Espaço Econômico Europeu**" ou "**EEE**" significa os Estados-Membros da União Europeia e três países da Associação Europeia de Livre Comércio.

"**Empresa Capgemini do EEE**" significa qualquer empresa Capgemini localizada no Espaço Econômico Europeu ("EEE").

"**Dados Pessoais do Funcionário**" significa Dados Pessoais relacionados a um Funcionário da Capgemini atual, antigo ou potencial.

"**Regulamento Geral de Proteção de Dados**" ou "**GDPR"** significa o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

"**Contrato Intragrupo**" significa o acordo juridicamente vinculativo projetado para tornar as BCR da Capgemini vinculativas para as Empresas da Capgemini.

"**Empresa Capgemini fora do EEE**" significa qualquer empresa Capgemini localizada fora do EEE.

"**Dados Pessoais**" significa qualquer informação relacionada a uma pessoa física identificada ou identificável ("Titular de dados"); Uma pessoa física identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador, como um nome, um número de identificação, dados de localização ou identificador on-line ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa física.

"Violação de Dados Pessoais" ou "**Violação de Dados**" significa uma violação de segurança que leva à destruição, perda, alteração, divulgação ou acesso não autorizado acidental ou ilegal a dados pessoais transmitidos, armazenados ou processados de outra forma.

"**Tratamento**" significa qualquer operação ou conjunto de operações realizadas em dados pessoais ou em conjuntos de dados pessoais, por meios automatizados ou não, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição.

"**Contrato de Serviço**" significa um contrato escrito entre um Controlador e um Operador pelo qual o Operador deve fornecer serviços ao Controlador e que envolve o tratamento de Dados Pessoais pelo Operador sob as instruções do Controlador.

"**Cláusulas Contratuais Padrão**" significa as cláusulas contratuais emitidas pela Comissão Europeia para enquadrar as transferências de dados de Controladores estabelecidos no EEE para Controladores estabelecidos fora do EEE e de Controladores estabelecidos no EEE para Operadores estabelecidos fora do EEE.

"**Autoridade(s) Fiscalizadora(s)**" ou "**Autoridades de Proteção de Dados**" refere-se a uma autoridade pública independente criada por um Estado-Membro da União Europeia ou por qualquer outro Estado.

"**País terceiro**" significa um país que não foi reconhecido pela Comissão Europeia como oferecendo um nível adequado de proteção de dados.

"**Transferência**" significa a divulgação, transmissão ou o processo de disponibilização de Dados Pessoais a terceiros.

1. Âmbito de aplicação das BCR

As BCR-C da Capgemini aplicam-se a todo o tratamento de dados pessoais realizado pela Capgemini como controladora de dados. As BCR-C da Capgemini enquadram todas as transferências de dados pessoais de uma empresa da Capgemini que atua como controladora de dados para outra empresa da Capgemini que atua como controladora ou Operadora. As empresas da Capgemini são responsáveis e podem demonstrar que cumprem as BCR-C.

Quando a lei local for mais rigorosa e exigir um nível de proteção mais alto do que os compromissos previstos nas BCR-C da Capgemini, ela terá precedência sobre as BCR-C. A Capgemini deve cumprir a lei local de proteção de dados aplicável.

1.1. Escopo do material

Estas BCR-C se aplicam a todos os dados pessoais processados na Capgemini, onde a Capgemini atua como controladora. Mais especificamente, as presentes BCR-C aplicam-se e enquadram as seguintes transferências de dados pessoais:

- De uma empresa da Capgemini atuando como controladora para outra empresa da Capgemini atuando como controladora.
- De uma empresa da Capgemini atuando como controladora para uma empresa da Capgemini atuando como Operadora.

Na prática, ao atuar como controladora de dados, a Capgemini processa principalmente os dados pessoais de seus funcionários e contatos comerciais. As finalidades de tal tratamento estão relacionadas principalmente a recursos humanos, segurança cibernética, comunicações internas e externas, marketing e conformidade.

Para obter uma visão geral mais abrangente das atividades de tratamento da Capgemini como controladora, incluindo as transferências de dados mais comuns realizadas pela Capgemini, consulte o Apêndice 2.

1.2. Âmbito geográfico

Estas BCR-C abrangem todos os dados pessoais que estão sendo transferidos e processados posteriormente dentro do grupo, independentemente da origem dos dados pessoais. As BCR-C abrangem todas as transferências de dados pessoais realizadas dentro do grupo, incluindo transferências subsequentes.

Na prática, isso significa que as BCR-C se aplicam aos dados pessoais transferidos de:

- Uma empresa Capgemini do EEE para outra empresa Capgemini do EEE
- Uma empresa Capgemini do EEE para uma empresa Capgemini não pertencente ao EEE
- Uma empresa Capgemini fora do EEE para uma empresa Capgemini do EEE
- Uma empresa da Capgemini fora do EEE para outra empresa da Capgemini fora do EEE.

As empresas da Capgemini obrigadas a cumprir estas BCR-C estão listadas no Apêndice 1.

2. Vinculação da BCR-C

Todas as empresas da Capgemini e seus funcionários são legalmente obrigados a cumprir estas BCR-C.

2.1. Vinculação nas empresas da Capgemini

Na prática, cada entidade da Capgemini dá uma procuração à Capgemini International BV para assinar o acordo intragrupo em seu nome, para que cada entidade da Capgemini seja efetivamente obrigada a cumprir as BCR-C. Ao assinar o acordo intragrupo, as entidades da Capgemini se comprometem a cumprir as disposições da BCR-C e a implementar seus princípios dentro de sua própria organização.

Quando a Capgemini criar ou adquirir novas entidades, em particular quando estas estiverem localizadas fora do EEE, nenhum dado pessoal será transferido para elas até que estejam totalmente aptas a cumprir e efetivamente vinculadas às BCR-C de acordo com o mecanismo acima mencionado.

2.2. Vinculação para os funcionários da Capgemini

Todos os funcionários da Capgemini são obrigados a cumprir estas BCR-C por meio de uma menção específica em seu contrato de trabalho e/ou por meio da obrigação, contida em todos os contratos de trabalho, de cumprir as políticas da Capgemini, que incluem as BCR.

Na prática, uma avaliação é realizada localmente para determinar como a BCR pode ser juridicamente vinculativo para os funcionários de acordo com a(s) lei(s) aplicável(is). Na maioria dos casos, consiste em adicionar uma disposição ao contrato de trabalho e/ou ao acordo coletivo. A informação e/ou consulta dos conselhos de empresa competentes são igualmente asseguradas em tempo útil, se necessário.

Conforme detalhado nas Seções 10 e 17 das BCR-C, os funcionários da Capgemini são informados sobre a BCR e as obrigações relevantes por meio de comunicação interna e treinamento. Os funcionários da Capgemini também são informados do fato de que qualquer não conformidade com as BCR levará a sanções disciplinares de acordo com as leis aplicáveis.

3. Aplicação dos princípios de proteção de dados

A Capgemini está comprometida em cumprir e implementar os princípios de proteção de dados estabelecidos nestas BCR-C, independentemente das leis locais de proteção de dados aplicáveis, a menos que tais leis forneçam requisitos mais rigorosos do que os fornecidos por estas BCR-C.

Na prática, isso significa que, no mínimo, a Capgemini deve cumprir os princípios e obrigações estabelecidos nas BCR. Quando a lei local aplicável exigir que a Capgemini cumpra quaisquer princípios e/ou obrigações adicionais ou mais rigorosos, a Capgemini deverá fazê-lo.

Todos os princípios e obrigações descritos nas BCR são promovidos e implementados na Capgemini por meio de um conjunto de políticas, processos, diretrizes e treinamentos.

3.1. Finalidade claramente identificada

Ao atuar como controladora, a Capgemini apenas coletará e processará dados pessoais para fins específicos, explícitos e legítimos, e não os processará de maneira incompatível com esses fins.

Na prática, isto significa que o(s) objetivo(s) para o(s) qual(is) os dados pessoais são recolhidos e tratados posteriormente devem ser definidos antes de essa recolha ocorrer. Ao atuar como controladora, a Capgemini pode coletar e processar dados pessoais por vários motivos, incluindo, em particular: fins relacionados a RH (recrutamento, gerenciamento da força de trabalho, etc.), segurança cibernética, promoção das ofertas da Capgemini, etc. Como parte do processo de revisão e aprovação, o proprietário da empresa de cada projeto que envolva o tratamento de dados pessoais deve detalhar os motivos pelos quais esses dados devem ser coletados e processados posteriormente.

3.2. Base jurídica

Ao atuar como controladora, a Capgemini só processará dados pessoais se uma das seguintes condições for atendida:

1. O tratamento é necessário para fins do **interesse legítimo perseguido pela Capgemini** ou por terceiros.
   Por exemplo, a Capgemini deve confiar no interesse legítimo como base legal ao processar os dados pessoais de seus funcionários para fins relacionados à segurança, para proteger sua rede, ativos e/ou instalações.
   Ao confiar no interesse legítimo, a Capgemini realizará um teste de equilíbrio para determinar se seus interesses legítimos são anulados pelos dos indivíduos cujos dados pessoais são processados, ou seus direitos e liberdades fundamentais, em circunstâncias em que os dados pessoais desses indivíduos devem ser protegidos.

2. **Os indivíduos cujos dados pessoais são processados consentiram com tal tratamento**. Para ser válido, tal consentimento deve ser dado livremente, específico, informado e inequívoco.
   Por exemplo, ao coletar dados pessoais diretamente de indivíduos para permitir que eles se inscrevam em um evento, assinem um boletim informativo ou baixem um relatório, por meio de formulários de contato em seu site, a Capgemini deve contar com o consentimento dos indivíduos.

3. A coleta e o tratamento posterior de dados pessoais são **necessários para a execução de um contrato** do qual o indivíduo cujos dados pessoais são processados é parte, ou para tomar medidas, a pedido do indivíduo, antes de celebrar tal contrato.
   Por exemplo, o tratamento de informações salariais e detalhes de contas bancárias é necessário para pagar salários, o que faz parte da execução de um contrato de trabalho.

4. O tratamento é necessário **para cumprir uma obrigação legal** à qual a Capgemini está sujeita.
   Por exemplo, a comunicação de dados pessoais às autoridades fiscais pode ser exigida pela legislação local aplicável.

   Na prática, essas 4 bases legais são aquelas nas quais a Capgemini provavelmente confiará ao processar dados pessoais.

5. O tratamento é **necessário para proteger os interesses vitais do indivíduo** cujos dados pessoais são processados ou de outro indivíduo.
   Por exemplo, quando o indivíduo é física ou legalmente incapaz de dar seu consentimento para o tratamento e sua segurança ou saúde está em jogo.

6. O tratamento é **necessário para o desempenho de uma tarefa realizada no interesse público** ou no exercício da autoridade pública investida no controlador.
   Na prática, é improvável que a Capgemini se baseie nessa base legal.

3.3. Minimização de dados

A Capgemini apenas coletará e processará os dados pessoais estritamente necessários em relação à(s) finalidade(s) definida(s) anteriormente.

Na prática, isso significa que a Capgemini determinará, antes do tratamento, quais dados pessoais são necessários para atingir o(s) objetivo(s). Como resultado, a Capgemini não coletará, armazenará ou processará dados pessoais não essenciais apenas para que possa usá-los para uma finalidade hipotética que seria definida

no futuro.

3.4. Qualidade dos dados

A Capgemini deve garantir que os dados pessoais sejam precisos e mantidos atualizados durante todo o ciclo de vida do tratamento.

Na prática, isso significa que o local do processo para determinar quais dados devem ser atualizados ou excluídos para garantir que a qualidade dos dados nos sistemas permaneça no nível certo. Isso também significa que a Capgemini fornecerá aos indivíduos meios para solicitar que dados imprecisos sejam corrigidos, atualizados ou excluídos. Por exemplo, os funcionários da Capgemini podem fazer alterações em seu perfil por meio de um painel dedicado.

3.5. Limitação da retenção de dados

A Capgemini manterá os dados pessoais por não mais do que o necessário em relação à(s) finalidade(s) para a(s) qual(is) os dados pessoais foram coletados.

Isso significa que a Capgemini definirá o período de retenção de dados com antecedência e de acordo com a(s) finalidade(s) do tratamento, considerando e ponderando o seguinte:

- Quaisquer requisitos legais aplicáveis/locais
- As necessidades do negócio
- Os interesses dos indivíduos cujos dados pessoais são processados.

Na prática, para cada projeto que envolva o tratamento de dados pessoais, a Capgemini determinará se alguma lei local fornece requisitos de retenção de dados e equilibra o objetivo geral do projeto com os interesses dos titulares de dados. Essa avaliação permitirá que a Capgemini determine o período de retenção de dados relacionado à atividade de tratamento relevante.

3.6. Segurança de dados

A Capgemini implementará medidas técnicas e organizacionais apropriadas para garantir a segurança dos dados pessoais que lhe são confiados e proteger contra acesso ilegal, perda, destruição ou alteração dos dados pessoais.

Na prática, isso significa que, no mínimo, a Capgemini implementará os requisitos e boas práticas definidos por sua Organização de Segurança Cibernética. Tais medidas de segurança devem ser desenvolvidas considerando a natureza dos dados pessoais a serem processados e os riscos associados a esse tratamento.

Em caso de violação de dados, a Capgemini deve cumprir sua Política de Gerenciamento de Incidentes de Segurança Cibernética e Notificação de Violação de Dados. A política indica todas as etapas necessárias que a Capgemini deve realizar para atender aos requisitos de gerenciamento de incidentes, desde o estágio de preparação até o encerramento. Em particular, a Capgemini deve envolver o DPO em qualquer incidente que possa afetar os dados pessoais e manter registros de todos esses incidentes de acordo com os requisitos regulamentares. Na prática, esses registos devem incluir os factos relacionados com o incidente, os seus efeitos e as medidas corretivas tomadas, e devem ser disponibilizados à autoridade fiscalizadora competente, mediante pedido. O DPO deve então avaliar a gravidade de todos os incidentes à luz dos critérios baseados nas recomendações da ENISA (Agência da União Europeia para a Cibersegurança) e determinar todas as notificações e informações que a Capgemini deve realizar à luz dos riscos identificados:

- quando a violação de dados puder resultar em risco para os direitos e liberdades dos indivíduos, a Capgemini também notificará a(s) autoridade(s) supervisora(s) relevante(s), sujeita à(s) lei(s) de proteção de dados aplicável(is), sem atrasos indevidos e no prazo máximo de 72 horas após ter tomado conhecimento disso.
- Além disso, a Capgemini notificará o(s) titular(es) dos dados sem demora injustificada, quando a violação de dados pessoais puder resultar em um alto risco para os direitos e liberdades das pessoas físicas.

Por fim, e mais especificamente, quando a empresa Capgemini que importa dados pessoais tomar conhecimento de uma violação de dados, ela deve notificar a empresa Capgemini que exporta os dados pessoais sem atrasos indevidos.

3.7. Tratamento de categorias especiais de dados pessoais e dados relacionados a condenações criminais e infrações

A Capgemini só tratará categorias especiais de dados pessoais e/ou dados relacionados a condenações criminais e ofensas – revelando origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou filiação sindical, e dados genéticos e/ou biométricos com a finalidade de identificar exclusivamente um indivíduo, dados relativos à saúde ou à vida sexual ou orientação sexual de um indivíduo – quando estritamente necessário e/ou legalmente exigido.

- O indivíduo deu consentimento explícito para o tratamento desses dados pessoais para um ou mais fins específicos.
- O tratamento desses dados é necessário para que a Capgemini ou o indivíduo cumpra uma obrigação ou exerça direitos específicos na legislação trabalhista, previdenciária e de proteção social.
- O tratamento é necessário para proteger os interesses vitais do indivíduo cujos dados são processados ou de outro indivíduo.
- O tratamento é necessário para o estabelecimento, exercício ou defesa de reivindicações legais ou sempre que os tribunais estiverem agindo em sua capacidade judicial.
- O tratamento é necessário por motivos de interesse público substancial.

O tratamento é necessário por razões de interesse público no domínio da saúde pública, como a proteção contra ameaças transfronteiriças graves para a saúde.

Na prática, a Capgemini deve abster-se de processar quaisquer categorias especiais de dados pessoais e/ou quaisquer dados pessoais relacionados a condenações criminais e ofensas, a menos que uma das condições listadas acima seja atendida.

Categorias especiais de dados pessoais e/ou dados relacionados a condenações criminais e infrações só serão transferidas do EEE para outros países, quando cobertos por um nível de proteção equivalente ao fornecido pela legislação do EEE.

3.8. Tomada de decisão com base no tratamento automatizado

Os titulares de dados têm o direito de não ficar sujeitos a uma decisão baseada exclusivamente no tratamento automatizado, incluindo a definição de perfis, que produza efeitos jurídicos que lhes digam respeito ou que os afetem significativamente. No entanto, este direito não se aplica se o tratamento for:

- Necessário para celebrar ou executar um contrato entre o indivíduo e a Capgemini.

- Autorizado pela lei local aplicável à qual a Capgemini está sujeita e que também estabelece medidas adequadas para salvaguardar os direitos e liberdades e interesses legítimos do indivíduo.
- Com base no consentimento do indivíduo.

Além disso, a Capgemini se esforçará para explicar aos indivíduos a lógica subjacente de qualquer tratamento automatizado que os afete.

Na prática, a Capgemini informará os titulares de dados por meio de um aviso de proteção de dados que definirá o método pelo qual os titulares de dados podem entrar em contato com a Capgemini buscando o direito à intervenção humana e/ou contestar a decisão, quando aplicável.

4. Transparência

A Capgemini fornecerá aos titulares de dados todas as informações necessárias sobre o tratamento de seus dados pessoais.

Quando os dados pessoais relacionados a indivíduos são coletados diretamente deles, a Capgemini deve, no mínimo, compartilhar as seguintes informações:

- A identidade e os detalhes de contato da empresa Capgemini que atua como controladora de dados;
- Os dados de contacto do encarregado da proteção de dados competente;
- A(s) finalidade(s) para a(s) qual(is) os dados pessoais são tratados, bem como a(s) base(s) legal(is) para o tratamento;
- Quando o tratamento for baseado no interesse legítimo da Capgemini, a descrição do interesse perseguido pela Capgemini;
- Os destinatários ou categorias de destinatários, se houver, isso é relevante nos casos em que a Capgemini compartilharia;
- Se a Capgemini pretende transferir dados pessoais para fora do EEE e a existência ou ausência de uma decisão de adequação da Comissão Europeia, ou a referência às salvaguardas apropriadas (coma BCR ou Cláusulas-Padrão Contratuais) e como obter uma cópia delas;
- O período durante o qual os dados pessoais serão armazenados ou, se não for possível, os critérios utilizados para determinar esse período;
- O direito do Titular de dados de solicitar o acesso e a retificação ou apagamento dos dados pessoais ou a limitação do tratamento ou de se opor ao tratamento, bem como o direito à portabilidade;
- Quando o tratamento for baseado no consentimento do indivíduo, o direito de retirar o consentimento a qualquer momento, sem afetar a legalidade do tratamento;
- O direito de apresentar uma reclamação perante uma autoridade de proteção de dados e/ou supervisora;
- Se o fornecimento de dados pessoais é um requisito legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o indivíduo é obrigado a fornecer os dados pessoais e as possíveis consequências do não fornecimento desses dados;
- A existência de tomadas de decisão automatizadas, incluindo a definição de perfis, e informações sobre a lógica envolvida, bem como a importância e as consequências previstas de tal tratamento para o indivíduo.

Quando os dados pessoais não forem obtidos diretamente do indivíduo, a Capgemini ainda fornecerá as informações acima mencionadas dentro de um período razoável após a obtenção dos dados pessoais, bem como a descrição das categorias de dados pessoais e a(s) fonte(s) desses dados pessoais. Se os dados forem usados para entrar em contato com o indivíduo, a Capgemini fornecerá as informações no momento dessa primeira comunicação.

Na prática, a Capgemini disponibiliza avisos de "proteção de dados" ou "privacidade" aos indivíduos para fornecer as informações necessárias.

Ao coletar dados pessoais diretamente de indivíduos para fins específicos, por exemplo, por meio de aplicativos ou ferramentas voltados para o usuário, a Capgemini elaborará e disponibilizará avisos personalizados.

A Capgemini também elaborou e publicou avisos de proteção de dados mais gerais, como o disponível em seu site, que abrange uma gama mais ampla de atividades de tratamento, incluindo, por exemplo, tratamento

relacionado a marketing.

5. Direitos dos titulares de dados

Os indivíduos cujos dados pessoais são coletados, usados ou processados pela Capgemini podem solicitar acesso, retificação ou exclusão de seus dados. Além disso, os titulares de dados podem opor-se ao tratamento dos seus dados e têm o direito de não ficar sujeitos a decisões baseadas exclusivamente no tratamento automatizado, incluindo a definição de perfis. Além disso, os titulares de dados podem solicitar a comunicação de seus dados pessoais em um formato estruturado, comumente usado e legível por máquina.

Na prática, os indivíduos são informados de seus direitos por meio de avisos dedicados e podem exercer seus direitos entrando em contato com a Capgemini de acordo com o processo detalhado no Apêndice 7.

Os titulares de dados podem exercer esses direitos entrando em contato com o DPO, ou outro ponto de contato que possa ser relevante. O Titular de dados também pode apresentar uma reclamação com relação ao tratamento de seus dados pessoais, por meio desse mesmo processo.

Além disso, os indivíduos têm o direito de apresentar uma reclamação sobre o tratamento de seus dados pessoais junto à(s) autoridade(s) supervisora(s) competente(s) e/ou perante o tribunal competente.

Em caso de violação dos direitos garantidos e/ou obrigações previstas nas BCR-C, a Capgemini incentiva os indivíduos a enviar uma reclamação. No entanto, os indivíduos também têm o direito de apresentar uma reclamação perante a(s) autoridade(s) supervisora(s) competente(s) – que pode ser a do Estado-Membro da UE de sua residência habitual, local de trabalho ou local da suposta violação. Além disso, os particulares podem apresentar uma queixa perante o tribunal do Estado-Membro da sua residência habitual, do seu local de trabalho ou do local da alegada infração. Quando o tratamento de dados pessoais for realizado por uma empresa da Capgemini fora do EEE, os indivíduos poderão apresentar uma reclamação perante o tribunal competente, conforme previsto na legislação local aplicável, a menos que o tratamento e/ou a empresa da Capgemini fora do EEE esteja sujeita ao GDPR, caso em que as disposições acima mencionadas serão aplicadas.

Os Titulares de Dados têm direito a recursos judiciais e o direito de obter reparação e, se for caso disso, compensação em caso de violação de um dos elementos aplicáveis da BCR-C, conforme listado na Seção 6. Os titulares de dados podem ser representados por uma organização ou associação sem fins lucrativos para exercer esses direitos, nas condições previstas pela legislação local aplicável.

Na prática, em caso de violação das BCR-C, os indivíduos podem apresentar uma reclamação diretamente à Capgemini e/ou à autoridade de proteção de dados e/ou tribunal competente. Além disso, os indivíduos podem buscar reparação, reparação e compensação em caso de violação de um dos elementos listados na Seção 6.

6. Direitos de aplicação dos titulares de dados

Os titulares de dados podem fazer valer os seguintes elementos da BCR-C, como terceiros beneficiários:

- A implementação dos princípios de proteção de dados detalhados nas Seções 3, 4 e 12 da BCR-C.
- A obrigação da Capgemini de compartilhar informações relevantes com os indivíduos sobre o tratamento de seus dados pessoais, conforme previsto na Seção 4; bem como a obrigação de fornecer acesso fácil às BCR-C, conforme previsto na Seção 17.
- Direitos dos indivíduos em relação ao tratamento de seus dados pessoais, conforme previsto na Seção 5.
- Direito dos indivíduos de reclamar por meio do processo interno de reclamação da Capgemini, conforme previsto na Seção 5 e detalhado nos Apêndices 6 e 7.
- Direitos dos indivíduos de apresentar uma reclamação à(s) autoridade(s) supervisora(s) competente(s) e/ou perante os tribunais competentes, conforme previsto nas Seções 5 e nos Apêndices 6 e 7.

- A obrigação, para cada empresa da Capgemini fora do EEE que importa dados pessoais, de notificar a Capgemini do EEE que exporta esses dados pessoais, bem como a sede da Capgemini, em caso de conflito entre a legislação local aplicável e as BCR-C, conforme previsto na Seção 13.
- A obrigação, para cada empresa da Capgemini que importa dados pessoais, de informar a entidade exportadora da Capgemini, bem como a sede da Capgemini, e se legalmente permitido ao Titular de dados, sobre quaisquer solicitações de uma autoridade pública e/ou agência de aplicação da lei para acessar os dados pessoais conforme fornecido e detalhado na Seção 14.
- O dever da Capgemini de cooperar com as autoridades de supervisão, conforme previsto na Seção 16.
- A obrigação de cada empresa da Capgemini do EEE que transfere dados pessoais para uma empresa da Capgemini fora do EEE aceitar a responsabilidade por quaisquer violações das BCR-C pela empresa da Capgemini que não é do EEE que recebe os dados, conforme previsto na Seção 15.
- O fato de que, em caso de violação das BCR-C por uma empresa não pertencente ao EEE, cabe à empresa Capgemini do EEE que exportou os dados pessoais demonstrar que o destinatário (ou seja, a empresa Capgemini não pertencente ao EEE) não violou as BCR-C, conforme previsto na Seção 15.
- A obrigação da Capgemini de informar o Titular de dados sobre qualquer atualização das BCR-C – inclusive no que diz respeito à lista de empresas da Capgemini vinculadas às BCR-C – conforme previsto na Seção 18.
- A obrigação da Capgemini de permitir que os titulares de dados apliquem os elementos das BCR-C listados nesta Seção como terceiros beneficiários.
- O direito dos indivíduos de buscar recursos judiciais, obter reparação e, quando apropriado, indenização em caso de violação dos elementos executórios da BCR-C listados nesta Seção – conforme previsto na Seção 5.

7. Processo de tratamento de solicitações dos titulares de dados

A Capgemini criou um processo interno dedicado que permite que os indivíduos enviem solicitações e/ou reclamações sobre o tratamento de seus dados pessoais e/ou qualquer violação das BCR-C. Conforme detalhado no Apêndice 4, os indivíduos podem entrar em contato diretamente com o grupo, DPO regional e/ou local e/ou outro(s) ponto(s) de contato.

O processo detalhado no Apêndice 4 explica aos titulares de dados onde e como apresentar uma solicitação e/ou reclamação, os atrasos na resposta, as consequências em caso de rejeição da solicitação ou reclamação, as consequências se a solicitação ou reclamação for considerada justificada e o direito do Titular de dados de apresentar uma reclamação perante a(s) autoridade(s) supervisora(s) competente(s) ou tribunal(es) de justiça.

Na prática, os indivíduos podem enviar qualquer solicitação relacionada ao tratamento de seus dados pessoais entrando em contato com um DPO ou outro ponto de contato, conforme descrito no Apêndice 4. A Capgemini deve primeiro acusar o recebimento da solicitação e pode solicitar mais informações para facilitar o gerenciamento da solicitação. Após a análise da solicitação e/ou reclamação, o DPO e/ou outra função habilitada para lidar com solicitações, determinará se e em que medida a solicitação pode ser atendida e, em seguida, responderá ao solicitante.

A Capgemini responderá ao solicitante sem atrasos indevidos e, em qualquer caso, no prazo máximo de 30 dias após o recebimento da solicitação. Caso a Capgemini não consiga processar adequadamente a solicitação dentro do período de 30 dias, ela notificará o solicitante. Essa notificação deve ser enviada ao solicitante dentro do período de 30 dias, explicando que o período de revisão e tratamento pode ser prorrogado por mais 2 meses e detalhando os motivos da prorrogação.

A Capgemini gerenciará essas solicitações conforme detalhado em seu processo interno.

8. Organização de proteção de dados da Capgemini

A Capgemini nomeou um escritório de proteção de dados do grupo chefiado pelo responsável pela proteção de dados do grupo, bem como responsáveis regionais e locais pela proteção de dados, defensores da proteção de dados e pontos de contato específicos (SPOCS), conforme descrito no Apêndice 3.

Se você deseja entrar em contato com nosso Escritório de Proteção de Dados do Grupo, por favor:

- Envie-nos um e-mail para: dpocapgemini.global@capgemini.com
- Escreva-nos para o seguinte endereço: 11 rue de Tilsitt, 75017 Paris, França.

Para entrar em contato com qualquer um de nossos responsáveis locais pela proteção de dados, preencha nossos formulários de contato dedicados disponíveis em nosso site.

Os responsáveis pela proteção de dados monitoram e garantem a conformidade da(s) empresa(s) Capgemini dentro de seu escopo com as leis locais de proteção de dados aplicáveis, bem como com as BCR. Os DPOs prestam apoio em todas as questões relacionadas com a proteção de dados, implementam o programa global de proteção de dados, tratam e/ou aconselham sobre violações de dados e mantêm uma relação ativa com a autoridade fiscalizadora local.

Como parte da função jurídica, os DPOs são apoiados em sua missão por suas equipes jurídicas locais. Os DPOs relatam anualmente ao conselho local do país ou à comissão executiva sobre questões relacionadas à privacidade, como a implementação do programa global de proteção de dados, questões de privacidade que podem ter ocorrido em grandes negócios, violações críticas de dados e/ou solicitações de titulares de dados, quando relevante, etc.

Os DPOs atuam como parceiros de negócios para apoiar as diferentes funções e operações para garantir que eles entendam e implementem os princípios e obrigações de proteção de dados em suas operações diárias.

Na prática, isso significa que os DPOs devem implementar uma estratégia e um programa de proteção de dados para garantir a conformidade com a legislação local aplicável, bem como com as políticas e processos do grupo.

→ Os DPOs devem aconselhar a empresa quando um projeto envolver a coleta e o uso posterior de dados pessoais para garantir que a proteção de dados seja incorporada desde o início. Os DPOs devem então revisar e aprovar projetos que envolvam o tratamento de dados pessoais. Além disso, os DPOs devem fornecer modelos, processos e diretrizes para garantir que as restrições de proteção de dados sejam consideradas por padrão pela empresa.
→ Os DPOs devem apoiar os advogados internos na revisão e negociação de acordos de tratamento de dados com clientes, fornecedores e/ou parceiros.
→ Os DPOs devem revisar e avaliar os riscos de proteção de dados associados às oportunidades e recomendar medidas de mitigação para eliminar ou minimizar esses riscos.
→ Os EPD devem desenvolver e ministrar ações de formação específicas para funções de proteção de dados.
→ Os DPOs devem gerir as violações de dados, em cooperação com a cibersegurança e quaisquer outras partes interessadas relevantes, avaliando a gravidade da violação, efetuando as notificações necessárias e apoiando a aplicação de medidas de atenuação.
→ Os DPOs devem analisar e atender às solicitações dos titulares de dados, em cooperação com as TI do Grupo, RH e/ou qualquer outra parte interessada relevante.
→

A rede DPO é apoiada por defensores de proteção de dados que representam cada função do grupo e, quando relevante, cada linha de negócios global (GBL). Os defensores da proteção de dados são nomeados como representantes de sua função ou GBL para garantir que as diretrizes, processos e procedimentos de proteção de dados sejam implementados adequadamente em todo o grupo. Os defensores da proteção de dados desempenham um papel fundamental na organização de proteção de dados, pois permitem que os DPOs obtenham uma melhor visão das operações para oferecer melhor suporte aos negócios com conteúdo personalizado.

9. Privacidade desde a concepção

9.1. Registro das atividades de tratamento

Quando atuar como controladora, a Capgemini manterá e manterá, por escrito, um registro das atividades de tratamento contendo as seguintes informações:

- O nome e os detalhes de contato da empresa Capgemini que atua como controladora, do DPO competente e, quando aplicável, do(s) controlador(es) conjunto(s).
- O(s) objetivo(s) das atividades de tratamento.
- Uma descrição das categorias de titulares de dados e das categorias de dados pessoais tratados.
- As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo destinatários localizados fora do EEE.
- Se for caso disso, as transferências transfronteiriças de dados pessoais, incluindo o(s) país(es) de destino, bem como o(s) mecanismo(s) de transferência utilizado(s) para enquadrar essas transferências.
- O período de retenção de dados.
- Uma descrição geral das medidas de segurança.

Na prática, o proprietário da empresa de qualquer ferramenta, aplicação ou qualquer outro projeto que envolva o tratamento de dados pessoais deve criar uma inscrição no registo, incluindo todos os dados acima mencionados. O(s) encarregado da proteção de dados competente(s) deve(m) rever a entrada para garantir que contém todas as informações necessárias para lhes permitir avaliar a conformidade do projeto em causa com a legislação aplicável em matéria de PD. Com base em sua avaliação, o DPO deve fazer recomendações para garantir que o proprietário da empresa realize atividades de tratamento em conformidade com estas BCR-C e com as leis de DP aplicáveis.

Ao atuar como Operador de dados, a Capgemini também manterá e manterá um registro das atividades de tratamento realizadas em nome do controlador e incluindo:

- O(s) nome(s) e detalhes de contato da(s) empresa(s) Capgemini que atua(m) como Operador(es), bem como o(s) nome(s) e detalhes de contato de cada controlador(es) em nome do(s) qual(is) estão processando os dados.
- As categorias de tratamento realizadas em nome de cada controlador.
- Se for caso disso, a(s) transferência(s) transfronteiriça(s) de dados pessoais, incluindo o(s) país(es) de destino, bem como o(s) mecanismo(s) de transferência utilizado(s) para enquadrar essas transferências.
- Uma descrição geral das medidas de segurança.

A Capgemini disponibilizará os registros de tratamento à(s) autoridade(s) supervisora(s) competente(s) mediante solicitação.

9.2. Relatórios de impacto da proteção de dados

A Capgemini realizará um relatório de impacto sobre a proteção de dados (DPIA) quando uma atividade de tratamento provavelmente resultar em um alto risco para os direitos e liberdades dos indivíduos.

O grupo e/ou o DPO local devem avaliar as atividades de tratamento para determinar se devem ser consideradas de "alto risco" usando uma metodologia alinhada com as recomendações do Conselho Europeu de Proteção de Dados e com quaisquer outras práticas e/ou diretrizes locais emitidas pela autoridade de proteção de dados.

O Grupo e/ou os DPOs devem determinar a necessidade de realizar uma AIPD para um tratamento de alto risco, considerando:

1. A possibilidade de um evento indesejável – por exemplo, acesso ilegítimo ou não autorizado aos dados, modificação ou exclusão dos dados, etc.
2. A probabilidade de ocorrência de tal evento indesejável.

3. A gravidade das consequências para os direitos e liberdades dos titulares de dados.

Na prática, ao revisar as atividades de tratamento de dados, conforme descrito na subseção 9.1., o grupo ou DPO local deve determinar se o proprietário precisa iniciar um DPIA, respondendo a um questionário projetado para avaliar os riscos. O grupo ou o encarregado da proteção de dados local deve então rever a avaliação e formular recomendações para atenuar os riscos.

Se a AIPD indicar que a atividade de tratamento resultaria num risco elevado e o grupo ou o encarregado da proteção de dados local determinar que não pode ser aplicada nenhuma medida para atenuar esse risco, deve consultar a autoridade fiscalizadora competente. A autoridade supervisora deve revisar e avaliar a atividade de tratamento e determinar se a Capgemini avaliou adequadamente os riscos por meio da DPIA e se as salvaguardas que a Capgemini pretende implementar para lidar com os riscos são adequadas.

10. Treinamento e conscientização

10.1. Treinamento obrigatório global

A Capgemini criou e implementou um treinamento obrigatório de proteção de dados para todos os funcionários. O objetivo do treinamento obrigatório é garantir que todos os Capgemini estejam cientes e entendam os principais princípios e requisitos de proteção de dados. Este eLearning obrigatório aborda o seguinte:

- Entendendo os principais princípios e requisitos de proteção de dados
- Transferências de dados e uso de fornecedores
- Gerenciamento de violações de dados
- Solicitações de divulgação de dados pessoais de autoridades policiais e/ou públicas (bem como de terceiros)

No final do treinamento, os funcionários são obrigados a fazer um teste. Se não obtiverem um mínimo de 80% para o teste, precisam refazer todo o treinamento. Além disso, uma vez aprovados no teste no final do treinamento, os funcionários são solicitados a baixar a BCR para que seu treinamento seja registrado como "assistido" – incluindo, em particular, o processo que deve ser seguido em caso de solicitação de terceiros, autoridade pública ou agência de aplicação da lei, para divulgar dados pessoais.

Os funcionários da Capgemini são obrigados a concluir o treinamento ao ingressar na empresa. Todos os anos, os funcionários devem responder a perguntas relacionadas à proteção de dados para avaliar seus conhecimentos. Caso o funcionário não consiga responder às perguntas corretamente, ele deverá concluir o treinamento completo novamente. Em qualquer caso, os Funcionários são obrigados a fazer o treinamento completo a cada três anos, independentemente das respostas fornecidas ao questionário acima mencionado.

10.2. Treinamentos e diretrizes específicas para funções

Além do eLearning obrigatório global, a organização de proteção de dados cria diretrizes e treinamentos específicos para cada função. O objetivo é oferecer melhor suporte a funções com conteúdo personalizado: abordar casos de uso específicos de algumas funções.

Na prática, todos os funcionários da Capgemini, independentemente de sua descrição de cargo, são obrigados a preencher o eLearning de proteção de dados obrigatório global, para garantir que estejam cientes e entendam os princípios e obrigações fornecidos pelas BCR. Além disso, os responsáveis pela proteção de dados e os defensores da proteção de dados oferecem treinamentos específicos para cada país e/ou função.

11. Auditorias

A Capgemini realizará auditorias de proteção cobrindo todos os aspectos da BCR regularmente. As auditorias e controles devem garantir especialmente que as BCR, todas as políticas, procedimentos ou diretrizes relacionados adotados na Capgemini ("Programa de Proteção de Dados"), bem como as Leis de Proteção de Dados Aplicáveis, sejam implementadas, documentadas e avaliadas.

As auditorias devem ser realizadas por auditores internos ou externos qualificados e independentes.

A Capgemini realiza auditorias de obrigações de proteção de dados que afetam os aspectos de governança e política ("Auditorias de Entidades") e obrigações de proteção de dados que afetam a execução de tais políticas nas atividades reais que envolvem o tratamento de dados pessoais ("Auditorias de Atividades"). A combinação de todas essas auditorias compõe o Programa de Auditorias BCR.

Na prática, a Capgemini realizará 3 tipos de auditorias de proteção de dados:

- **Nível 1 - As partes interessadas locais são responsáveis pela auditoria de suas atividades locais.**
  - O DPO Local deve realizar uma autoavaliação anual de seu Programa de Proteção de Dados.
  - O DPO Local também é responsável pela auditoria das partes interessadas locais (funções centrais e/ou GBL) que podem ser auditadas por eles ou por terceiros mandatados por eles, de acordo com suas responsabilidades sob as BCR e o Programa de Proteção de Dados da Capgemini.
  - Por fim, o DPO Local auditará as atividades locais (atividades de engajamento, fornecedores e/ou controladores) para verificar a implementação do Programa de Proteção de Dados.

- **Nível 2 – O Diretor de Proteção de Dados do Grupo é responsável pela auditoria das atividades locais.**
  - O DPO do Grupo deve auditar o Programa de Proteção de Dados do DPO Local para garantir a conformidade com as BCR exigidas pelo Grupo.
  - O DPO do Grupo também é responsável pela auditoria de atividades locais e/ou globais que possam afetar a conformidade local (compromissos, fornecedores, atividades de controladoria).
  - As auditorias de Nível 2 podem ser realizadas por auditores externos qualificados e independentes.

- **Nível 3 – A Auditoria Interna do Grupo Capgemini** é responsável pela auditoria de DPOs locais e globais, Linhas de Negócios Globais (GBL) e/ou funções centrais em relação ao Livro Azul e às BCR.

Como parte do nosso compromisso com a implementação de mecanismos de controle rigorosos e considerando as diversas localizações e estruturas de nossa empresa, nosso Programa de Auditorias BCR foi projetado para abranger todas as áreas, ano após ano, em um período máximo de cinco anos. Isso garante que todos os aspectos de nossas operações sejam representados e auditados dentro desse prazo.

Os relatórios de auditoria, incluindo as medidas corretivas propostas para fazer face e atenuar os riscos, devem ser comunicados à organização de proteção de dados – e, em particular, ao(s) DPO local(is) competente(s) – e à direção de topo, e devem ser disponibilizados à(s) autoridade(s) de supervisão competente(s), mediante pedido.

12. Uso de Operadores internos ou externos

12.1. Acordos de tratamento de dados ou cláusulas de proteção de dados

A Capgemini contará com Operadores de dados, dentro ou fora do grupo, apenas na medida em que tais Operadores forneçam garantias suficientes para implementar medidas técnicas e organizacionais para garantir que o tratamento seja realizado em conformidade com a lei local de proteção de dados aplicável.

Ao confiar em outra empresa da Capgemini (Operador interno) ou em um provedor terceirizado (Operador externo) para processar dados pessoais, a Capgemini celebrará um contrato de tratamento de dados (DPA) ou cláusula de proteção de dados que forneça as condições sob as quais o Operador processará os dados pessoais. No mínimo, o DPA ou a cláusula de proteção de dados deve prever que o Operador deve:

- Processar os dados pessoais apenas de acordo com as instruções documentadas da Capgemini – inclusive no que diz respeito a transferências de dados para países localizados fora do EEE.
- Garantir que as pessoas autorizadas a processar os dados pessoais se comprometeram com uma obrigação de confidencialidade.
- Implementar medidas técnicas e organizativas que garantam um nível adequado de proteção dos dados pessoais.
- Use apenas um suboperador com a autorização prévia específica ou geral da Capgemini e celebre um contrato com esse suboperador que forneça as mesmas obrigações que as descritas aqui.
- Auxiliar a Capgemini no cumprimento de sua obrigação de responder às solicitações dos titulares de dados.
- Auxiliar a Capgemini a garantir o cumprimento de suas obrigações em termos de segurança do tratamento, realizando DPIAs, relatando violações de dados.
- À escolha da Capgemini, e conforme acordado no DPA ou na cláusula de proteção de dados, excluir ou devolver os dados pessoais após o término da prestação de serviços.
- Disponibilizar à Capgemini todas as informações necessárias para demonstrar a conformidade com suas obrigações sob a lei de proteção de dados aplicável e, em particular, o GDPR, e permitir auditorias de proteção de dados.
- Relate qualquer violação de dados sem atrasos indevidos.

Na prática, antes de confiar em qualquer Operador externo, a Capgemini deve:

1. Realizar uma due diligence de proteção de dados e segurança cibernética para avaliar a maturidade dos provedores e garantir que os dados pessoais sejam processados de maneira segura.
   A Capgemini elaborou questionários dedicados que permitem que essa avaliação seja realizada. Os provedores são obrigados a preencher esse questionário, permitindo que a Capgemini determine seu nível de maturidade em proteção de dados, bem como o dos serviços que prestariam.

2. Celebrar um contrato contendo um DPA ou cláusula de proteção de dados que forneça as condições sob as quais o provedor processará dados pessoais em nome da Capgemini.
   A Capgemini elaborou modelos de DPA para abordar diferentes cenários – dependendo da qualificação das partes (Controlador/Controlador, Controlador/Operador, etc.). Independentemente de a Capgemini confiar ou não em tal modelo, a Capgemini analisará e negociará todos os DPAs para garantir que os provedores acessem, coletem ou processem dados pessoais apenas em conformidade com a lei de proteção de dados aplicável.

12.2. Obrigações adicionais em caso de transferências para países terceiros

Além da implementação do DPA ou da cláusula de proteção de dados acima mencionados, quando o uso de um Operador de dados envolver transferência(s) internacional(is) de dados pessoais, a Capgemini deve garantir que um nível adequado de proteção seja fornecido, de acordo com os requisitos detalhados abaixo.

Na prática, significa que:

- Quando uma empresa da Capgemini do EEE que atua como controladora transfere dados pessoais para uma empresa da Capgemini que não é do EEE que atua como controladora ou operadora, estas BCR-C serão aplicadas.

- Quando uma empresa da Capgemini do EEE que atua como controladora transfere dados pessoais para um terceiro localizado fora do EEE e que atua como controlador ou Operador, a Capgemini deve inserir os módulos relevantes das Cláusulas Contratuais Padrão aprovadas pela Comissão Europeia.

- Quando uma empresa da Capgemini fora do EEE que atua como controladora transfere dados pessoais para uma empresa da Capgemini ou para um terceiro localizado em um país que não é considerado como fornecendo um nível adequado de proteção pela lei de proteção de dados aplicável, a Capgemini implementará qualquer salvaguarda que possa ser exigida por tal lei aplicável, além destas BCR-C.

Além disso, ao transferir dados pessoais do EEE para um país que não se beneficia de uma decisão de adequação concedida pela Comissão Europeia, a Capgemini deve cumprir ainda as disposições das Seções 13 destas BCR-C.

13. Avaliações de impacto de transferência

As empresas da Capgemini no EEE só devem transferir dados pessoais para empresas da Capgemini fora do EEE ou para terceiros – ou seja, importadores de dados – localizados em um país que não se beneficie de uma decisão de adequação emitida pela Comissão Europeia, quando avaliarem que as leis e práticas de tal país não impedem o importador de dados de cumprir suas obrigações sob as BCR.

Esta avaliação deve ser feita no pressuposto de que a legislação e a prática do país para onde os dados pessoais são transferidos respeitam a essência dos direitos e liberdades fundamentais das pessoas e não excedem o que é necessário e proporcionado numa sociedade democrática para salvaguardar objetivos de interesse público.

Na prática, ao realizar uma avaliação de impacto de transferência (TIA), a Capgemini deve considerar:

1. As circunstâncias específicas da transferência ou conjunto de transferências e de qualquer transferência subsequente prevista dentro do mesmo país ou para outro país, incluindo:
    - A(s) finalidade(s) para a(s) qual(is) os dados são transferidos e processados posteriormente (por exemplo, RH, suporte de TI, etc.)
    - Os tipos de entidades envolvidas na transferência.
    - O setor econômico do importador e do exportador de dados e no qual a transferência ocorre.
    - A(s) categoria(s) e o formato dos dados pessoais transferidos.
    - O local do tratamento, incluindo armazenamento, e
    - Os canais de transmissão usados.

2. As leis e práticas do país de destino, relevantes à luz das circunstâncias da transferência, incluindo aquelas que exigem a divulgação de dados pessoais às autoridades públicas ou autorizam o acesso por essas autoridades e aquelas que fornecem acesso a esses dados pessoais durante a transferência, bem como as limitações e salvaguardas aplicáveis.

3. Quaisquer salvaguardas contratuais, técnicas ou organizacionais relevantes implementadas para complementar as salvaguardas sob a BCR-C, incluindo medidas aplicadas durante a transmissão e o tratamento de dados pessoais no país de destino.

Quando o TIA revelar que salvaguardas suplementares devem ser implementadas, além daquelas fornecidas pela BCR-C, a(s) Empresa(s) Capgemini do EEE que transfere(m) os dados e seu(s) DPO(s) deve(m) ser notificada(s) e envolvida(s) na implementação de tais salvaguardas.

A Capgemini monitorará continuamente as leis e práticas de países terceiros onde as empresas da Capgemini estão estabelecidas e onde os dados pessoais são transferidos de acordo com as BCR-C, para identificar quaisquer alterações que exijam a atualização do(s) TIA(s) e a implementação de salvaguardas suplementares.

Quando uma empresa da Capgemini fora do EEE que importa dados pessoais tiver motivos para acreditar que está sujeita a leis e práticas que a impediriam de cumprir suas obrigações sob a BCR-C, ela deverá notificar o escritório

de proteção de dados do grupo, para garantir que as salvaguardas adicionais apropriadas sejam implementadas para proteger a(s) transferência(s).

Da mesma forma, quando uma empresa da Capgemini que exporta dados pessoais tiver motivos para acreditar que uma empresa da Capgemini que atua como importadora não pode mais cumprir suas obrigações sob as BCR-C, ela deve notificar o escritório de proteção de dados do grupo para garantir que as salvaguardas adicionais apropriadas sejam implementadas para proteger a(s) transferência(s).

O(s) DPO(s) local(is) competente(s) deve(m) apoiar as empresas da Capgemini que atuam como exportadoras e importadoras na identificação e implementação das medidas suplementares apropriadas para garantir que as transferências de dados estejam em conformidade com as leis locais aplicáveis e estas BCR-C.

Quando uma empresa da Capgemini determinar que as BCR-C não podem mais ser cumpridas – mesmo após a implementação de medidas suplementares – para uma transferência ou conjunto de transferências específico, ou se instruída por uma autoridade supervisora competente a fazê-lo, ela deverá suspender essa transferência ou conjunto de transferências em jogo – bem como todas as transferências para as quais a mesma avaliação e raciocínio levariam a um resultado semelhante – até que a conformidade possa ser alcançada ou A transferência é encerrada. Se o cumprimento das BCR-C não for restabelecido no prazo de um mês a contar da suspensão, a transferência ou conjunto de transferências em causa cessa. Os dados pessoais que foram transferidos antes da suspensão e suas cópias serão devolvidos ou destruídos em sua totalidade à escolha da empresa Capgemini que atua como exportadora de dados.

A Capgemini deve documentar e registrar TIAs – incluindo a natureza das salvaguardas suplementares implementadas para garantir a transferência. Essa documentação deve ser disponibilizada à(s) autoridade(s) fiscalizadora(s) competente(s), mediante pedido.

Na prática, as avaliações das leis e práticas de países terceiros, bem como os TIAs específicos realizados para uma transferência ou conjunto de transferências e as salvaguardas suplementares identificadas e implementadas, bem como toda a documentação relevante – incluindo casos em que medidas suplementares não puderam ser implementadas, devem ser disponibilizadas a todos os DPOs da Capgemini. Assim, permitindo que a Capgemini garanta a conformidade com as BCR-C e a consistência na forma como são implementadas em todo o grupo.

14. Gestão de solicitações de acesso de autoridades públicas

A Capgemini deve revisar sistematicamente a legalidade de uma solicitação de acesso ou divulgação de dados pessoais. A Capgemini contestará tal solicitação se, após uma análise cuidadosa, determinar que há motivos razoáveis para considerar que a solicitação é ilegal de acordo com a lei aplicável, as obrigações aplicáveis de acordo com o direito internacional e os princípios de cortesia internacional. A Capgemini deverá, nas mesmas condições, buscar possibilidades de recurso.

Na prática, os funcionários da Capgemini são instruídos a transferir qualquer solicitação de divulgação de dados pessoais que possam receber para o departamento jurídico local para análise.

Ao contestar um pedido, a Capgemini deve buscar medidas provisórias para suspender os efeitos do pedido até que a autoridade judicial competente tenha decidido sobre seu mérito. A Capgemini não divulgará os dados pessoais solicitados pela autoridade até que seja expressamente exigido de acordo com as regras processuais aplicáveis.

Quando a Capgemini for obrigada a responder à solicitação, ela deverá fornecer a quantidade mínima de informações permitidas. Além disso, qualquer transferência ou conjunto de transferências realizadas pela Capgemini para atender a uma solicitação de uma autoridade pública ou de aplicação da lei não deve ser massiva, desproporcional ou indiscriminada de maneira que vá além do que é necessário em uma sociedade democrática.

Quando legalmente permitido, a empresa Capgemini que atua como importadora de dados deve notificar imediatamente a empresa Capgemini que atua como exportadora de dados e, quando possível, o(s) titular(es) dos dados envolvidos, quando:

1. Recebe um pedido juridicamente vinculativo emitido por uma autoridade pública para a divulgação de dados pessoais transferidos ao abrigo da BCR-C.
2. Tome conhecimento de qualquer acesso direto por uma autoridade pública a dados pessoais transferidos ao abrigo da BCR-C.

Essa notificação deve incluir todas as informações disponíveis para a empresa Capgemini que atua como importadora de dados e, em particular: os dados pessoais solicitados, a autoridade solicitante, a base legal para a solicitação e a resposta fornecida.

Quando proibido de notificar o exportador de dados e/ou o(s) titular(es) envolvido(s), o importador de dados deve envidar todos os esforços para obter uma isenção de tal proibição de comunicar o máximo de informações possível e o mais rápido possível. Deve documentar esses esforços para poder demonstrá-los a pedido do exportador de dados.

Na prática, todas as empresas da Capgemini são obrigadas a monitorar e registrar, mensalmente, informações sobre quaisquer solicitações públicas e/ou de autoridades policiais para acessar dados pessoais que possam ter recebido. Esses relatórios incluem, em particular:

- O número de solicitações.
- O(s) tipo(s) de dados solicitado(s).
- A(s) autoridade(s) que emitiu(ões) o(s) pedido(s).
- Se os pedidos foram contestados.
- O resultado.

Os DPOs locais e regionais registram essas informações e as compartilham com o escritório de proteção de dados do grupo. As informações devem ser acessíveis a todos os EPD regionais e locais, conservadas durante o tempo necessário e disponibilizadas às autoridades fiscalizadoras, mediante pedido.

Quando uma empresa da Capgemini for ou for proibida de relatar as informações listadas acima, ela deverá notificar o escritório de proteção de dados do grupo sem atrasos indevidos.

15. Responsabilidade da Capgemini em caso de violação das BCR-C

Cada empresa da Capgemini do EEE que exporta dados pessoais para uma empresa da Capgemini fora do EEE será responsável, perante os titulares de dados, por quaisquer violações das BCR-C causadas pela empresa da Capgemini fora do EEE.

Em todos os outros casos – (1) transferências de uma Capgemini do EEE para outra empresa da Capgemini do EEE, (2) transferências entre duas empresas da Capgemini fora do EEE ou (3) transferências de uma empresa da Capgemini fora do EEE para uma empresa da Capgemini do EEE – cada empresa da Capgemini será responsável por uma violação das BCR-C que causou.

Quando uma transferência entre duas empresas da Capgemini fora do EEE constituir uma transferência subsequente, a empresa da Capgemini do EEE que iniciou a transferência pela primeira vez será responsável perante os titulares de dados, por quaisquer violações da BCR-C causadas por qualquer uma das empresas não pertencentes ao EEE.

A lista de empresas da Capgemini é fornecida no Apêndice 1. Os indivíduos podem exercer seus direitos de proteção de dados e/ou enviar uma reclamação por meio do processo dedicado da Capgemini descrito na Seção 7.

Na prática, isso significa que a empresa Capgemini identificada como responsável de acordo com o esquema acima mencionado deve aceitar a responsabilidade pelo pagamento da indenização e pela reparação da violação quando ela causou um dano a um titular de dados. Os titulares de dados enviam solicitações ou reclamações entrando em contato com o(s) DPO(s) competente(s) por meio do processo dedicado.

Se uma empresa da Capgemini fora do EEE violar as BCR-C, os tribunais ou outras autoridades judiciais do EEE terão jurisdição e os titulares de dados terão os direitos e recursos contra a empresa responsável da Capgemini do EEE (ou seja, a Capgemini do EEE que transferiu os dados pessoais para uma empresa da Capgemini fora do EEE) como se a violação tivesse sido causada por esta última no Estado-Membro em que está sediada.

Além disso, cabe à Capgemini demonstrar que não violou a BCR-C. No caso de uma transferência entre uma empresa Capgemini do EEE e uma empresa Capgemini não pertencente ao EEE, se a suposta violação for atribuída à empresa Capgemini não pertencente ao EEE, a empresa Capgemini do EEE deve demonstrar que a empresa Capgemini não pertencente ao EEE não violou realmente as BCR-C.

16. Não conformidade com a BCR-C

Caso uma empresa da Capgemini que atue como importadora de dados não consiga cumprir as BCR-C por qualquer motivo, ela deverá informar a(s) empresa(s) Capgemini que atua(m) como exportadora de dados. Caso uma empresa da Capgemini que atua como exportadora de dados tome conhecimento de uma violação e/ou incapacidade da empresa da Capgemini que atua como importadora de dados de cumprir as BCR-C, ela deve suspender a transferência.

A empresa Capgemini que atua como importadora de dados deve, à escolha da empresa Capgemini que atua como exportadora de dados, devolver ou excluir imediatamente os dados pessoais – incluindo quaisquer cópias deles – que foram transferidos sob a BCR-C em sua totalidade, quando:

- O exportador de dados suspendeu a transferência e a conformidade com as BCR-C não foi restaurada dentro de um prazo razoável e, em qualquer caso, dentro de um mês após a suspensão, ou
- O importador de dados viola substancialmente ou persistentemente as BCR-C, ou
- O importador de dados não cumpre uma decisão vinculativa de um tribunal competente ou autoridade de supervisão competente em relação às suas obrigações nos termos da BCR-C.

Quando a empresa Capgemini que atua como exportadora de dados exigiu que a empresa Capgemini que atua como importadora de dados excluísse os dados, a empresa Capgemini que atua como importadora de dados deverá certificar a exclusão dos dados para a empresa Capgemini que atua como exportadora de dados. Até que os dados sejam apagados ou devolvidos, o importador de dados deve continuar a assegurar a conformidade com as BCR-C.

Quando as leis locais aplicáveis à empresa Capgemini que atua como importadora de dados proibirem a devolução ou exclusão dos dados pessoais transferidos, ela se comprometerá a continuar garantindo a conformidade com as BCR-C e processará os dados apenas na medida e pelo tempo exigido por essa lei local.

17. Cooperação com as autoridades Fiscalizadoras

A Capgemini cooperará com as autoridades de supervisão.

Na prática, isso significa que a Capgemini deve cumprir o conselho e/ou decisão das autoridades supervisoras competentes e aceitar ser auditada e/ou inspecionada por elas (se necessário no local) e/ou compartilhar documentação com elas mediante solicitação.

Qualquer disputa relacionada ao exercício da supervisão da conformidade com as BCR-C pela autoridade supervisora competente será resolvida pelos tribunais do Estado-Membro dessa autoridade supervisora, de

acordo com a lei processual desse Estado-Membro, e as empresas da Capgemini concordam em se submeter à jurisdição desses tribunais.

18. Fácil acesso à BCR

A versão pública da BCR-C está disponível no site da Capgemini https://www.capgemini.com/about-us/management-and-governance/policies/data-protection-policy/ , bem como na Intranet da Capgemini.

A versão pública da BCR-C contém todos os elementos da versão interna da BCR-C, exceto os seguintes apêndices, que são documentos confidenciais que não podem ser compartilhados fora da organização:

- O acordo BCR intragrupo
- Política de tratamento de solicitações dos titulares de dados da Capgemini
- Descrição do trabalho de DPO de grupo, regional e local
- eLearning obrigatório de proteção de dados da Capgemini
- Política de auditoria de proteção de dados da Capgemini
- Gestão de solicitações de divulgação de dados pessoais

A versão mais recente da BCR-C será disponibilizada a todos os funcionários da Capgemini. No caso de uma atualização significativa das BCR-C, a Capgemini informará seus funcionários, lançando uma campanha de comunicação dedicada para garantir que os funcionários estejam cientes e compreendam suas obrigações e direitos sob a BCR-C. Além disso, o eLearning obrigatório de proteção de dados da Capgemini inclui referências às BCR-C e os funcionários são obrigados a baixar e ler as BCR-C após a conclusão do treinamento.

19. Atualizações BCR

A Capgemini manterá as BCR-C atualizadas, em particular para refletir quaisquer alterações regulatórias, incluindo recomendações do Conselho Europeu de Proteção de Dados.

O escritório de proteção de dados do grupo é responsável pela atualização da BCR-C – incluindo a manutenção da lista de empresas da Capgemini. O escritório de proteção de dados do grupo deve compartilhar qualquer atualização da BCR-C com as empresas da Capgemini e seus respectivos DPOs sem atrasos indevidos. Como tal, o escritório de proteção de dados do grupo deve fornecer as informações necessárias aos titulares de dados e/ou às autoridades de supervisão.

Caso a Capgemini faça qualquer alteração substancial nas BCR-C, ela deverá primeiro entrar em contato com sua principal autoridade supervisora, a CNIL, e fornecer uma explicação sobre tais alterações.

Uma vez por ano, a Capgemini comunicará à CNIL quaisquer modificações feitas nas BCR-C, incluindo uma lista atualizada de empresas da Capgemini. Essa comunicação deve incluir igualmente uma confirmação relativa aos ativos do grupo.

20. Rescisão

Caso qualquer empresa da Capgemini, atuando como importadora de dados, deixe de estar vinculada às BCR-C, ela deverá manter, devolver ou excluir os dados pessoais transferidos sob as BCR-C.

A decisão de permitir que a antiga empresa Capgemini mantenha os dados pessoais será tomada pelo escritório de proteção de dados do grupo. Caso a antiga empresa da Capgemini tenha permissão para manter os dados pessoais, ela se comprometerá a processar esses dados em conformidade com todos os requisitos de proteção de dados aplicáveis, incluindo o GDPR.

Sobre a Capgemini

A Capgemini é líder global em parcerias com empresas para transformar e gerenciar seus negócios, aproveitando o poder da tecnologia. O Grupo é guiado todos os dias por seu propósito de liberar a energia humana por meio da tecnologia para um futuro inclusivo e sustentável. É uma organização responsável e diversificada de mais de 360.000 membros da equipe em mais de 50 países. Com sua forte herança de 55 anos e profunda experiência no setor, a Capgemini tem a confiança de seus clientes para atender a toda a amplitude de suas necessidades de negócios, desde estratégia e design até operações, alimentadas pelo mundo inovador e em rápida evolução da nuvem, dados, IA, conectividade, software, engenharia digital e plataformas. O Grupo registrou em 2022 receitas globais de € 22 bilhões.

Obtenha o futuro que você deseja | www.capgemini.com

ANEXO ÀS REGRAS CORPORATIVAS VINCULANTES – CONTROLADOR DA CAPGEMINI – APLICAÇÃO NO BRASIL ("ANEXO BRASIL-C ")

Para fins de atendimento à legislação brasileira de proteção de dados, especialmente a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), as seguintes disposições das **Regras Corporativas Vinculantes---Controlador** da Capgemini, aprovadas pela Autoridade Francesa de Proteção de Dados - *CNIL (Commission Nationale de l'Informatique et des Libertés)*, passarão a vigorar conforme alterações sugeridas neste Anexo.

A. Na seção "Introdução" a redação passará a vigorar da seguinte forma:

Como líder global em consultoria, serviços de tecnologia e transformação digital, a Capgemini está na vanguarda da inovação, aproveitando nuvem, dados, conectividade de IA, software, engenharia digital e plataformas para atender a toda a amplitude das necessidades de nossos clientes. Desde o avanço da experiência digital do consumidor até a aceleração da indústria inteligente e a transformação da eficiência empresarial, ajudamos nossos clientes a definir o caminho certo para um futuro melhor.

A Capgemini está comprometida em proteger todos os dados pessoais que lhe são confiados como parte de suas atividades. Como um grupo internacional com entidades localizadas em mais de 40 países, é essencial para a Capgemini que as informações fluam livremente e com segurança. Fornecer um forte nível de proteção aos dados pessoais transferidos dentro do grupo é uma das razões pelas quais a Capgemini optou por implementar essas Regras Corporativas Vinculantes (BCR), que foram aprovadas pela primeira vez pela autoridade francesa de proteção de dados, a CNIL, em março de 2016 e posteriormente alteradas em 2019 e 2023 para cumprir o Regulamento Geral de Proteção de Dados (GDPR) e o Conselho Europeu de Proteção de Dados atualizou os requisitos além dos chamados *Schrems II* decisão.

Mais do que um mero mecanismo de transferência de dados, as BCR da Capgemini são nossa política global de proteção de dados, uma estrutura abrangente que define toda a nossa abordagem de responsabilidade para o tratamento de dados pessoais. As BCR da Capgemini não apenas definem os princípios que devem ser cumpridos ao processar Dados Pessoais, mas também especificam os procedimentos implementados para cumprir as leis de proteção de dados aplicáveis e, em particular, o Regulamento Geral de Proteção de Dados 2016/679 e, localmente no Brasil, a Lei Geral de Proteção de Dados Pessoais - Lei nº. 13.709 de 14 de agosto de 2018 (LGPD).

B. Na seção "Definições", será adotado o seguinte:
B,1. A redação dos itens abaixo passarão a vigorar da seguinte forma:

"**Empresa Capgemini do EEE" será referido como "Empresa Capgemini do EEE/Brasil**": significa qualquer empresa Capgemini localizada no EEE, ou localizada no Brasil.

"**Empresa Capgemini fora do EEE"** será referido como **Empresa Capgemini fora do EEE/Brasil**": significa qualquer empresa Capgemini localizada fora do EEE/Brasil.

"**Cláusulas-Padrão Contratuais**" significa as cláusulas contratuais emitidas pela Comissão Europeia e pela Autoridade Nacional de Proteção de Dados (ANPD) para enquadrar as transferências internacional de dados de Controladores estabelecidos

no EEE/Brasil para Controladores estabelecidos fora do EEE/Brasil e de Controladores estabelecidos no EEE/Brasil para Operadores estabelecidos fora do EEE/Brasil.

B.2. A inclusão do seguinte item:

"**Lei Geral de Proteção de Dados Pessoais**" ou "**LGPD**", refere-se a Lei Federal nº. 13.709 de 14 de agosto de 2018 em vigor no Brasil, que dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

B.3. A leitura dos seguintes termos:

Onde se lê **"Diretor de Proteção de Dados"**, será adotado o termo **"Encarregado pelo tratamento de dados pessoais"**

Onde se lê "**Categorias Especiais de Dados Pessoais"** será adotado o termo "**Dados Pessoais Sensíveis"**.

C. Na seção "1.2 Âmbito geográfico", a redação passará a vigorar da seguinte forma:

1.2 Âmbito geográfico

Estas BCR-C abrangem todos os dados pessoais que estão sendo transferidos e processados posteriormente dentro do grupo, independentemente da origem dos dados pessoais. As BCR-C abrangem todas as transferências de dados pessoais realizadas dentro do grupo, incluindo transferências subsequentes.

Na prática, isso significa que as BCR-C se aplicam aos dados pessoais transferidos de:

- Uma empresa Capgemini do EEE para outra empresa Capgemini do EEE
- Uma empresa Capgemini do EEE/Brasil para uma empresa Capgemini não pertencente ao EEE/Brasil
- Uma empresa Capgemini fora do EEE/Brasil para uma empresa Capgemini do EEE/Brasil
- Uma empresa da Capgemini fora do EEE/Brasil para outra empresa da Capgemini fora do EEE/Brasil.

As empresas da Capgemini obrigadas a cumprir estas BCR-C estão listadas no Apêndice 1.

D. Na seção "2.1. Vinculação nas empresas da Capgemini", a redação passará a vigorar da seguinte forma:

2.1 Vinculação nas empresas da Capgemini

Na prática, cada entidade da Capgemini dá uma procuração à Capgemini International BV para assinar o acordo intragrupo e o Anexo às Regras Corporativas Vinculantes – Controlador da Capgemini- Aplicação Brasil em seu nome, para que cada entidade da Capgemini seja efetivamente obrigada a cumprir as BCR-C. Ao assinar o acordo intragrupo e Anexo às Regras Corporativas Vinculantes – Controlador da Capgemini-Aplicação Brasil, as entidades da Capgemini se comprometem a cumprir as disposições

da BCR-C e do Anexo às Regras Corporativas Vinculantes – Controlador da Capgemini-Aplicação Brasil e a implementar seus princípios dentro de sua própria organização.

Quando a Capgemini criar ou adquirir novas entidades, em particular quando estas estiverem localizadas fora do EEE/Brasil, nenhum dado pessoal será transferido para elas até que estejam totalmente aptas a cumprir e efetivamente vinculadas às BCR-C e ao Anexo às Regras Corporativas Vinculantes – Controlador da Capgemini- Aplicação Brasil de acordo com o mecanismo acima mencionado.

E. Na seção "3.2 Base Jurídica", a inclusão do seguinte trecho:

Quando o tratamento de dados pessoais for fundamentado em uma base legal prevista no GDPR e na LGPD, a base legal eleita pela controladora será a hipótese correspondente em ambas as legislações. Caso não haja correspondência, as bases legais eleitas são aquelas elencadas nos artigos 7º e 11 da LGPD, conforme finalidades e categorias de dados pessoais envolvidas, conforme Apêndice 2.

F. Na seção "3.7. Tratamento de categorias especiais de dados pessoais e dados relacionados a condenações criminais e infrações", a redação passará a vigorar da seguinte forma:

3.7. Tratamento de categorias especiais de dados pessoais e dados relacionados a condenações criminais e infrações

A Capgemini só tratará categorias especiais de dados pessoais e/ou dados relacionados a condenações criminais e ofensas – revelando origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas ou filiação sindical, e dados genéticos e/ou biométricos com a finalidade de identificar exclusivamente um indivíduo, dados relativos à saúde ou à vida sexual ou orientação sexual de um indivíduo – quando estritamente necessário e/ou legalmente exigido.

No contexto do EEE:

- O indivíduo deu consentimento explícito para o tratamento desses dados pessoais para um ou mais fins específicos.
- O tratamento desses dados é necessário para que a Capgemini ou o indivíduo cumpra uma obrigação ou exerça direitos específicos na legislação trabalhista, previdenciária e de proteção social.
- O tratamento é necessário para proteger os interesses vitais do indivíduo cujos dados são processados ou de outro indivíduo.
- O tratamento é necessário para o estabelecimento, exercício ou defesa de reivindicações legais ou sempre que os tribunais estiverem agindo em sua capacidade judicial.
- O tratamento é necessário por motivos de interesse público substancial.
- O tratamento é necessário por razões de interesse público no domínio da saúde pública, como a proteção contra ameaças transfronteiriças graves para a saúde.

No contexto do Brasil:

- O indivíduo forneceu consentimento de forma específica, destacada e explícita para o tratamento dos seus dados sensíveis para uma ou mais finalidades determinadas.

- O tratamento desses dados é essencial para o cumprimento de uma obrigação legal ou regulatória pela Capgemini.
- O tratamento destes dados é necessário para que a Capgemini ou o indivíduo exerçam regularmente seus direitos, inclusive em contratos e em processos judiciais, administrativos e arbitrais;
- O tratamento é indispensável para a proteção da vida ou da segurança física de um indivíduo ou de um terceiro.
- O tratamento dos dados é necessário para a prevenção de fraudes e garantia a da segurança do titular, especificamente nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Na prática, a Capgemini deve abster-se de processar quaisquer categorias especiais de dados pessoais e/ou quaisquer dados pessoais relacionados a condenações criminais e ofensas, a menos que uma das condições listadas acima seja atendida.

Categorias especiais de dados pessoais e/ou dados relacionados a condenações criminais e infrações só serão transferidas do EEE/Brasil para outros países, quando cobertos por um nível de proteção equivalente ao fornecido pela legislação do EEE/Brasil.

G. Na seção "4. Transparência", a redação passará a vigorar da seguinte forma:

4. Transparência

A Capgemini fornecerá aos titulares de dados todas as informações necessárias sobre o tratamento de seus dados pessoais.

Quando os dados pessoais relacionados a indivíduos são coletados diretamente deles, a Capgemini deve, no mínimo, compartilhar as seguintes informações:

- A identidade e os detalhes de contato da empresa Capgemini que atua como controladora de dados;
- Os dados de contacto do encarregado da proteção de dados competente;
- A(s) finalidade(s) para a(s) qual(is) os dados pessoais são tratados, bem como a(s) base(s) legal(is) para o tratamento;
- Quando o tratamento for baseado no interesse legítimo da Capgemini, a descrição do interesse perseguido pela Capgemini;
- Os destinatários ou categorias de destinatários, se houver, isso é relevante nos casos em que a Capgemini compartilharia;
- Se a Capgemini pretende transferir dados pessoais para fora do EEE/Brasil e a existência ou ausência de uma decisão de adequação da Comissão Europeia/ANPD, ou a referência às salvaguardas apropriadas (coma BCR ou Cláusulas-Padrão Contratuais) e como obter uma cópia delas;
- O período durante o qual os dados pessoais serão armazenados ou, se não for possível, os critérios utilizados para determinar esse período;
- O direito do Titular de dados de solicitar o acesso e a retificação ou apagamento dos dados pessoais ou a limitação do tratamento ou de se opor ao tratamento, bem como o direito à portabilidade;
- Quando o tratamento for baseado no consentimento do indivíduo, o direito de retirar o consentimento a qualquer momento, sem afetar a legalidade do tratamento;
- O direito de apresentar uma reclamação perante uma autoridade de proteção de dados e/ou supervisora;

- Se o fornecimento de dados pessoais é um requisito legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o indivíduo é obrigado a fornecer os dados pessoais e as possíveis consequências do não fornecimento desses dados;
- A existência de tomadas de decisão automatizadas, incluindo a definição de perfis, e informações sobre a lógica envolvida, bem como a importância e as consequências previstas de tal tratamento para o indivíduo.

Quando os dados pessoais não forem obtidos diretamente do indivíduo, a Capgemini ainda fornecerá as informações acima mencionadas dentro de um período razoável após a obtenção dos dados pessoais, bem como a descrição das categorias de dados pessoais e a(s) fonte(s) desses dados pessoais. Se os dados forem usados para entrar em contato com o indivíduo, a Capgemini fornecerá as informações no momento dessa primeira comunicação.

Na prática, a Capgemini disponibiliza avisos de "proteção de dados" ou "privacidade" aos indivíduos para fornecer as informações necessárias.
Ao coletar dados pessoais diretamente de indivíduos para fins específicos, por exemplo, por meio de aplicativos ou ferramentas voltados para o usuário, a Capgemini elaborará e disponibilizará avisos personalizados.
A Capgemini também elaborou e publicou avisos de proteção de dados mais gerais, como o disponível em seu site, que abrange uma gama mais ampla de atividades de tratamento, incluindo, por exemplo, tratamento relacionado a marketing.

H. Na seção "5. Direitos dos titulares de dados", a redação passará a vigorar da seguinte forma:

5. Direitos dos titulares de dados

Os indivíduos cujos dados pessoais são tratados pela Capgemini podem exercer todos os direitos previstos no Capítulo III da LGPD, incluindo, mas não se limitando, os direitos de solicitar acesso, retificação ou exclusão de seus dados, opor-se ao tratamento dos seus dados e têm o direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, , incluindo a definição de perfis.

Na prática, os indivíduos são informados de seus direitos por meio de avisos dedicados e podem exercer seus direitos entrando em contato com a Capgemini de acordo com o processo detalhado no Apêndice 4.

Os titulares de dados podem exercer esses direitos entrando em contato com o DPO, ou outro ponto de contato que possa ser relevante. O Titular de dados também pode apresentar uma reclamação com relação ao tratamento de seus dados pessoais, por meio desse mesmo processo.

Além disso, os indivíduos têm o direito de peticionar contra o controlador perante à(s) autoridade(s) supervisora(s) competente(s) e/ou perante o tribunal competente.

Em caso de violação dos direitos garantidos e/ou obrigações previstas nas BCR-C, a Capgemini incentiva os indivíduos a enviar uma reclamação. No entanto, os indivíduos também têm o direito de apresentar uma reclamação perante a(s) autoridade(s) supervisora(s) competente(s) – que pode ser a do Brasil ou do Estado-Membro da UE de sua residência habitual, local de trabalho ou local da suposta violação. Além disso,

os particulares podem apresentar uma queixa perante o tribunal do Brasil ou do Estado-Membro da sua residência habitual, do seu local de trabalho ou do local da alegada infração. Quando o tratamento de dados pessoais for realizado por uma empresa da Capgemini fora do EEE/Brasil, os indivíduos poderão apresentar uma reclamação perante o tribunal competente, conforme previsto na legislação local aplicável, a menos que o tratamento e/ou a empresa da Capgemini fora do EEE/Brasil esteja sujeita ao(à) GDPR/LGPD, caso em que as disposições acima mencionadas serão aplicadas.

Os Titulares de Dados têm direito a recursos judiciais e o direito de obter reparação e, se for caso disso, compensação em caso de violação de um dos elementos aplicáveis da BCR-C, conforme listado na Seção 6. Os titulares de dados podem ser representados por uma organização ou associação sem fins lucrativos para exercer esses direitos, nas condições previstas pela legislação local aplicável.

Na prática, em caso de violação das BCR-C, os indivíduos podem apresentar uma reclamação diretamente à Capgemini e/ou à autoridade de proteção de dados e/ou tribunal competente. Além disso, os indivíduos podem buscar reparação, reparação e compensação em caso de violação de um dos elementos listados na Seção 6.

I. **Na seção "6. Direitos de aplicação dos titulares de dados", a redação passará a vigorar da seguinte forma:**

6. Direitos de aplicação dos titulares de dados

Os titulares de dados podem fazer valer os seguintes elementos da BCR-C, como terceiros beneficiários:

- A implementação dos princípios de proteção de dados detalhados nas Seções 3, 4 e 12 da BCR-C.
- A obrigação da Capgemini de compartilhar informações relevantes com os indivíduos sobre o tratamento de seus dados pessoais, conforme previsto na Seção 4; bem como a obrigação de fornecer acesso fácil às BCR-C, conforme previsto na Seção 17.
- Direitos dos indivíduos em relação ao tratamento de seus dados pessoais, conforme previsto na Seção 5.
- Direito dos indivíduos de reclamar por meio do processo interno de reclamação da Capgemini, conforme previsto na Seção 5.
- Direitos dos indivíduos de apresentar uma reclamação à(s) autoridade(s) supervisora(s) competente(s) e/ou perante os tribunais competentes, conforme previsto nas Seções 5.
- A obrigação, para cada empresa da Capgemini fora do EEE/Brasil que importa dados pessoais, de notificar a Capgemini do EEE/Brasil que exporta esses dados pessoais, bem como a sede da Capgemini, em caso de conflito entre a legislação local aplicável e as BCR-C, conforme previsto na Seção 13.
- A obrigação, para cada empresa da Capgemini que importa dados pessoais, de informar a entidade exportadora da Capgemini, bem como a sede da Capgemini, e se legalmente permitido ao Titular de dados, sobre quaisquer solicitações de uma autoridade pública e/ou agência de aplicação da lei para acessar os dados pessoais conforme fornecido e detalhado na Seção 14.
- O dever da Capgemini de cooperar com as autoridades de supervisão, conforme previsto na Seção 16.

- A obrigação de cada empresa da Capgemini do EEE/Brasil que transfere dados pessoais para uma empresa da Capgemini fora do EEE/Brasil aceitar a responsabilidade por quaisquer violações das BCR-C pela empresa da Capgemini que não é do EEE/Brasil que recebe os dados, conforme previsto na Seção 15.
- O fato de que, em caso de violação das BCR-C por uma empresa não pertencente ao EEE/Brasil, cabe à empresa Capgemini do EEE/Brasil que exportou os dados pessoais demonstrar que o destinatário (ou seja, a empresa Capgemini não pertencente ao EEE/Brasil) não violou as BCR-C, conforme previsto na Seção 15.
- A obrigação da Capgemini de informar o Titular de dados sobre qualquer atualização das BCR-C – inclusive no que diz respeito à lista de empresas da Capgemini vinculadas às BCR-C – conforme previsto na Seção 18.
- A obrigação da Capgemini de permitir que os titulares de dados apliquem os elementos das BCR-C listados nesta Seção como terceiros beneficiários.
- O direito dos indivíduos de buscar recursos judiciais, obter reparação e, quando apropriado, indenização em caso de violação dos elementos executórios da BCR-C listados nesta Seção – conforme previsto na Seção 5.

J. Na seções "9. Privacidade desde a concepção" e "9.1. Registro das atividades de tratamento", a redação passará a vigorar da seguinte forma:

9. Privacidade desde a concepção

9.1. Registro das atividades de tratamento

Quando atuar como controladora, a Capgemini manterá e manterá, por escrito, um registro das atividades de tratamento contendo as seguintes informações:

- O nome e os detalhes de contato da empresa Capgemini que atua como controladora, do DPO competente e, quando aplicável, do(s) controlador(es) conjunto(s).
- O(s) objetivo(s) das atividades de tratamento.
- Uma descrição das categorias de titulares de dados e das categorias de dados pessoais tratados.
- As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo destinatários localizados fora do EEE/Brasil.
- Se for caso disso, as transferências transfronteiriças de dados pessoais, incluindo o(s) país(es) de destino, bem como o(s) mecanismo(s) de transferência utilizado(s) para enquadrar essas transferências.
- O período de retenção de dados.
- Uma descrição geral das medidas de segurança.

Na prática, o proprietário da empresa de qualquer ferramenta, aplicação ou qualquer outro projeto que envolva o tratamento de dados pessoais deve criar uma inscrição no registo, incluindo todos os dados acima mencionados. O(s) encarregado da proteção de dados competente(s) deve(m) rever a entrada para garantir que contém todas as informações necessárias para lhes permitir avaliar a conformidade do projeto em causa com a legislação aplicável em matéria de PD. Com base em sua avaliação, o DPO deve fazer recomendações para garantir que o proprietário da empresa realize atividades de tratamento em conformidade com estas BCR-C e com as leis de DP aplicáveis.

Ao atuar como Operador de dados, a Capgemini também manterá e manterá um registro das atividades de tratamento realizadas em nome do controlador e incluindo:

- O(s) nome(s) e detalhes de contato da(s) empresa(s) Capgemini que atua(m) como Operador(es), bem como o(s) nome(s) e detalhes de contato de cada controlador(es) em nome do(s) qual(is) estão processando os dados.
- As categorias de tratamento realizadas em nome de cada controlador.
- Se for caso disso, a(s) transferência(s) transfronteiriça(s) de dados pessoais, incluindo o(s) país(es) de destino, bem como o(s) mecanismo(s) de transferência utilizado(s) para enquadrar essas transferências.
- Uma descrição geral das medidas de segurança.

A Capgemini disponibilizará os registros de tratamento à(s) autoridade(s) supervisora(s) competente(s) mediante solicitação.

K. Na seção "9.2. Relatórios de impacto da proteção de dados", a redação passará a vigorar da seguinte forma:

9.2. Relatórios de impacto da proteção de dados

A Capgemini realizará um relatório de impacto sobre a proteção de dados (RIPD) quando uma atividade de tratamento provavelmente resultar em um alto risco para os direitos e liberdades dos indivíduos.

O grupo e/ou o DPO local devem avaliar as atividades de tratamento para determinar se devem ser consideradas de "alto risco" usando uma metodologia alinhada com as recomendações do Conselho Europeu de Proteção de Dados no contexto europeu, com as orientações da Autoridade Nacional Proteção de Dados (ANPD) no contexto brasileiro e com quaisquer outras práticas e/ou diretrizes locais emitidas pela autoridade de proteção de dados.

O Grupo e/ou os DPOs devem determinar a necessidade de realizar um RIPD para um tratamento de alto risco, considerando:

1. A possibilidade de um evento indesejável – por exemplo, acesso ilegítimo ou não autorizado aos dados, modificação ou exclusão dos dados etc.
2. A probabilidade de ocorrência de tal evento indesejável.
3. A gravidade das consequências para os direitos e liberdades dos titulares de dados.

Na prática, ao revisar as atividades de tratamento de dados, conforme descrito na subseção 9.1., o grupo ou DPO local deve determinar se o proprietário precisa iniciar um RIPD, respondendo a um questionário projetado para avaliar os riscos. O grupo ou o encarregado da proteção de dados local deve então rever a avaliação e formular recomendações para atenuar os riscos.

Se o RIPD indicar que a atividade de tratamento resultaria num risco elevado e o grupo ou o encarregado da proteção de dados local determinar que não pode ser aplicada nenhuma medida para atenuar esse risco, deve consultar a autoridade fiscalizadora competente. Quando aplicável, a autoridade supervisora deve revisar e avaliar a atividade de tratamento e determinar se a Capgemini avaliou adequadamente os riscos por meio do RIPD e se as salvaguardas que a Capgemini pretende implementar para lidar com os riscos são adequadas.

L. **Na seções "12. Uso de Operadores internos ou externos" e "12.1 Acordos de tratamento de dados ou cláusulas de proteção de dados", a redação passará a vigorar da seguinte forma:**

12 Uso de Operadores internos ou externos

12.1. Acordos de tratamento de dados ou cláusulas de proteção de dados

A Capgemini contará com Operadores de dados, dentro ou fora do grupo, apenas na medida em que tais Operadores forneçam garantias suficientes para implementar medidas técnicas e organizacionais para garantir que o tratamento seja realizado em conformidade com a lei local de proteção de dados aplicável.

Ao confiar em outra empresa da Capgemini (Operador interno) ou em um provedor terceirizado (Operador externo) para processar dados pessoais, a Capgemini celebrará um contrato de tratamento de dados (DPA) ou cláusula de proteção de dados que forneça as condições sob as quais o Operador processará os dados pessoais. No mínimo, o DPA ou a cláusula de proteção de dados deve prever que o Operador deve:

- Processar os dados pessoais apenas de acordo com as instruções documentadas da Capgemini – inclusive no que diz respeito a transferências de dados para países localizados fora do EEE/Brasil.
- Garantir que as pessoas autorizadas a processar os dados pessoais se comprometeram com uma obrigação de confidencialidade.
- Implementar medidas técnicas e organizativas que garantam um nível adequado de proteção dos dados pessoais.
- Use apenas um suboperador com a autorização prévia específica ou geral da Capgemini e celebre um contrato com esse suboperador que forneça as mesmas obrigações que as descritas aqui.
- Auxiliar a Capgemini no cumprimento de sua obrigação de responder às solicitações dos titulares de dados.
- Auxiliar a Capgemini a garantir o cumprimento de suas obrigações em termos de segurança do tratamento, realizando RIPDs, relatando violações de dados.
- À escolha da Capgemini, e conforme acordado no DPA ou na cláusula de proteção de dados, excluir ou devolver os dados pessoais após o término da prestação de serviços.
- Disponibilizar à Capgemini todas as informações necessárias para demonstrar a conformidade com suas obrigações sob a lei de proteção de dados aplicável e, em particular, o GDPR, e permitir auditorias de proteção de dados.
- Relate qualquer violação de dados sem atrasos indevidos.

Na prática, antes de confiar em qualquer Operador externo, a Capgemini deve:

1. Realizar uma due diligence de proteção de dados e segurança cibernética para avaliar a maturidade dos provedores e garantir que os dados pessoais sejam processados de maneira segura.
   A Capgemini elaborou questionários dedicados que permitem que essa avaliação seja realizada. Os provedores são obrigados a preencher esse questionário, permitindo que a Capgemini determine seu nível de maturidade em proteção de dados, bem como o dos serviços que prestariam.

2. Celebrar um contrato contendo um DPA ou cláusula de proteção de dados que forneça as condições sob as quais o provedor processará dados pessoais em nome da Capgemini.

A Capgemini elaborou modelos de DPA para abordar diferentes cenários – dependendo da qualificação das partes (Controlador/Controlador, Controlador/Operador, etc.). Independentemente de a Capgemini confiar ou não em tal modelo, a Capgemini analisará e negociará todos os DPAs para garantir que os provedores acessem, coletem ou processem dados pessoais apenas em conformidade com a lei de proteção de dados aplicável.

M. Na seção "12.2. Obrigações adicionais em caso de transferências para países terceiros", a redação passará a vigorar da seguinte forma:

12.2. Obrigações adicionais em caso de transferências para países terceiros

Além da implementação do DPA ou da cláusula de proteção de dados acima mencionados, quando o uso de um Operador de dados envolver transferência(s) internacional(is) de dados pessoais, a Capgemini deve garantir que um nível adequado de proteção seja fornecido, de acordo com os requisitos detalhados abaixo.

Na prática, significa que:

- Quando uma empresa da Capgemini do EEE/Brasil que atua como controladora transfere dados pessoais para uma empresa da Capgemini que não é do EEE/Brasil que atua como controladora ou operadora, estas BCR-C serão aplicadas.

- Quando uma empresa da Capgemini do EEE/Brasil que atua como controladora transfere dados pessoais para um terceiro localizado fora do EEE/Brasil e que atua como controlador ou Operador, a Capgemini deve inserir os módulos relevantes das Cláusulas-Padrão Contratuais aprovadas pela Comissão Europeia e pela Autoridade Nacional de Proteção de Dados (ANPD), conforme aplicável

- Quando uma empresa da Capgemini fora do EEE/Brasil que atua como controladora transfere dados pessoais para uma empresa da Capgemini ou para um terceiro localizado em um país que não é considerado como fornecendo um nível adequado de proteção pela lei de proteção de dados aplicável, a Capgemini implementará qualquer salvaguarda que possa ser exigida por tal lei aplicável, além destas BCR-C.

N. Na seção "13. Avaliações de impacto de transferência", a redação passará a vigorar da seguinte forma:

13. Avaliações de impacto de transferência

As empresas da Capgemini no EEE/Brasil só devem transferir dados pessoais para empresas da Capgemini fora do EEE/Brasil ou para terceiros – ou seja, importadores de dados – localizados em um país que não se beneficie de uma decisão de adequação emitida, quando aplicável pela Comissão Europeia ou pela Autoridade Nacional de Proteção de Dados (ANPD), quando (i) avaliarem que as leis e práticas de tal país não impedem o importador de dados de cumprir suas obrigações sob as BCR; e (ii) adotarem as salvaguardas adequadas previstas na LGPD, conforme regulado pela ANPD.

Esta avaliação deve ser feita no pressuposto de que a legislação e a prática do país para onde os dados pessoais são transferidos respeitam a essência dos direitos e

liberdades fundamentais das pessoas e não excedem o que é necessário e proporcionado numa sociedade democrática para salvaguardar objetivos de interesse público.

Na prática, ao realizar uma avaliação de impacto de transferência (TIA), a Capgemini deve considerar:

1. As circunstâncias específicas da transferência ou conjunto de transferências e de qualquer transferência subsequente prevista dentro do mesmo país ou para outro país, incluindo:
    - A(s) finalidade(s) para a(s) qual(is) os dados são transferidos e processados posteriormente (por exemplo, RH, suporte de TI, etc.)
    - Os tipos de entidades envolvidas na transferência.
    - O setor econômico do importador e do exportador de dados e no qual a transferência ocorre.
    - A(s) categoria(s) e o formato dos dados pessoais transferidos.
    - O local do tratamento, incluindo armazenamento, e
    - Os canais de transmissão usados.

2. As leis e práticas do país de destino, relevantes à luz das circunstâncias da transferência, incluindo aquelas que exigem a divulgação de dados pessoais às autoridades públicas ou autorizam o acesso por essas autoridades e aquelas que fornecem acesso a esses dados pessoais durante a transferência, bem como as limitações e salvaguardas aplicáveis.

3. Quaisquer salvaguardas contratuais, técnicas ou organizacionais relevantes implementadas para complementar as salvaguardas sob a BCR-C, incluindo medidas aplicadas durante a transmissão e o tratamento de dados pessoais no país de destino.

Quando o TIA revelar que salvaguardas suplementares devem ser implementadas, além daquelas fornecidas pela BCR-C, a(s) Empresa(s) Capgemini do EEE/Brasil que transfere(m) os dados e seu(s) DPO(s) deve(m) ser notificada(s) e envolvida(s) na implementação de tais salvaguardas.

A Capgemini monitorará continuamente as leis e práticas de países terceiros onde as empresas da Capgemini estão estabelecidas e onde os dados pessoais são transferidos de acordo com as BCR-C, para identificar quaisquer alterações que exijam a atualização do(s) TIA(s) e a implementação de salvaguardas suplementares.

Quando uma empresa da Capgemini fora do EEE/Brasil que importa dados pessoais tiver motivos para acreditar que está sujeita a leis e práticas que a impediriam de cumprir suas obrigações sob a BCR-C, ela deverá notificar o escritório de proteção de dados do grupo, para garantir que as salvaguardas adicionais apropriadas sejam implementadas para proteger a(s) transferência(s).

Da mesma forma, quando uma empresa da Capgemini que exporta dados pessoais tiver motivos para acreditar que uma empresa da Capgemini que atua como importadora não pode mais cumprir suas obrigações sob as BCR-C, ela deve notificar o escritório de proteção de dados do grupo para garantir que as salvaguardas adicionais apropriadas sejam implementadas para proteger a(s) transferência(s).

O(s) DPO(s) local(is) competente(s) deve(m) apoiar as empresas da Capgemini que atuam como exportadoras e importadoras na identificação e implementação das medidas suplementares apropriadas para garantir que as transferências de dados estejam em conformidade com as leis locais aplicáveis e estas BCR-C.

Quando uma empresa da Capgemini determinar que as BCR-C não podem mais ser cumpridas – mesmo após a implementação de medidas suplementares – para uma transferência ou conjunto de transferências específico, ou se instruída por uma autoridade supervisora competente a fazê-lo, ela deverá suspender essa transferência ou conjunto de transferências em jogo – bem como todas as transferências para as quais a mesma avaliação e raciocínio levariam a um resultado semelhante – até que a conformidade possa ser alcançada ou A transferência é encerrada. Se o cumprimento das BCR-C não for restabelecido no prazo de um mês a contar da suspensão, a transferência ou conjunto de transferências em causa cessa. Os dados pessoais que foram transferidos antes da suspensão e suas cópias serão devolvidos ou destruídos em sua totalidade à escolha da empresa Capgemini que atua como exportadora de dados.

A Capgemini deve documentar e registrar TIAs – incluindo a natureza das salvaguardas suplementares implementadas para garantir a transferência. Essa documentação deve ser disponibilizada à(s) autoridade(s) fiscalizadora(s) competente(s), mediante pedido.

Na prática, as avaliações das leis e práticas de países terceiros, bem como os TIAs específicos realizados para uma transferência ou conjunto de transferências e as salvaguardas suplementares identificadas e implementadas, bem como toda a documentação relevante – incluindo casos em que medidas suplementares não puderam ser implementadas, devem ser disponibilizadas a todos os DPOs da Capgemini. Assim, permitindo que a Capgemini garanta a conformidade com as BCR-C e a consistência na forma como são implementadas em todo o grupo.

O. Na seção "15. Responsabilidade da Capgemini em caso de violação das BCR-C", a redação passará a vigorar da seguinte forma:

15. Responsabilidade da Capgemini em caso de violação das BCR-C

Cada empresa da Capgemini do EEE/Brasil que exporta dados pessoais para uma empresa da Capgemini fora do EEE/Brasil será responsável, perante os titulares de dados, por quaisquer violações das BCR-C causadas pela empresa da Capgemini fora do EEE/Brasil.

Em todos os outros casos – (1) transferências de uma Capgemini do EEE para outra empresa da Capgemini do EEE, (2) transferências entre duas empresas da Capgemini fora do EEE, (3) transferências de uma empresa da Capgemini fora do EEE para uma empresa da Capgemini do EEE ou (4) transferências de uma Capgemini do Brasil para outra empresa da Capgemini– cada empresa da Capgemini será responsável por uma violação das BCR-C que causou.

Quando uma transferência entre duas empresas da Capgemini fora do EEE/Brasil constituir uma transferência subsequente, a empresa da Capgemini do EEE/Brasil que iniciou a transferência pela primeira vez será responsável perante os titulares de dados, por quaisquer violações da BCR-C causadas por qualquer uma das empresas não pertencentes ao EEE/Brasil.

A lista de empresas da Capgemini é fornecida no Apêndice 1. Os indivíduos podem exercer seus direitos de proteção de dados e/ou enviar uma reclamação por meio do processo dedicado da Capgemini descrito na Seção 7 e no Apêndice 4.

Na prática, isso significa que a empresa Capgemini identificada como responsável de acordo com o esquema acima mencionado deve aceitar a responsabilidade pelo pagamento da indenização e pela reparação da violação quando ela causou um dano a um titular de dados. Os titulares de dados enviam solicitações ou reclamações entrando em contato com o(s) DPO(s) competente(s) por meio do processo dedicado.

Se uma empresa da Capgemini fora do EEE/Brasil violar as BCR-C, os tribunais ou outras autoridades judiciais do EEE/Brasil terão jurisdição e os titulares de dados terão os direitos e recursos contra a empresa responsável da Capgemini do EEE/Brasil (ou seja, a Capgemini do EEE/Brasil que transferiu os dados pessoais para uma empresa da Capgemini fora do EEE/Brasil) como se a violação tivesse sido causada por esta última no Estado-Membro em que está sediada.

Além disso, cabe à Capgemini demonstrar que não violou a BCR-C. No caso de uma transferência entre uma empresa Capgemini do EEE/Brasil e uma empresa Capgemini não pertencente ao EEE/Brasil, se a suposta violação for atribuída à empresa Capgemini não pertencente ao EEE/Brasil, a empresa Capgemini do EEE/Brasil deve demonstrar que a empresa Capgemini não pertencente ao EEE/Brasil não violou realmente as BCR-C.

P. Na seção "19. Atualizações BCR", a redação passará a vigorar da seguinte forma:

19. Atualizações BCR

A Capgemini manterá as BCR-C e o Anexo às Regras Corporativas Vinculantes – Controlador da Capgemini- Aplicação no Brasil atualizados, em particular para refletir quaisquer alterações regulatórias, incluindo recomendações do Conselho Europeu de Proteção de Dados e da Autoridade Nacional de Proteção de Dados (ANPD).

O escritório de proteção de dados do grupo é responsável pela atualização da BCR-C e do Anexo às Regras Corporativas Vinculantes – Controlador da Capgemini- Aplicação no Brasil – incluindo a manutenção da lista de empresas da Capgemini. O escritório de proteção de dados do grupo deve compartilhar qualquer atualização da BCR-C e do o Anexo às Regras Corporativas Vinculantes – Controlador da Capgemini- Aplicação no Brasil com as empresas da Capgemini e seus respectivos DPOs sem atrasos indevidos. Como tal, o escritório de proteção de dados do grupo deve fornecer as informações necessárias aos titulares de dados e/ou às autoridades de supervisão.

Caso a Capgemini faça qualquer alteração substancial nas BCR-C e/ou no Anexo às Regras Corporativas Vinculantes – Controlador da Capgemini- Aplicação no Brasil, ela deverá primeiro entrar em contato com sua principal Autoridade Supervisora Competente, e fornecer uma explicação sobre tais alterações.

Uma vez por ano, a Capgemini comunicará à CNIL e à Autoridade Nacional de Proteção de Dados (ANPD) quaisquer modificações feitas nas BCR-C, incluindo uma lista atualizada de empresas da Capgemini. Essa comunicação deve incluir igualmente uma confirmação relativa aos ativos do grupo.

Lista de entidades vinculadas às Regras Corporativas Vinculativas (BCR-C)

País	Nome / Forma Jurídica	Número de Registro	Endereço Registrado
Argentina	**Capgemini Argentina SA**	1.613.291 Inspeccion General de Justicia	Avenida Presidente Roque Sáenz Peña 615, Piso 2º, Edificio Bencich C1035AAB Buenos Aires Argentina
Australia	**The WorksSydney Pty Ltd**	ACN 102 213 794	Level 10, 420 George Street, Sydney, NSW 2000 Australia
Australia	**Purpose Asia Pacific Pty Ltd**	ACN 625 798 807	Level 10, 420 George Street, Sydney, NSW 2000 Australia
Australia	**Capgemini Australia Pty Ltd**	ACN 092 284 314	Level 10, 420 George Street, Sydney, NSW 2000 Australia
Austria	**Capgemini Consulting Osterreich AG**	FN 194903y Handelsgericht Wien	Millenium Tower Handelskai 94-96, 22. Stock 1200 Wien Austria
Bélgica	**Capgemini Belgium NV/SA**	0407.184.521 Brussels	Hermeslaan 9, 1831 Machelen Belgium
Brasil	**RADI Software Do Brasil Ltda**	11.855.485/0001-11	Rua Alexandre Dumas, No. 1711, 1º Andar, Unidade101, Chácara Santo Antônio, CEP 04717-004, Cidade de São Paulo, Estado de São Paulo, Brasil
Brasil	**Purpose Campaigns Do Brasil Ltda**	35231013042	RUA CUBATAO 472 SAO PAULO - SP Brasil
Brasil	**Capgemini Brasil Ltda**	65.599.953\0001-63	ALAMEDA GRAJAÚ, 60, 14º ANDAR Alphaville, Cidade de Barueri 06454-050 BARUERI, ALPHAVILLE São Paulo Brasil

Canada	**Microsys Technologies Inc**	001909086	3710 Nashua Drive, Suite 1 L4V 1M5 Mississauga Canada
Canada	**Capgemini Solutions Canada Inc.**	860883149NP002	44 Chipman Hill, 10th Floor, P.O. Box 7289 Station "A", E2L 4S6 Saint John New Brunswick Canada
Canada	**Société en Commandite Capgemini Québec - Capgemini Québec LP**	NEZ 3367034736	1100 boul. René-Lévesque Ouest, Suite 1110 H3B 4N4 Montréal Québec Canada
Canada	**Capgemini Canada Inc**	610099	44 Chipman Hill, 10th Floor, P.O. Box 7289 Station "A", E2L 4S6 Saint John New Brunswick Canada
China	**Altran (Beijing) Technologies Company Limited**	91110108078535347A	Room 132008, 17th FL, Building C, Tower 1 of Wangjing SOHO, No. 1 Futong East Road, Chaoyang District 100020 Beijing, China
China	**Altran (Shanghai) Information & Technologies Company Limited**	913101153125083000	The 3rd floor, Building 1, No. 400 Fangchun Road, Pilot Free Trade Zone 201203 Shanghai China
China	**Altran (Xi'an) Technologies Company Limited**	91610131MA6UQKMU7U	5th FL, A11 Building, No.156 Tian Gu 8 Road, Software New Town of Hi-tech Development Zone. Xi'an China
China	**Sicon Design Technologies (Shanghai) Company Limited**	9131011509422053X2	700 Shangfeng Road, Unit 8, Room 301A, Pudong 200120 Shanghai China
China	**Capgemini (Hangzhou) Co Ltd**	330100400004425	15F, Building E,Tiantang Software Park, 3 XiDouMen Road 310012 Hangzhou Zhe Jiang Province China

China	**Capgemini Business Services (China) Limited**	440101400083545	6/F Podium, Glory IFC No. 25 Ronghe Road 528200 Nanhai District, Foshan City China
China	**Capgemini (China) Co Ltd**	310115400049352	Room A256, Floor 2, Building 3, 2250 South Pudong Road, China (Shanghai) Pilot Free Trade Zone China
China	**Capgemini (KunShan) Co Ltd**	320583400050999	NO.1 Jinjie Road, service outsourcing area Huaqiao, Kunshan Jiangsu Province China
China_HK	**Altran China Limited**	876293	Suites 1202-04, Tower 2, The Gateway, 25 Canton Road, TST, Kowloon Hong Kong China
China_HK	**Capgemini Hong Kong Ltd**	536651	Suites 4101-02, 41/F., One Island East, Taikoo Place, 18 Westlands Road, Quarry Bay, Hong Kong, China
Colombia	**Capgemini Colombia SAS**	2197990	Cra 7 No.71 - 72 Torre B Piso 9 Bogota DC Colombia
Costa Rica	**Capgemini Costa Rica SRL (formerly Rivet Logic Costa SRL)**	NUMERO DE CERTIFICACION: RNPDIGITAL-1423520-2022	San José, Escazú, Guachipelín, 400 meters north of Construplaza, Edificio Latitud Norte, 3rd floor, Quatro Legal Office
República Checa	**Capgemini Czech Republic SRO**	260 33 062	5. května 1746/22 CZ-140 00 Praha 4 Czech Republic
Dinamarca	**Capgemini Danmark AS**	25606965	Delta Park 40 2665 Vallensbaeck Strand Denmark
Dinamarca	**Capgemini Services Danmark ApS**	43792067	Delta Park 40 2665 Vallensbaeck Strand

			Denmark
Egito	**Capgemini Egypt LLC**	183227	Plot 202 - Sector 2, Fifth Settlement, New Cairo, Cairo 12477, Egypt
Finlândia	**Capgemini Finland Oy**	1628142-5	Keilaranta 10 E 02150 Espoo Finland
França	**Knowledge Expert SAS**	841 323 736 RCS THONON LES BAINS	77 T Impasse du Clou 74500 Evian les Bains France
França	**Open Cascade SAS**	RCS: 420 919 805 RCS NANTERRE SIRET: 420 919 805 00093	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France
França	**Capgemini Engineering Allemagne SAS [France] (formerly Altran Allemagne)**	519 093 041 RCS PARIS SIRET: 519 093 041 00043	76 avenue Kléber 75016 Paris France
França	**Logiqual SAS**	487 550 683 RCS TOULOUSE SIRET: 487 550 683 00030	4 avenue Didier Daurat 31700 Blagnac France
França	**Capgemini France SAS**	328 781 786 RCS NANTERRE SIRET: 328 781 786 01143	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France
França	**Sogeti SAS**	434 325 973 RCS PARIS SIRET: 434 325 973 00031	11, rue de Tilsitt 75017 PARIS France
França	**Altran Lab SAS**	449 397 561 RCS NANTERRE SIRET: 449 397 561 00043	145-151 Quai du Président Roosevelt 92130 Issy-les-Moulineaux France
França	**Altran Technology & Engineering Center SAS**	817 459 357 RCS TOULOUSE SIRET: 817 459 357 00023	4 avenue Didier Daurat 31700 Blagnac France
França	**Altran Prototypes Automobiles SAS**	487 549 693 RCS NANTERRE SIRET: 487 549 693 00025	145-151 Quai du Président Roosevelt 92130 Issy-les-Moulineaux France
França	**Altran Technologies**	702 012 956 RCS PARIS SIRET Paris:	76 avenue Kléber

	SAS	702 012 956 00935 SIRET Issy: 702 012 956 00943	75016 Paris France
França	**Capgemini Engineering ACT SAS (formerly Altran ACT)**	817 459 209 RCS NANTERRE SIRET: 817 549 203 00026	145-151 Quai du Président Roosevelt 92130 Issy-les-Moulineaux France
França	**Global Management Treasury Services SNC**	448 370 080 RCS PARIS SIRET: 448 370 080 00054	11 rue de Tilsitt 75017 Paris France
França	**Capgemini SE**	330 703 844 RCS PARIS SIRET : 330 703 844 00036	11, rue de Tilsitt 75017 PARIS France
França	**Capgemini Service SAS**	652 025 792 RCS PARIS SIRET: 652 025 792 00084	11, rue de Tilsitt 75017 PARIS France
França	**Capgemini Gouvieux SAS**	428571186 RCS PARIS SIRET: 428571186 00017	11, rue de Tilsitt 75017 PARIS France
França	**Immobilière Les Fontaines SARL**	421 776 311 RCS PARIS SIRET: 421 776 311 00019	11, rue de Tilsitt 75017 PARIS France
França	**SCI Paris Etoile**	331 338 558 R.C.S PARIS SIRET: 331 338 558 00033	11, rue de Tilsitt 75017 PARIS France
França	**Capgemini Latin America SAS**	487 606 782 RCS PARIS SIRET: 487 606 782 00018	11, rue de Tilsitt 75017 PARIS France
França	**Capgemini Ventures SAS**	440 330 090 RCS PARIS SIRET: 440 330 090 00018	11, rue de Tilsitt 75017 PARIS France
França	**Capgemini Technology Services SAS**	479 766 842 RCS NANTERRE SIRET: 479 766 842 00724	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France
França	**Capgemini Consulting SAS**	479766800 RCS NANTERRE SIRET: 479 766 800 00060	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France
França	**Capgemini Engineering Research and**	444495774 RCS NANTERRE SIRET:	145-151 Quai du Président Roosevelt 92130 ISSY- LES-

	Development SAS	444 495 774 00531	MOULINEAUX France
Alemanha	**Capgemini Engineering Deutschland SAS & Co KG (formerly Altran Deutschland SAS & Co KG)**	HRA 100894	81 Frankfurter Ring 80807 München Germany
Alemanha	**Capgemini Deutschland Holding Gmbh**	HRB 102576 Amtsgericht Berlin-Charlotttenburg	Potsdamer Platz 5 10785 Berlin Germany
Alemanha	**Capgemini Deutschland Services Gmbh**	HRB 215542 B Amtsgericht Berlin-Charlottenburg	Potsdamer Platz 5 10785 Berlin Germany
Alemanha	**Capgemini Engineering Service GmbH (formerly Altran Service GmbH)**	HRA 89337	81 Frankfurter Ring 80807 München Germany
Alemanha	**XL2 Gmbh**	HRB 773865 Amtsgericht Stuttgart	Potsdamer Platz 5 10785 Berlin Germany
Alemanha	**Capgemini Deutschland Gmbh**	HRB 98814 Amtsgericht Berlin-Charlottenburg	Potsdamer Platz 5 10785 Berlin Germany
Alemanha	**Capgemini Outsourcing Services Gmbh**	HRB 58881 Amtsgericht Düsseldorf	Balcke-Dürr-Allee 7 40882 Ratingen Germany
Grécia	**HDL Design House Greece Private Company**	N° 134685604000	1, Plateia Dimokratias, Thessaloniki, 54629 (floor 6, office no. 610) Greece
Guatemala	**Capgemini Business Services Guatemala SA**	Company Patent - No.77886 Folio 548 Book 171 of Companies	15, avenida 5-00 Zona 13 Edifico World Technology Center Torre Sur Nivel 11 Ciudad de Guatemala Guatemala
Hungria	**Restaurant Application Development International Hungary**	Tax number: 23528480-2-09 EU tax number: HU23528480 Company registration number: 09-09-	028 Debrecen, Tüzér utca 4. A. ép. 2. em., Magyarország / H-4028 Debrecen, Tüzér Street 4. A building 2nd floor,

		035337	Hungary
Hungria	**Capgemini Magyarorszag Kft**	13-09-087168 Pest County Registry Court	Rétköz utca 5 HU-1118 Budapest Hungary
India	**Capgemini IT Solutions India Pte Ltd**	CIN No. U74995MH2018FTC330429	5th Floor Part A, Block IV, Plot IT-3 IT-4, Airoli Knowledge Park, TTC Industrial Area, MIDC, Airoli, 400708 Navi Mumbai, Maharashtra, India
India	**Leading Purpose Campaigns (India) Pte Ltd**	U74999DL2018FTC329926	FIRST FLOOR D-3 SOAMI NAGAR 110017 DELHI NEW DELHI India
India	**Capgemini Technology Services India Limited**	U85110PN1993PLC145950	No. 14, Rajiv Gandhi Infotech Park Hinjewadi Phase-III, MIDC-SEZ, Village Man, Taluka Mulshi, 411057 PUNE, Maharashtra India
Irlanda	**Capgemini Ireland Ltd**	67792	Ground Floor, Metropolitan Building, James Joyce Street, Dublin 1 Ireland
Israel	**Altran Israel Limited**	514792282	7 Rival Street 6777840 Tel-Aviv-Yafo Israel
Itália	**Knowledge Expert SRL**	6988270820	Via Mariano Stabile 160 90139 Palermo Italy
Itália	**Capgemini Italia SPA**	4877961005	Via di Torre Spaccata, 140 00173 Roma Italy
Itália	**Capgemini Finance Tech SRL**	16239151000	Via di Torre Spaccata, 140 00173 Roma Italy
Japão	**Cambridge Consultants Japan Incorporated**	9-0104-01-126095	6F Spline Aoyama Tokyu Building, 3-1-3 Minamiaoyama, Minato-ku, 107-0062 Tokyo Japan
Japão	**Capgemini Japan**	0104-02-035069	Toranomon Hills Mori

	KK		Tower, 1-23-1 Toranomon, Minato-ku, Tokyo
Japão	**BTC Corporation [Japan]**	0100－01－193831	Mita 43MT Bld, 3-13-16 Mita, Minato-ku, Tokyo
Luxemburgo	**Capgemini Reinsurance International SA**	163.854 RCS Luxemburg	534 rue de Neudorf 2220 Luxembourg Grand-Duché de Luxembourg
Luxemburgo	**Sogeti Luxembourg SA**	B42610	36 Route de Longwy 8080 Bertrange Grand-Duché de Luxembourg
Malásia	**Capgemini Services Malaysia Sdn Bhd**	201101031070 (959205-M)	Suite 15-01,G Tower, 199 Jalan Tun Razak 50400 Kuala Lumpur Malaysia
México	**Capgemini Mexico S De RL De CV**	219759	Av. Santa Fe No. 428, Torre 3, Piso 15, Colonia Santa Fe Cuajimalpa, Alcaldía Cuajimalpa, Ciudad de México, 05348 Mexico
Marrocos	**Altran Maroc SARLU**	IF N°14457667 RC N°289225	1100 boulevard Al Qods, Casanearshore, Shore 17, Quartier Sidi Mâarouf 20270 Casablanca Morocco
Marrocos	**MG2 Engineering SA**	IF N° 26143419 RC N°412549	1100 boulevard Al Qods, Casanearshore, Shore 12, Quartier Sidi Mâarouf 20270 Casablanca Morocco
Marrocos	**Capgemini Technology Services Maroc SA**	164141	Shore 8 - A - Casanearshore 1100, Boulevard Al Qods - Sidi Maarouf Casablanca Morocco
Nova Zelândia	**Capgemini New Zealand Ltd**	1128855	Level 4, 80 Willis Street Wellington, 6011 New Zealand

Noruega	**Capgemini Norge AS**	943 574 537	Karenslyst Allé 20 0278 Oslo Norway
Noruega	**Matiq AS**	985 149 437	Abels gate 7 7030 TRONDHEIM Norway
Filipinas	**Whitesky Labs (Philippines) Inc**	CS201410583 Metro Manila, Philippines	3304 ROBINSONS EQUITABLE BUILDING 4 ADB AVENUE ORTIGAS MANILA Philippines
Filipinas	**Capgemini Digital Services Philippines Corp**	CS201405679	7th Floor, Tower 2 Insular Life Corporate Centre, Insular Life Drive, Filinvest Corporate City, Alabang, 1781 Muntinlupa City, Philippines
Filipinas	**Capgemini Philippines Corp**	CS200714668	12 Floor, 10 West Campus, McKinely West, Fort Bonifacio, Taguig City, Philippines
Polônia	**Capgemini Polska SP Zoo**	KRS 0000040605 District Court for Warsaw, XIIth Commercial Division of the National Court Register	Ul. Żwirki i Wigury 16a 02-092 Warsaw Poland
Portugal	**Capgemini Portugal SA**	504272179	Av. Colégio Militar, Torre Colombo, Piso 10 Lisboa Portugal
Roménia	**Capgemini Services Romania SRL**	J40/22612/2007 Bucharest Trade Registry	Gara Herastrau Street, no. 4D Green Court building, 4th floor Bucharest, Sector 2 Romania
Arábia Saudita	**Capgemini Saudi Ltd**	1024341133776	Centria Mall Office Tower, Suite 506, 5th floor, Prince Muhammad ibn Abdulaziz Road / Olaya Street, Al Olaya District, 12241-6055 Riyadh Kingdom of Saudi Arabia

Servia	**PRIVREDNO DRUŠTVO HDL DESIGN HOUSE ZA INŽENJERING I KONSALTING EXPORT-IMPORT DRUŠTVO SA OGRANIČENOM ODGOVORNOŠĆU BEOGRAD (VRAČAR) [Serbia]**	17376667	Golsvortijeva 35, Beograd, Serbia
Singapura	**Altran (Singapore) Pte Ltd**	200106758M	4 Battery Road, #25-01 Bank of China Building 049908 Singapore Singapore
Singapura	**Liquidhub Pte Ltd**	Registration Number : 201703318C	12 Marina Boulevard # 32 - 02 Marina Bay Financial Centre 018982 Singapore
Singapura	**Cambridge Consultants (Singapore), Private Limited**	201230536C	4 Battery Road, #25-01 Bank of China Building 049908 Singapore Singapore
Singapura	**Capgemini Asia Pacific Pte Ltd**	199602754G	12 Marina Boulevard # 32 - 02 Marina Bay Financial Centre 018982 Singapore
Singapura	**Capgemini Singapore Pte Ltd**	199106419N	12 Marina Boulevard # 32 - 02 Marina Bay Financial Centre 018982 Singapore
Eslováquia	**Altran Slovakia SRO**	46655956	Piešťanská 3 917 01 Trnava Slovakia
Espanha	**Ecosat Airships SL**	B-47794425	Calle Nicostrato Vela, 20 24009 León Spain
Espanha	**ACIE Agencia de Certification Espanola SLU**	B-82271313	En calle Campezo 1, edificio 4, planta 0 28022 Madrid Spain
Espanha	**Capgemini Espana SL**	Tomo 27.544; Folio 54; Hoja M-287781 Registro Mercantil de Madrid	Calle Puerto de Somport, Edificio Oxxeo, CP 28050 Madrid Spain
Sweden	**Capgemini Engineering Sverige AB (formerly Altran**	556542-2531	37 Södra Hamngatan SE 411 06 Göteborg

	Sverige)		Sweden
Suécia	**Sogeti Sverige AB**	556631-4687 Stockholm	Svetsarvägen 4 171 41 Solna Sweden
Suécia	**Capgemini AB**	556447-9763 Stockholm	Flemingatan 18, 112 26 Stockholm Sweden
Suécia	**Capgemini Sverige AB**	556092-3053 Stockholm	Flemingatan 18, 112 26 Stockholm Sweden
Suíça	**Knowledge Expert SA**	CHE-114.807.854	9 rue de la Gabelle 1227 Carouges (GE) Switzerland
Suíça	**Capgemini Suisse SA**	CHE-106.108.52 Handelsregister des Kantons Zürich	World Trade Center Leutschenbachstrass e 95 8050 Zurich Switzerland
Países Baixos	**Capgemini Semiconnext Platform BV**	865742030	"Reykjavikplein 1 3543 KA Utrecht The Netherlands "
Países Baixos	**Altran Netherlands BV**	34106539	1Reykjavikplein 3543KA Utrecht The Netherlands
Países Baixos	**Altran International BV**	33294562	1 Reykjavikplein 3543KA Utrecht The Netherlands
Países Baixos	**Sogeti Nederland BV**	30200252 Kamer van Koophandel Midden-Nederland (Utrecht)	Lange Dreef 17 4131 NJ Vianen The Netherlands
Países Baixos	**Capgemini NV**	30067608 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
Países Baixos	**Capgemini Business Services BV**	33030578 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
Países Baixos	**Knowledge Expert BV**	85051232	Lange Viestraat 2B 3511 BK Utrecht The Netherlands
Países Baixos	**Capgemini International BV**	33268283 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
Países Baixos	**Capgemini Nederland BV**	30053172 Utrecht	Reykjavikplein 1 3543 KA Utrecht The

			Netherlands
Países Baixos	**Capgemini Sourcing BV**	30135992 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
Países Baixos	**Capgemini Educational Services BV**	30197497 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
Tunísia	**Altran Telnet Corporation SA**	Identifiant unique 1062046P Ancien numéro d'enregistrement B2455592008 (à noter : Selon la nouvelle loi relative au registre national des entreprises, le matricule fiscal sera l'identifiant unique annulant et remplaçant ainsi le numéro d'immatriculation au registre de commerce.)	Centre urbain Nord, Immeuble Ennour 1082 Tunis El Mahrajène Tunisia
Tunísia	**KE Tunisie SARL**	Identifiant unique 1760466T Ancien numéro d'enregistrement C0182112022 (à noter : Selon la nouvelle loi relative au registre national des entreprises, le matricule fiscal sera l'identifiant unique annulant et remplaçant ainsi le numéro d'immatriculation au registre de commerce.)	Rue du Lac Lochness, Immeuble Fajr, RDC, 1053 Les Berges du Lac, Tunis Tunisia
Emirados Árabes Unidos	**Altran Middle East FZ-LLC**	17595	1803-1804 Al Thuraya Tower 1, PO Box 502709 Dubai Media City United Arab Emirates
Reino Unido	**Quorsus Limited**	11521293	1 Forge End GU21

			6DB Woking United Kingdom
Reino Unido	**Altran UK Holding Ltd**	03066512	1 Forge End GU21 6DB Woking United Kingdom
Reino Unido	**Information Risk Management Ltd**	03612719	1 Forge End GU21 6DB Woking United Kingdom
Reino Unido	**23RED Ltd**	3974936	1 Forge End GU21 6DB Woking United Kingdom
Reino Unido	**Cambridge Consultants Ltd**	01036298	Milton Road, Science Park - Unit 29 CB4 0DW Cambridge United Kingdom
Reino Unido	**Purpose Europe Ltd**	8340026	Raleigh House 14C Compass Point Business PK Stocks Bridge Way PE27 5JL ST Ives, Cambridgeshire, United Kingdom
Reino Unido	**CGS Holdings Ltd**	02798276 England & Wales	No. 1 Forge End, Woking GU21 6DB, Surrey United Kingdom
Reino Unido	**Capgemini UK PLC**	943935 England & Wales	No. 1 Forge End, Woking GU21 6DB, Surrey United Kingdom
Ucrânia	**Lohika LTD, LLC**	37413934	50 Prakhovykh Simi Str. 01033 Kyiv Ukraine
Estados Unidos	**Annik Inc**	Registration Number in Florida : P07000081250	Corporation Service Company 1201 Hays Street 32301 Tallahassee, County of Leon, Florida United States of America
Estados Unidos	**VariQ Corporation**	Employer identification number (EIN) / Tax Identification Number : 13-4269151	Corporation service company 112 North Curry street Carson city, NV 89703 United

		(Nevada)	States of America
Estados Unidos	**Altran Engineering Solutions Inc**	800653319	40600 Ann Arbor Road E, Suite 201 MI 48170-4675 Plymouth USA
Estados Unidos	**Cambridge Consultants Inc**	000867390	745 Atlantic Ave. 6th floor MA 02111 Boston USA Email Eve 28.09.22 : 2 Drydock Avenue Suite 1210 Boston, MA 02210
Estados Unidos	**Capgemini VariQ JV LLC**	11267185	Corporation Service Company 100 Shockoe Slip, 2nd Floor Richmond, VA 23219 United States of America
Estados Unidos	**Purpose Global PBC**	5045539	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
Estados Unidos	**Purpose Campaigns LLC**	3971119	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
Estados Unidos	**Capgemini North America Inc**	Registration number in Delaware: 3509818	c/o Corporation Service Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
Estados Unidos	**Capgemini America Inc**	Registration Number in NewJersey: 0100245598	c/o Corporation Service Company Priceton South Corporate Ctr., Ste. 160, 100 Charles Ewing Blvd., 08628 Ewing, New Jersey United States of America
Estados Unidos	**Capgemini**	Registration Number	c/o Corporation

	Government Solutions LLC	in Delaware: 3584244	Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
Estados Unidos	**Capgemini Technologies LLC**	Registration number in Delaware- 3529062	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
Estados Unidos	**Capgemini Business Services USA LLC**	Registration Number in Delaware: 5010627	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
Vietnã	**Capgemini Services Vietnam Limited Liability Company (formerly Aodigy Vietnam Limited Liability Company)**	401966898	150-156 Nguyen Van Linh, Vinh Trung Ward, Thanh Khe District, Da Nang City, Vietnam
Vietnã	**Capgemini Vietnam Co Ltd**	411043001695	Centre Point Building, 106 Nguyen Van Troi, Ward 8, Phu Nhuan District, Ho Chi Minh City Vietnam
Vietnã	**Công Ty THNN Bigtree Technology & Consulting Vietnam**	107650321	Floor 7, No. 444 Hoang Hoa Tham, Thuy Khue Ward, Tay Ho District, Hanoi, Vietnam
Tailândia	**Capgemini Services (Thailand) Co Ltd**	N° 105557076173	8 Wework, T-One Building, 20th Floor, Soi Sukhumvit 40, Sukhumvit Road, Khlong Toei District, Phra Khanong Sub-District, Bangkok THAILAND

Apêndice 3 – Atividades de processamento da Capgemini e principais transferências

A tabela copiada abaixo descreve as principais atividades de processamento de dados realizadas pela Capgemini e cobertas pelas BCR, nas quais a Capgemini atua como controladora de dados.
A lista abaixo pretende ser o mais completa possível, mas não deve ser interpretada como exaustiva e será atualizada sempre que necessário.

Propósito	Categorias de dados	Titulares dos dados	Base legal	Países para onde os dados são transferidos
Recrutamento, incluindo verificações de antecedentes sujeitas à lei aplicável	▪ **Detalhes de contato**, como nome, data de nascimento, sexo, idade, endereço, números de telefone, endereço de e-mail, número de filhos, cidadania, detalhes de identidade, detalhes de visto, detalhes de permissão de trabalho, detalhes de contato de emergência, detalhes de dependentes, estado civil, beneficiários de seguro de vida, fotos ou imagens; ▪ **Informações financeiras** relacionadas a remuneração, benefícios e acordos de pensão, como detalhes de salário, conta bancária, códigos fiscais, despesas de viagem, opções de ações, plano de compra de ações;	Candidatos	**Art. 7º, inciso V** – execução de contrato ou procedimentos preliminares relacionados a contrato do qual seja parte o titular	Países em que a Capgemini está estabelecida

	▪ **Informações de recrutamento**, como currículo, formulário de inscrição, notas de entrevistas, referências de candidatos (se registradas), qualificações, resultados de testes (se aplicável); ▪ **Informações sobre a experiência profissional**, como currículo profissional, qualificações, detalhes dos projetos em que os funcionários trabalharam, registros de treinamento, registros de mobilidade; ▪ **Fotos**			
Avaliação de desempenho e treinamento	▪ **Detalhes de contato**, como nome, data de nascimento, sexo, idade, endereço, números de telefone, endereço de e-mail, número de filhos, cidadania, detalhes de identidade, detalhes de visto, detalhes de permissão de trabalho, detalhes de contato de emergência, detalhes de dependentes, estado civil, beneficiários de seguro de vida, fotos ou imagens; ▪ **Informações de treinamento**; ▪ **Avaliação de desempenho** , incluindo avaliação de final de ano	Empregados	**Art. 7º, inciso V** – execução de contrato; **Art. 7º, inciso IX** – legítimo interesse	Países em que a Capgemini está estabelecida
Folha de pagamento e administração de outros benefícios relacionados ao emprego (incluindo opções de ações, plano	▪ **Detalhes de contato**, como nome, data de nascimento, sexo, idade, endereço, números de telefone, endereço de e-mail, número de filhos, cidadania, detalhes de identidade, detalhes de visto, detalhes de	Empregados Consultores terceirizados	**Art. 7º, inciso II** – cumprimento de obrigação legal ou regulatória;	Países em que a Capgemini está estabelecida

de compra de ações ou outros planos ou benefícios corporativos)	permissão de trabalho, detalhes de contato de emergência, detalhes de dependentes, estado civil, beneficiários de seguro de vida, fotos ou imagens; ▪ **Informações financeiras** relacionadas a remuneração, benefícios e acordos de pensão, como detalhes de salário, conta bancária, códigos fiscais, despesas de viagem, opções de ações, plano de compra de ações; ▪ **Informações de administração de emprego**, como histórico de emprego e carreira, notas, gerentes, detalhes do contrato de trabalho, registros de ausência, registros de segurança, registros de saúde e doença, relatórios de acidentes, avaliações de desenvolvimento pessoal, detalhes da carteira de motorista e documentos associados, registros de habilidades, números de identificação emitidos pelo governo		**Art. 7º, inciso V** – execução de contrato	
Atividades de gerenciamento do dia-a-dia, como implantação de pessoal em projetos, promoção, atividades disciplinares, tratamento de procedimentos de reclamação	▪ **Detalhes de contato**, como nome, data de nascimento, sexo, idade, endereço, números de telefone, endereço de e-mail, número de filhos, cidadania, detalhes de identidade, detalhes de visto, detalhes de permissão de trabalho, detalhes de contato de emergência, detalhes de dependentes, estado civil, beneficiários de seguro de vida, fotos ou imagens;	Empregados	**Art. 7º, inciso V** – execução de contrato; **Art. 7º, inciso IX** – legítimo interesse	Qualquer país onde a Capgemini esteja estabelecida

	▪ **Informações de administração de emprego**, como histórico de emprego e carreira, notas, gerentes, detalhes do contrato de trabalho, registros de ausência, registros de segurança, registros de saúde e doença, relatórios de acidentes, avaliações de desenvolvimento pessoal, detalhes da carteira de motorista e documentos associados, registros de habilidades, números de identificação emitidos pelo governo; ▪ **Informações sobre a experiência profissional**, como currículo profissional, qualificações, detalhes dos projetos em que os funcionários trabalharam, registros de treinamento, registros de mobilidade; ▪ **Detalhes do paradeiro dos funcionários** na Capgemini na medida em que registrado pelos sistemas de acesso ao cartão eletrônico da Capgemini; ▪ **Detalhes de TI e dados de conexão** com os sistemas de TI da Capgemini			
Comercializar os serviços profissionais de consultores para potenciais clientes da Capgemini (por exemplo, fornecendo detalhes da experiência em projetos anteriores)	▪ **Detalhes de contato**, como nome, data de nascimento, sexo, idade, endereço, números de telefone, endereço de e-mail, número de filhos, cidadania, detalhes de identidade, detalhes de visto, detalhes de permissão de trabalho, detalhes de contato de emergência, detalhes de dependentes, estado civil, beneficiários de seguro de vida, fotos	FuncionáriosConsultores	**Art. 7º, inciso IX** – legítimo interesse	Em todos os países em que a Capgemini está estabelecida

	ou imagens; ▪ **Informações de recrutamento**, como currículo, formulário de inscrição, notas de entrevistas, referências de candidatos (se registradas), qualificações, resultados de testes (se aplicável); ▪ **Informações de administração de emprego**, como histórico de emprego e carreira, notas, gerentes, detalhes do contrato de trabalho, registros de ausência, registros de segurança, registros de saúde e doença, relatórios de acidentes, avaliações de desenvolvimento pessoal, detalhes da carteira de motorista e documentos associados, registros de habilidades, números de identificação emitidos pelo governo; ▪ **Informações sobre a experiência profissional**, como currículo profissional, qualificações, detalhes dos projetos em que os funcionários trabalharam, registros de treinamento, registros de mobilidade; ▪ **Fotos.**			
Administração dos benefícios atuais, incluindo o plano de previdência pessoal Capgemini, plano de seguro de vida, plano de seguro de saúde privado	▪ **Detalhes de contato**, como nome, data de nascimento, sexo, idade, endereço, números de telefone, endereço de e-mail, número de filhos, cidadania, detalhes de identidade, detalhes de visto, detalhes de permissão de trabalho, detalhes de contato de emergência, detalhes de	Empregados	**Art. 7º, inciso II** – obrigação legal; **Art. 7º, inciso V** – execução de contrato	Países em que a Capgemini está estabelecida

	dependentes, estado civil, beneficiários de seguro de vida, fotos ou imagens; ▪ **Informações financeiras** relacionadas a remuneração, benefícios e acordos de pensão, como detalhes de salário, conta bancária, códigos fiscais, despesas de viagem, opções de ações, plano de compra de ações; ▪ **Informações de administração de emprego**, como histórico de emprego e carreira, notas, gerentes, detalhes do contrato de trabalho, registros de ausência, registros de segurança, registros de saúde e doença, relatórios de acidentes, avaliações de desenvolvimento pessoal, detalhes da carteira de motorista e documentos associados, registros de habilidades, números de identificação emitidos pelo governo			
Análise de emprego, por exemplo, comparando o sucesso de vários programas de recrutamento e/ou retenção de funcionários	▪ **Informações de recrutamento**, como currículo, formulário de inscrição, notas de entrevistas, referências de candidatos (se registradas), qualificações, resultados de testes (se aplicável);	Empregados Candidatos	**Art. 7º, inciso IX** – legítimo interesse	Índia

	▪ **Informações de administração de emprego**, como histórico de emprego e carreira, notas, gerentes, detalhes do contrato de trabalho, registros de ausência, registros de segurança, registros de saúde e doença, relatórios de acidentes, avaliações de desenvolvimento pessoal, detalhes da carteira de motorista e documentos associados, registros de habilidades, números de identificação emitidos pelo governo; ▪ **Informações sobre a experiência profissional**, como currículo profissional, qualificações, detalhes dos projetos em que os funcionários trabalharam, registros de treinamento, registros de mobilidade			
Conformidade com as regras de saúde e segurança e outras obrigações legais impostas à Capgemini como empregadora	▪ **Detalhes de contato**, como nome, data de nascimento, sexo, idade, endereço, números de telefone, endereço de e-mail, número de filhos, cidadania, detalhes de identidade, detalhes de visto, detalhes de permissão de trabalho, detalhes de contato de emergência, detalhes de dependentes, estado civil, beneficiários de seguro de vida, fotos ou imagens;	Empregados	**Art. 7º, inciso II** – cumprimento de obrigação legal	Países em que a Capgemini está estabelecida

	▪ **Informações de administração de emprego**, como histórico de emprego e carreira, notas, gerentes, detalhes do contrato de trabalho, registros de ausência, registros de segurança, registros de saúde e doença, relatórios de acidentes, avaliações de desenvolvimento pessoal, detalhes da carteira de motorista e documentos associados, registros de habilidades, números de identificação emitidos pelo governo; ▪ **Informações sobre a experiência profissional**, como currículo profissional, qualificações, detalhes dos projetos em que os funcionários trabalharam, registros de treinamento, registros de mobilidade.			
Quando necessário, o processamento projetado para permitir que a Capgemini exerça seus direitos legais e/ou cumpra suas obrigações legais como empregador, na medida em que seja exigido pela Lei Aplicável do país onde a empresa Capgemini responsável pelos Dados Pessoais está estabelecida	▪ **Detalhes de contato**, como nome, data de nascimento, sexo, idade, endereço, números de telefone, endereço de e-mail, número de filhos, cidadania, detalhes de identidade, detalhes de visto, detalhes de permissão de trabalho, detalhes de contato de emergência, detalhes de dependentes, estado civil, beneficiários de seguro de vida, fotos ou imagens; ▪ **Informações financeiras** relacionadas a remuneração, benefícios e acordos de pensão, como detalhes de salário, conta bancária, códigos fiscais, despesas de viagem, opções de ações, plano de compra de ações;	Empregados Consultores	**Art. 7º, inciso II** – obrigação legal; **Art. 7º, inciso VI** – exercício regular de direitos	Países em que a Capgemini está estabelecida

	▪ **Informações de recrutamento**, como currículo, formulário de inscrição, notas de entrevistas, referências de candidatos (se registradas), qualificações, resultados de testes (se aplicável); ▪ **Informações de administração de emprego**, como histórico de emprego e carreira, notas, gerentes, detalhes do contrato de trabalho, registros de ausência, registros de segurança, registros de saúde e doença, relatórios de acidentes, avaliações de desenvolvimento pessoal, detalhes da carteira de motorista e documentos associados, registros de habilidades, números de identificação emitidos pelo governo; ▪ **Informações sobre a experiência profissional**, como currículo profissional, qualificações, detalhes dos projetos em que os funcionários trabalharam, registros de treinamento, registros de mobilidade; ▪ **Detalhes do paradeiro dos funcionários** na Capgemini na medida em que registrado pelos sistemas de acesso ao cartão eletrônico da Capgemini; ▪ **Detalhes de TI e dados de conexão** com os sistemas de TI da Capgemini.			
Gestão de Recursos Humanos, Gestão de Carreira e Mobilidade	▪ **Detalhes de contato**, como nome, data de nascimento, sexo, idade, endereço, números de telefone, endereço de e-mail, número de filhos, cidadania, detalhes de identidade,	Empregados Candidatos	**Art. 7º, inciso V** – execução de contrato; **Art. 7º, inciso**	Países em que a Capgemini está estabelecida

	detalhes de visto, detalhes de permissão de trabalho, detalhes de contato de emergência, detalhes de dependentes, estado civil, beneficiários de seguro de vida, fotos ou imagens; ▪ **Informações financeiras** relacionadas a remuneração, benefícios e acordos de pensão, como detalhes de salário, conta bancária, códigos fiscais, despesas de viagem, opções de ações, plano de compra de ações; ▪ **Informações de recrutamento**, como currículo, formulário de inscrição, notas de entrevistas, referências de candidatos (se registradas), qualificações, resultados de testes (se aplicável); ▪ **Informações de administração de emprego**, como histórico de emprego e carreira, notas, gerentes, detalhes do contrato de trabalho, registros de ausência, registros de segurança, registros de saúde e doença, relatórios de acidentes, avaliações de desenvolvimento pessoal, detalhes da carteira de motorista e documentos associados, registros de habilidades, números de identificação emitidos pelo governo; ▪ **Informações sobre a experiência profissional**, como currículo profissional, qualificações, detalhes dos projetos em que os funcionários trabalharam, registros de treinamento, registros de mobilidade		**IX** – legítimo interesse	

Comunicação interna e externa	▪ **Detalhes de contato**, como nome, endereço, números de telefone, endereço de e-mail; ▪ **Fotos**	Empregados	**Art. 7º, inciso IX** – legítimo interesse	Países em que a Capgemini está estabelecida
Plano de recuperação de desastres e gerenciamento de crises	▪ **Detalhes de contato**, como nome, data de nascimento, sexo, idade, endereço, números de telefone, endereço de e-mail, número de filhos, cidadania, detalhes de identidade, detalhes de visto, detalhes de permissão de trabalho, detalhes de contato de emergência, detalhes de dependentes, estado civil, beneficiários de seguro de vida, fotos ou imagens; ▪ **Informações de administração de emprego**, como histórico de emprego e carreira, notas, gerentes, detalhes do contrato de trabalho, registros de ausência, registros de segurança, registros de saúde e doença, relatórios de acidentes, avaliações de desenvolvimento pessoal, detalhes da carteira de motorista e documentos associados, registros de habilidades, números de identificação emitidos pelo governo; ▪ **Detalhes do paradeiro dos funcionários** na Capgemini na medida em que registrado pelos sistemas de acesso ao cartão eletrônico da Capgemini; ▪ **Detalhes de TI e dados de conexão** com os sistemas de TI da Capgemini; ▪ **Fotos.**	Empregados Familiares dos colaboradores	**Art. 7º, inciso II** – obrigação legal; **Art. 7º, inciso IX** – legítimo interesse	Países em que a Capgemini está estabelecida
Auditoria e estatísticas	▪ **Detalhes de contato**, como nome, data de nascimento, sexo, idade,	Empregados	**Art. 7º, inciso IX** – legítimo	Índia

	endereço, números de telefone, endereço de e-mail, número de filhos, cidadania, detalhes de identidade, detalhes de visto, detalhes de permissão de trabalho, detalhes de contato de emergência, detalhes de dependentes, estado civil, beneficiários de seguro de vida, fotos ou imagens; ▪ **Informações financeiras** relacionadas a remuneração, benefícios e acordos de pensão, como detalhes de salário, conta bancária, códigos fiscais, despesas de viagem, opções de ações, plano de compra de ações; ▪ **Informações de recrutamento**, como currículo, formulário de inscrição, notas de entrevistas, referências de candidatos (se registradas), qualificações, resultados de testes (se aplicável); ▪ **Informações de administração de emprego**, como histórico de emprego e carreira, notas, gerentes, detalhes do contrato de trabalho, registros de ausência, registros de segurança, registros de saúde e doença, relatórios de acidentes, avaliações de desenvolvimento pessoal, detalhes da carteira de motorista e documentos associados, registros de habilidades, números de identificação emitidos pelo governo;	Candidatos Detalhes de contato do cliente Detalhes de contato dos fornecedores	interesse	

	▪ **Informações sobre a experiência profissional**, como currículo profissional, qualificações, detalhes dos projetos em que os funcionários trabalharam, registros de treinamento, registros de mobilidade; ▪ **Detalhes do paradeiro dos funcionários** na Capgemini na medida em que registrado pelos sistemas de acesso ao cartão eletrônico da Capgemini; ▪ **Detalhes de TI e dados de conexão** com os sistemas de TI da Capgemini			
Gestão de fornecedores terceirizados	▪ **Detalhes de contato**, como nome, endereço, números de telefone, endereço de e-mail	Empregados Funcionários de terceiros	**Art. 7º, inciso V** – execução de contrato; **Art. 7º, inciso IX** – legítimo interesse	Países em que a Capgemini está estabelecida
Prevenção de vazamentos	▪ **Detalhes de contato**, como nome, endereço, números de telefone, endereço de e-mail; ▪ **Detalhes de TI e dados de conexão** com os sistemas de TI da Capgemini	Empregados	**Art. 7º, inciso IX** – legítimo interesse	Países em que a Capgemini está estabelecida
Verificar o tráfego de rede em busca de atividades maliciosas	▪ **Detalhes de TI e dados de conexão** com os sistemas de TI da Capgemini	Empregados	**Art. 7º, inciso IX** – legítimo interesse	Países em que a Capgemini está estabelecida
Sistemas de Proteção, Rede, **Infraestrutura e Computadores**	▪ **Detalhes de contato**, como nome, endereço, números de telefone, endereço de e-mail;	Empregados	**Art. 7º, inciso IX** – legítimo interesse	Países em que a Capgemini está estabelecida

	▪ **Detalhes de TI e dados de conexão** com os sistemas de TI da Capgemini			
Gerenciamento de acesso de identidade	▪ **Detalhes de contato,** como nome, endereço, números de telefone, endereço de e-mail; ▪ **Detalhes de TI e dados de conexão** com os sistemas de TI da Capgemini	Empregados	**Art. 7º, inciso IX** – legítimo interesse	Países em que a Capgemini está estabelecida
Gerenciamento de programas BYOD	▪ **Detalhes de contato,** como nome, endereço, números de telefone, endereço de e-mail; ▪ **Informações de administração de emprego**, como histórico de emprego e carreira, notas, gerentes, detalhes do contrato de trabalho, registros de ausência, registros de segurança, registros de saúde e doença, relatórios de acidentes, avaliações de desenvolvimento pessoal, detalhes da carteira de motorista e documentos associados, registros de habilidades, números de identificação emitidos pelo governo; ▪ **Detalhes de TI e dados de conexão** com os sistemas de TI da Capgemini	Empregados	**Art. 7º, inciso V** – execução de contrato; **Art. 7º, inciso IX** – legítimo interesse	Países em que a Capgemini está estabelecida
Gerenciamento de incidentes e eventos **(Registro, correção, correção, etc.)**	▪ **Detalhes de contato,** como nome, endereço, números de telefone, endereço de e-mail; ▪ **Detalhes de TI e dados de conexão** com os sistemas de TI da Capgemini	Empregados	**Art. 7º, inciso IX** – legítimo interesse	Países em que a Capgemini está estabelecida
Investigação Forense	▪ **Detalhes de contato,** como nome, endereço, números de telefone, endereço de e-mail;	Empregados	**Art. 7º, inciso VI** – exercício regular de direitos; **Art.**	Países em que a Capgemini está estabelecida

	▪ **Detalhes de TI e dados de conexão** com os sistemas de TI da Capgemini		**7º, inciso IX** – legítimo interesse	

Organização de Proteção de Dados

Membro do Comitê Executivo do Grupo
Conselheiro Geral do Grupo e Gestão Comercial & Contratual

Vice-Presidente, Chefe de Proteção de Dados e Assuntos Regulatórios

Responsável pelos Riscos e Controles de Privacidade do Grupo – Consultor Jurídico Sênior

Responsável pelas Políticas de Privacidade e Assuntos Regulatórios do Grupo– Consultor Jurídico Sênior

DPO da Europa

- DPO Áustria
- DPO Bélgica e Luxemburgo
- DPO República Tcheca
- DPO França, Morrocos, Tunisia
- DPO Alemanha
- DPO Hungria
- DPO Italia
- DPO Ucrania
- DPO Holanda
- DPO Países Nórdicos
- DPO Polônia
- DPO Portugal
- DPO Romênia e Eslováquia
- DPO Espanha
- DPO Suiça
- DPO UK/ Ireland

DPO da América do Norte

DPO LATAM

- DPO Argentina
- DPO Brasil
- DPO Chile
- DPO Colombia
- DPO Guatemala
- DPO Mexico

DPO Ásia-Pacífico

- DPO Australia
- DPO Nova Zelândia
- DPO India
- DPO China
- DPO Singapora
- DPO Sudeste Asiático
- DPO Oriente Médio
- DPO Japão

Nota 1: Os DPOs reportam ao seu Conselheiro Geral local e, em linha pontilhada, ao DPO do Grupo

Como exercer seus direitos de proteção de dados?

Noções-chave de proteção de dados

Dados Pessoais	Qualquer informação que possa ser usada para identificar um indivíduo, direta ou indiretamente, quando combinada com outras.
Tratamento	Qualquer operação realizada sobre dados pessoais, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação, combinação, restrição, exclusão ou destruição.
Titular dos Dados	Qualquer pessoa natural identificada ou identificável, cujo Dado Pessoal esteja sendo processado.
Controlador	A pessoa natural ou jurídica que determina as finalidades e os meios do tratamento de dados pessoais.
Operador	A pessoa física ou jurídica que processa dados pessoais em nome do controlador.
Finalidade	A(s) razão(ões) pelas quais o controlador precisa coletar e tratar posteriormente os dados pessoais.
Autoridade Nacional de Proteção de Dados" (ou "ANPD")	Órgão da administração pública federal, integrante da Presidência da República, responsável por zelar pela proteção dos dados pessoais, elaborar diretrizes, fiscalizar e aplicar sanções em caso de descumprimento da legislação, além de outras atribuiçõe
Encarregado pela Proteção dos Dados Pessoais	É a pessoa indicada pelo Controlador e pelo Operador de Dados, cuja função é atuar, principalmente, como um canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)

A Capgemini Service SAS e/ou as afiliadas da Capgemini SE (juntas denominadas "Capgemini") coletam e tratam seus dados pessoais como controladora ou como operadora em nome de uma controladora. Em qualquer caso, você pode entrar em contato com a Capgemini – seguindo o procedimento descrito abaixo – para exercer seus direitos de proteção de dados.

Observe que você também pode apresentar uma reclamação a uma Autoridade de Controle e/ou buscar reparação judicial perante o tribunal.

Quais são os seus direitos?

Você pode solicitar o exercício dos seguintes direitos em relação aos dados pessoais que lhe dizem respeito e que a Capgemini coleta e trata posteriormente:

Confirmação da Existência e Acesso	Você pode perguntar à Capgemini se dados pessoais que lhe dizem respeito estão sendo tratados e, caso estejam, pode solicitar acesso a esses dados pessoais
Exclusão	Em alguns casos, você pode solicitar que a Capgemini exclua seus dados pessoais
Retificação	Você pode solicitar à Capgemini que retifique, atualize ou complemente seus dados pessoais
Objeção	Em alguns casos, você pode solicitar que a Capgemini não trate seus dados pessoais
Restrição	Em alguns casos, você pode solicitar que a Capgemini limite o tratamento dos seus dados pessoais a determinadas finalidades e sob certas condições
Revogar o consentimento	Você pode retirar seu consentimento para o tratamento dos seus dados pessoais, mesmo que tenha concedido esse consentimento anteriormente à Capgemini
Portabilidade	Em alguns casos, você pode solicitar que a Capgemini forneça seus dados pessoais em um formato estruturado, de uso comum e legível por máquina; e/ou que transmita esses dados a outro controlador
Reclamação	Você também pode apresentar uma reclamação caso considere que a Capgemini está infringindo a(s) regulamentação(ões) de proteção de dados aplicável(is) ou as Regras Corporativas Vinculativas (BCR)

Observe que esses direitos podem ser **limitados em algumas situações, conforme a legislação aplicável**. Por exemplo, se conceder a você acesso aos seus dados pessoais revelar dados pessoais de outra pessoa; ou se você solicitar à Capgemini a exclusão de seus dados pessoais enquanto houver obrigação legal de mantê-los.

Fale conosco

Para exercer seus direitos, ou se tiver dúvidas ou preocupações relacionadas às nossas políticas de proteção de dados, entre em contato conosco:

Usando nosso formulário de contato dedicado

Por e-mail

Por correspondência

Lista completa dos escritórios da Capgemini disponível em nosso site.

Por telefone

Lista completa dos escritórios da Capgemini disponível em nosso site

Para que possamos atender adequadamente à sua solicitação, por favor, forneça as seguintes informações:

- ☐ **Seu nome completo***
- ☐ Seu status (colaborador, candidato, etc.)
- ☐ **Seu endereço de e-mail ou outro meio de comunicação preferencial***
- ☐ Verificação de identidade: você poderá ser solicitado a fornecer documentação adequada de identificação.
- ☐ País / Região
- ☐ **A natureza da sua solicitação***

* Sem essas informações, a Capgemini não poderá atender à sua solicitação.

Como a Capgemini atenderá sua solicitação?

A Capgemini analisará e avaliará sua solicitação ou reclamação e a tratará sem demora injustificada.

Confirmação de recebimento

Análise da sua solicitação pelo Encarregado de Proteção de Dados local competente

Atendendo ao seu pedido

- Dentro de 15 dias após o recebimento da solicitação
- Caso não seja possível atender integralmente nesse prazo, a Capgemini poderá apresentar justificativa e fornecer informações sobre o andamento da análise.

Análise e conclusão da sua solicitação

Se você enviou sua solicitação por meios eletrônicos, a Capgemini fornecerá as informações solicitadas em um formato eletrônico de uso comum.

Caso a Capgemini não consiga ou se recuse a atender favoravelmente à sua solicitação, Ela deverá fornecer detalhes explicando sua decisão, bem como um lembrete de que você pode recorrer ao tribunal competente e/ou à autoridade supervisora.

Capgemini processando dados em nome de seus clientes

Quando a Capgemini estiver tratando Dados Pessoais em nome de seus Clientes (atuando como Controlador), a Capgemini recomenda fortemente que você envie sua solicitação diretamente ao controlador.

Em qualquer caso, se a Capgemini receber uma solicitação diretamente, ela deverá notificar o controlador dos dados sem demora injustificada, conforme os termos e condições acordados entre a Capgemini e o controlador.

Caso a Capgemini seja instruída pelo controlador a lidar diretamente com sua solicitação, ela seguirá o procedimento mencionado acima em estreita coordenação com o controlador dos dados.