SIEMENS

Regras Corporativas Vinculativas (“RCV”) - Síntese dos Direitos das Partes Terceiras

Este documento contém nas Secções 3 - 9 todas as provisões das “Regras Corporativas Vinculativas (RCV) para as Empresas do Grupo Siemens e Outras Empresas Adotantes para a Proteção de Dados Pessoais” que são vinculativas vis-à-vis para os titulares dos dados, por virtude dos direitos de terceiros beneficiários.

1. Propósito das RCV

Proteger a segurança e a privacidade dos dados pessoais é importante para a Siemens. Por esse motivo, a Siemens conduz os seus negócios em conformidade com as leis aplicáveis sobre a proteção da privacidade de dados e a segurança de dados. As RCV são regras internas adotadas pela Siemens, p.ex., Siemens AG e as empresas participantes no seu grupo, para produzir “salva-guardas adequadas para a proteção da privacidade e dos direitos e liberdades fundamentais dos indivíduos” de acordo com o significado das leis de proteção de dados aplicáveis, particularmente as leis de proteção de dados dos estados membros do Espaço Económico Europeu (“E**EE**”).

2. Âmbito das RCV

As RCV aplicam-se ao processamento de todos os dados pessoais relativos aos titulares dos dados através das empresas participantes estabelecidas:

- Fora de um país do EEE na medida em que estes dados pessoais tenham sido transferidos a partir de uma empresa participante estabelecida num país do EEE ou estabelecida num país com um nível adequado de proteção de dados como reconhecido pela decisão da Comissão da UE para uma empresa participante estabelecida fora do EEE; e
- num país do EEE ou num país com um nível adequado de proteção de dados como reconhecido pela decisão da Comissão da UE.

3. Princípios substantivos para o processamento dos dados pessoais

Os seguintes princípios, que derivam especificamente do Regulamento EU 2016/679 de 27 de abril, aplicam-se ao processamento de dados pessoais por empresas participantes dentro do âmbito destas RCV:

3.1 Legitimidade & legalidade do processamento de dados

O processamento dos dados pessoais deverá ser feito legalmente e em conformidade com as normas legislativas relevantes e com a devida consideração em relação aos princípios descritos nestas RCV.

O processamento só é autorizado se pelo menos um destes prérequisitos for cumprido:

- O titular dos dados deu de livre vontade o seu consentimento de forma efetiva e inequívoca; ou
- O processamento dos dados está incluido no propósito de estabelecer uma relação contratual ou uma relação semelhante de confiança com o titular dos dados; ou
- O processamento dos dados é necessário para salvaguardar os interesses do controlador (no âmbito destas RCV, “controlador” significa a empresa que determina os propósitos e meios do processamento de dados; ramos dependentes, locais de negócio e estabelecimentos permanentes são parte do controlador) e não existam motivos para assumir que o titular dos dados possui um interesse legítimo predominante em impedir o processamento dos dados; ou
- O processamento é estipulado ou permitido por lei nacional e regulamentos que se aplicam ao controlador; ou
- O processamento é necessário para a conformidade com as obrigações legais às quais o controlador está sujeito; ou
- O processamento é necessário excecionalmente para proteger a vida, saúde ou segurança do titular dos dados.

O controlador deverá fornecer procedimentos simples, rápidos e eficientes que permitam ao titular dos dados anular o seu consentimento em qualquer altura.

3.2 Propósito

Os dados pessoais devem ser processados exclusivamente para propósitos específicos, explícitos e legítimos. Em nenhumas cirscunstâncias, os dados pessoais devem ser processados de forma incompatível com os propósitos legítimos para os quais os dados pessoais foram recolhidos. As empresas participantes são obrigadas a aderir a estes propósitos originais quando armazenam, processam ou utilizam os dados que lhes foram transferidos por outra empresa participante; o propósito do processamento dos dados só deverá ser alterado com consentimento do titular dos dados ou na medida permitida por lei nacional e à qual a empresa participante e que transfere os dados está sujeita.

3.3 Transparência

Todas as empresas participantes devem processar os dados pessoais de forma transparente. As seguintes informações devem ser dadas pela empresa participante ao titular cujos dados estejam a ser processados (em concertação com a empresa contribuidora, se aplicável) :

- Identidade da empresa controladora e contribuidora dos dados;

- Categoria dos recetores ou identidade da entidade recetora;
- Propósito do processamento;
- Origem dos dados (a menos que sejam dados pessoais recolhidos diretamente a partir do titular dos mesmos);
- Direito de objeção ao processamento dos dados pessoais do titular para finalidades comerciais;
- Outras informações necessárias por razões de equidade, p.ex., direitos de informação, retificação e eliminação.

Na medida em que os dados pessoais não tenham sido recolhidos diretamente a partir do respetivo titular, tais informações não devem - excecionalmente - ser fornecidas, caso esta falta de fornecimento de informação seja necessária para proteger o titular dos dados ou os direitos de outras pessoas, se o titular já tiver sido informado ou se envolver um esforço desproporcional.

3.4 Qualidade dos dados e economia dos dados

Os dados pessoais devem estar factualmente corretos e - se necessário - atualizados. As medidas adequadas devem ser tomadas para garantir que dados incorretos ou imcompletos são corrigidos ou eliminados.

O processamento de dados deve ser guiado pelo princípio da economia de dados. O objetivo é recolher, processar e utilizar tais dados pessoais apenas na medida do necessário, p.ex., utilizar a menor quantidade de dados pessoais possível. Em particular, deve ser feita a utilização da possibilidade de dados anónimos ou pseudónimos, desde que o custo e esforço envolvido seja compatível com o propósito desejado. As avaliações estatísticas ou estudos baseados em dados anonimizados ou com pseudónimos não são relevantes para propósitos de proteção da privacidade dos dados, desde que estes dados não possam ser utilizados para identificar o titular dos dados.

Os dados pessoais que já não sejam necessários para as finalidades de negócio para as quais foram inicialmente recolhidas e armazenadas, devem ser eliminados. Caso se apliquem períodos de retenção regulamentares, os dados devem ser bloqueados em vez de eliminados.

3.5 Transferências posteriores dos dados

A transferência dos dados pessoais a partir de uma empresa participante para uma empresa não participante (p.ex., uma empresa que não esteja vinculada às RCV) fora do EEE só é permitida sob as seguintes condições:

- A entidade recetora é dotada de um nível adequado de proteção de dados pessoais tal como previsto no Regulamento EU 2016/679 de 27 de abril ou através da conclusão de outros acordos contratuais adequados entre a entidade contribuidora e recetora;

- A transferência é autorizada sob as exceções definidas no Artigo 26 da Diretiva 95/46/CE de Proteção de Dados da UE;
- Se a entidade recetora for processadora, devem ainda ser cumpridas as condições definidas no Regulamento EU 2016/679 de 27 de abril.

3.6 Categorias especiais de dados pessoais

As categorias especiais de dados pessoais, por outras palavras, informações sobre a origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiações sindicais, saúde ou vida sexual, não devem ser processadas como princípio geral.

Caso o processamento das categoriais especiais de dados pessoais seja necessário, o consentimento explícito do titular dos dados deve ser obtido, a não ser que,

- O titular dos dados não esteja em posição de dar o seu consentimento (p.ex., emergência médica) e o processamento seja necessáro para proteger os interesses vitais do titular ou de outra pessoa; ou
- O processamento é necessário em ligação com o diagnóstico médico, medicina preventiva, a provisão de cuidados ou tratamento ou a gestão de serviços de cuidados de saúde onde o processamento dos dados é levado a cabo por pessoal médico que está sujeito à obrigação do sigilo profissional ou por outro pessoal sujeito a uma obrigação equivalente de sigilo, ou
- O titular dos dados já tornou públicos os dados em questão; ou
- O processamento é necessário para o estabelecimento, exercício e defesa de ações judiciais em procedimentos de tribunal, desde que não existam razões para assumir que o titular dos dados não possui interesses legítimos predominantes em garantir que os dados não são processados; ou
- O processamento é expressamente permitido por lei sob a aplicação da legislação nacional (p.ex., para o propósito de registo/proteção de minorias), e das garantias adicionais dentro do âmbito do Regulamento EU 2016/679 de 27 de abril são fornecidos para o processamento de dados, incluindo medidas de segurança especificamente adequadas para estes dados.

O Responsável da Proteção de Dados (DPO) competente da empresa participante deve ser consultado anteriormente ao processamento das categorias especiais de dados pessoais.

3.7 Decisões individuais automatizadas

Se os dados pessoais forem processados para a tomada de decisões individuais automatizadas, os interesses legítimos do titular dos dados deve ser garantido através das medidas adequadas. Decisões que tenham consequências legais negativas para o titular dos dados ou que prejudiquem substancialmente o titular dos dados, não devem ser tomadas exclusivamente com base num procedimento individual automatizado concebido para avaliar as características pessoais de um indivíduo, p.ex., decisões que não se devem basear exclusivamente na utilização de tecnologias de informação. Uma exceção aplica-se apenas se a decisão

- for tomada durante a formação de ou durante o período de vigência de um contrato, desde que o pedido para formação de ou o período de vigência do contrato, apresentado pelo titular dos dados, tenha sido cumprido ou que existam medidas adequadas para salvaguardar os seus interesses legítimos, tais como dar a oportunidade de dar o seu ponto de vista; ou
- seja permitida por lei, o que também define as medidas para salvaguardar os interesses legítimos do titular dos dados.

3.8 Segurança dos dados

Os controladores devem tomar as medidas técnicas e organizacionais adequadas para garantir a segurança de dados necessária para proteger os dados pessoais contra eliminação acidental ou ilegal, utilização não autorizada, alteração, contra a perda e destruição, assim como contra a divulgação não autorizada ou acesso não autorizado. Tendo em atenção o nível e custo da sua implementação, tais medidas devem garantir um nível de segurança adequado aos riscos representados pelo processamento e à natureza dos dados a serem protegidos. Deve ser dada uma proteção diferenciada às categorias especiais de dados pessoais.

As medidas de segurança a serem fornecidas estão particularmente relacionadas com computadores (servidores e computadores do local de trabalho), redes, *links* de comunicação e aplicações.

Para garantir um nível adequado de medidas técnicas e organizacionais para a proteção de dados, a Siemens introduziu o Guia de Segurança de Informação Corporativa com efeito vinculativo sobre todo o o grupo Siemens.

As medidas específicas utilizadas para garantir uma proteção adequada aos dados pessoais incluem controlos de admissão, controlos de acesso ao sistema, controlos de acesso aos dados, controlos de transmissão, controlos de introdução, controlos dos trabalhos, controlos de disponibilidade e controlos de segregação.

Todos os computadores do local de trabalho - incluindo dispositivos móveis (p.ex., computadores portáteis) - estão protegidos por palavra-passe. A *intranet* da Siemens possui um sistema de *firewall* para proteger os conteúdos internos da empresa contra acessos não autorizados. A transmissão de dados pessoais dentro da rede da empresa está tipicamente encriptada - na medida em que a natureza e o propósito pretendido dos dados pessoais o torne necessário.

3.9 Confidencialidade do processamento de dados

Apenas o pessoal que tenha sido autorizado e especificamente instruído em conformidade com os requisitos de proteção da privacidade de dados pode recolher, processar ou utilizar os dados pessoais. A autorização de acesso do colaborador individual deverá ser restringida de acordo com a natureza e âmbito do seu campo de atividade. O colaborador está proíbido de utilizar os dados pessoais para propósitos privados, de transferir ou disponibilizar os dados pessoais a pessoas não autorizadas. As pessoas não autorizadas neste contexto incluem, por exemplo, outros colaboradores, na medida em que

estes não precisem dos dados pessoais para desempenhar as suas funções. A obrigação de confidencialidade continua além do termo da relação laboral do colaborador em questão.

3.10 Encomenda do processamento de dados

Se uma empresa participante encomendar outra empresa ("processador") para processar os dados pessoais sob os termos destas RCV, os seguintes requisitos devem ser cumpridos:

- O processador deve ser cuidadosamente selecionado pelo controlador; deve ser selecionado um processador capaz de garantir as medidas de segurança técnicas e organizacionais necessárias para realizar o processamento dos dados em conformidade com os regulamentos de proteção da privacidade de dados;
- O controlador deve garantir e verificar regularmente que o processador permanece em total conformidade com as medidas de segurança técnicas e organizacionais;
- A realização do processamento dos dados por encomenda deve ser regulamentada num contrato escrito ou documentada de outra forma, onde os direitos e obrigações do processador estejam definidos de forma inequívoca;
- O processador deverá estar vinculado através de contrato para processar os dados recebidos a partir do controlador apenas dentro do âmbito contratual e em conformidade com as instruções emitidas pelo controlador. O processamento dos dados para finalidades do processador ou para finalidades de partes terceiras deve ser proibida por contrato;
- O controlador retem a responsabilidade de legitimação do processamento e continua a ser o ponto de contacto para o titular dos dados.

4. Direitos substantivos do titular dos dados

O titular dos dados possui os direitos inalienáveis indicados abaixo a respeito dos seus dados pessoais processados por uma empresa participante dentro do âmbito destas RCV.

- O titular dos dados pode exigir que lhe seja comunicado, de forma intelegível, quais os dados pessoais processados relativos a si, sobre qualquer informação disponível assim como a sua

  fonte e o propósito do processamento. O titular dos dados também possui o direito a informações sobre a identidade do controlador e, no caso de transferência de dados pessoais, o titular dos dados também possui o direito a informações sobre os recipientes ou categorias de recipientes. O direito de informação também cobre a estrutura lógica das operações automatizadas de processamento, na medida em que as decisões automatizadas sejam afetadas. Quando previsto pela lei local aplicável, o titular dos dados não possui um direito de informação caso envolva um comprometimento considerável das intenções de negócio, incluindo particularmente se a revelação dos segredos de negócio e o interesse de salvaguarda dos segredos de negócio compensarem o interesse do titular dos dados na divulgação. Os

regulamentos legais locais podem restringir o direito a informação do titular dos dados se este direito for exercido repetidamente dentro de um curto período de tempo, a menos que o titular consiga apresentar uma razão legítima para repetição de pedidos de informação. A empresa participante pode cobrar uma taxa razoável pela prestação da informação, na medida em que a lei nacional aplicável o permita.

- O titular dos dados pode exigir a **rectificação** dos seus dados pessoais caso estejam incorretos ou imcompletos.
- O titular dos dados possui o direito de exigir que os seus dados pessoais sejam **bloqueados** caso não seja possível determinar se os dados estão corretos ou incorretos.
- O titular dos dados possui o direito de exigir que os seus dados pessoais sejam **eliminados** se o processamento dos dados tiver sido ilegal ou se tenha tornado ilegal ou assim que os dados já não sejam necessários para o propósito do processamento. As declarações justificadas pelo titular dos dados para rasura devem ter uma resposta dentro de um período razoável, na medida em que os períodos legais de retenção ou as obrigações contratuais não previnam a eliminação. No caso de períodos legais de retenção, o titular dos dados pode exigir que os seus dados sejam bloqueados em vez de eliminados. O mesmo se aplica quando for impossível eliminar os dados.
- O titular dos dados tem o direito de contestar o processamento dos seus dados pessoais para finalidades comerciais ou para propósitos de pesquisas de mercado e/ou de sondagens de opinião. O titular dos dados deverá ser informado sobre o seu direito de contestar sem pagamento de taxas.
- O titular dos dados também possui um direito geral de objeção ao processamento dos seus dados pessoais se, devido à situação especial do titular, o interesse legítimo do titular compensar o interesse legítimo do controlador no processamento de dados pessoais.

O titular dos dados poderá impor os direitos acima referidos por escrito *vis-à-vis* na respetiva empresa participante, o Responsável da Proteção de Dados (DPO) competente dessa empresa participante ou a função global de Proteção de Dados (LC CO DP) da Siemens Healthcare AG. O pedido justificado do titular dos dados deverá receber uma resposta a partir da entidade contactada dentro de um período razoável. A resposta deverá ser dada em formato escrito (*e-mail* é suficiente).

5. Natureza vinculativa *vis-à-vis* do titular dos dados

Os regulamentos das RCV contidos nas Secções 3 - 9 deste documento também são vinculativas do titular dos dados *vis-à-vis*, por virtude dos direitos de terceiro beneficiário.

Os titulares dos dados podem optar por apresentar uma reclamação por não conformidade com as regulações das RCV aqui contidas por uma empresa participante, seja contra a empresa participante ou contra a Siemens Healthcare AG (LC CO DP).

Além disso, os titulares dos dados estão autorizados a fazer cumprir a conformidade com um dos direitos beneficiários de partes terceiras através de uma empresa participante, através da apresentação de uma reclamação antes da autoridade de proteção de dados competente ou através da procura por

outras soluções legais nos tribunais competentes. Os titulares dos dados podem pedir uma compensação pelos danos.

Os titulares dos dados podem optar por apresentar a tal reclamação

- antes da jurisdição da empresa participante que transferiu os dados; ou
- antes da jurisdição da sede da Siemens Healthcare AG; ou
- antes da autoridade competente para a proteção de dados.

Isto significa que no caso de uma violação dos regulamentos por uma empresa participante estabelecida fora do EEE, os tribunais e as autoridades dentro do EEE também são competentes. O titular dos dados detem os mesmo direitos *vis-à-vis* da empresa participante que aceitou a fiabilidade, como se a violação tivesse sido cometida por uma empresa participante estabelecida num país do EEE.

A competência dos tribunais e autoridades no EEE como descritos acima não se aplica, contudo, se o recetor dos dados estiver estabelecido fora do EEE mas o país não possua um nível adequado de proteção de dados como reconhecido por decisão da Comissão da UE.

De forma a garantir que os titulares dos dados tiram partido de direitos de terceiro beneficiário legalmente aplicáveis também nos países onde a prestação de direitos de terceiro beneficiário no documento de RCV poderá não ser suficiente, a Siemens AG irá - na medida do necessário - conceber acordos contratuais adicionais com autorização das empresas participantes relevantes. Está incluida uma cláusula de terceiro beneficiário a conceder os direitos necessários aos titulares dos dados na Declaração de Compromisso que os grupos empresariais assinam para simbolizar a sua aceitação e implementação das RCV. O mesmo se aplica ao Acordo de Adoção que as outras empresas adotantes finalizam com a Siemens AG.

6. Processo de reclamação

O titular dos dados pode contactar o departamento competente para as reclamações da Siemens Healthcare AG (LC CO DP; para detalhes de contacto, ver o tópico 10) ou o ponto de contacto local competente para a proteção de dados da empresa participante (geralmente o Responsável da Proteção de Dados (DPO)), em qualquer momento, com reclamações sobre uma violação das RCV por uma empresa participante ou com qualquer outra questão. Deverá ser dada ao titular dos dados uma confirmação imediata da receção da reclamação na entidade contactada e a reclamação deverá ser processada dentro do período de três (3) meses após a receção da reclamação. Estes prazos podem ser excedidos em caso de atrasos não atribuíveis à empresa participante, p.ex., no caso de uma falha do titular dos dados em fornecer as informações necessárias dentro dos períodos adequados.

Os colaboradores envolvidos no processamento das reclamações no departamento competente beneficiam de um nível adequado de independência no exercício desta função.

No caso de inquérito, a empresa participante e LC CO DP são obrigados a cooperar com as autoridades de proteção de dados do país e respeitar as suas opiniões.

7. Assistência mútua e cooperação com as autoridades de proteção de dados

A Siemens Healthcare AG e as empresas participantes irão colaborar e dar apoio mútuo no caso de inquéritos ou reclamações dos titulares dos dados relativas à não conformidade com as RCV.

A Siemens Healthcare AG e as empresas participantes assumem colaborar com as autoridades competentes da proteção de dados no contexto da implementação da RCV. Ambas irão responder a pedidos relacionados com as RCV a partir da autoridade de proteção de dados dentro de um prazo aceitável e de forma adequada e irá seguir os conselhos e decisões da autoridade de proteção de dados competente tendo em conta a implementação das RCV.

8. Relação entre as RCV e os regulamentos legais locais

A legitimação do processamento dos dados pessoais é julgada com base na lei local aplicável. Na medida em que a lei local aplicável estipular um nível mais elevado de proteção dos dados pessoais do que estas RCV, o processamento de dados deverá ser feito em conformidade com a lei aplicável. Cada empresa participante deverá verificar por si mesma (p.ex., através do seu Responsável de Proteção de Dados (DPO) ou pelo departamento legal), se estes regulamentos legais locais (p.ex., as leis sobre a privacidade de dados) existem e devem garantir a conformidade com as mesmas. Se a lei local aplicável oferecer um nível mais baixo de proteção dos dados pessoais do que estas RCV, deverão ser aplicadas estas RCV.

No caso de as obrigações emergentes da lei local aplicável estarem em conflito com as RCV, a empresa participante deverá informar o LC C DP sem atraso indevido. LC C DP irá registar o conflito relatado.

LC C DP irá informar todas as empresas participantes que previamente transferiram dados para a empresa participante em causa, sobre o conflito entre as RCV e as leis locais. LC C DP também irá informar a autoridade de proteção de dados competente e, juntamente com a autoridade de proteção de dados e a empresa participante, irá procurar uma solução prática que se aproxima o mais possível dos princípios plasmados no Regulamento EU 2016/679 de 27 de abril.

9. Responsabilidades

A Siemens Healthcare AG assume a responsabilidade pela não conformidade com as RCV por empresas participantes estabelecidas fora do EEE. A Siemens AG assume monitorizar a conformidade com as RCV por empresas participantes estabelecidas fora do EEE e para garantir que as empresas participantes estabelecidas fora do EEE implementam as ações corretivas necessárias para corrigir violações das RCV.

A Siemens Healthcare AG assume também o pagamento de compensações por danos no caso de uma violação comprovada das RCV e uma consequente violação dos direitos do titular dos dados.

O ónus probatório pertence à Siemens Healthcare AG. A Siemens Healthcare AG deverá demonstrar que não ocorreu qualquer violação das RCV ou que a empresa participante estabelecida fora dos EEE não é responsável pela violação das RCV sobre as quais se baseia a reclamação por danos.

10. Contacto

O titular dos dados pode levantar qualquer questão com o Responsável de Proteção de Dados (DPO) da empresa participante relevante ou com a função global de Privacidade de Dados da Siemens AG:

Siemens Healthcare, Lda
LC CO DP
Rua Irmãos Siemens, 1 – 1A
2720-093 Amadora
Portugal
Email: hugo.pinho@siemens-healthineers.com
Internet: siemens.pt/healthineers