ACORDO DE TRATAMENTO DE DADOS

Última atualização em 14 de agosto de 2026

O presente **ACORDO DE TRATAMENTO DE DADOS** (doravante também designado por «**Acordo**») constitui um acordo jurídico vinculativo entre AJAX SYSTEMS TRADING FZE (doravante «**Ajax**» ou «**Subcontratante**») e o Responsável pelo Tratamento dos Produtos e Software Ajax, conforme definido na Secção 1 do presente Acordo (doravante também o «**Responsável pelo Tratamento**»), cada um individualmente designado por «Parte» e conjuntamente designados «Partes».

Ao utilizar os Produtos e o Software Ajax, o utilizador final aceita e celebra o presente Acordo; o utilizador final (e o seu signatário, se aplicável) declara e garante que o utilizador final e o seu signatário têm capacidade jurídica e poderes para celebrar o presente Acordo vinculativo e cumprir os seus termos, e que o utilizador final atuará em conformidade com o presente Acordo e com toda a legislação aplicável.

ENQUADRAMENTO E OBJETO

A. No âmbito do presente Acordo, o Subcontratante, o Responsável pelo Tratamento e quaisquer terceiros relevantes (ou seja, Subcontratantes Ulteriores) especificados no Acordo e aprovados por ambas as Partes estão envolvidos na prestação dos Serviços, a qual exige que os Dados Pessoais (conforme definidos abaixo) sejam tratados pelo Subcontratante por conta do Responsável pelo Tratamento. O Subcontratante pode tratar Dados Pessoais por conta do Responsável pelo Tratamento nos termos do presente Acordo e de todas as suas partes integrantes, nomeadamente anexos, aditamentos, entre outros.

B. As Partes pretendem executar o presente Acordo em conformidade com os requisitos do enquadramento legal aplicável relativo ao tratamento de dados e com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (doravante também designado por «Regulamento Geral sobre a Proteção de Dados» ou «RGPD»), relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

C. O presente Acordo tem por objeto definir as práticas de privacidade e proteção de dados a aplicar na prestação dos Serviços (conforme definidos abaixo). O presente Acordo e outros documentos contratuais relacionados constituem um acordo de tratamento de dados, conforme exigido pelo Artigo 28.º do RGPD. As Partes pretendem que o presente Acordo seja interpretado de forma consistente com este objetivo e com as suas obrigações nos termos do RGPD e de outra legislação aplicável em matéria de proteção de dados. Salvo se o contexto exigir o contrário, os termos utilizados no presente Acordo e nos seus anexos terão o mesmo significado que lhes é atribuído no RGPD.

1. DEFINIÇÕES E INTERPRETAÇÃO

Salvo indicação em contrário no presente Acordo, os termos e expressões iniciados por maiúscula aqui utilizados terão os seguintes significados:

1.1 «**Acordo**» significa o presente Acordo de Tratamento de Dados e todos os apêndices, anexos e documentação complementar. As referências no presente Acordo ao «Acordo de Utilizador Final» referem-se ao Acordo de Utilizador Final de Ajax, disponível em https://ajax.systems/end-user-agreement/;

1.2 «**Responsável pelo tratamento**» significa o titular da conta que registou uma conta para utilizar os Produtos e Software Ajax como utilizador final e que determina as finalidades e os meios do tratamento de Dados Pessoais realizado pelo Subcontratante em seu nome. O Responsável pelo tratamento pode ser uma pessoa singular ou coletiva.

1.3 «**Regulamentação de Proteção de Dados**» significa a Legislação da UE sobre Proteção de Dados (incluindo, entre outros, o Regulamento Geral sobre a Proteção de Dados da UE 2016/679 e as leis que

implementam ou complementam o RGPD) e, na medida em que seja aplicável, a legislação de proteção de dados ou privacidade de qualquer outro país relevante para o tratamento ao abrigo do presente Acordo;

1.4 «**EEE**» significa o Espaço Económico Europeu;

1.5 «**Dados Pessoais**» significa qualquer informação relativa a uma pessoa singular identificada ou identificável que o Subcontratante trate em nome do Responsável pelo Tratamento, nos termos ou no âmbito do Acordo de Utilizador Final disponível em https://ajax.systems/end-user-agreement/ ou de qualquer outro acordo, caso adicionalmente acordado entre as Partes.

1.6 «**Serviços**» significa os serviços prestados pelo Subcontratante ao Responsável pelo Tratamento no âmbito dos Produtos e Software Ajax.

1.7 «**Instruções**» significa qualquer instrução dada pelo Responsável pelo Tratamento ao Subcontratante relativamente ao tratamento de Dados Pessoais, quer seja prestada (a) através da funcionalidade dos Produtos e Software Ajax; (b) através de acordos técnicos, anexos ou outra documentação acordada com o Subcontratante; ou (c) de qualquer outra forma acordada por escrito entre as Partes. Para evitar dúvidas, o Subcontratante não está obrigado a verificar o fundamento jurídico ou a adequação das Instruções, salvo se estas contrairem a Regulamentação de Proteção de Dados aplicável.

1.8 «**Subcontratante Ulterior**» significa qualquer terceiro relevante nomeado pelo, ou em nome do, Subcontratante para tratar Dados Pessoais e quaisquer outros dados relacionados em nome do Responsável pelo Tratamento nos termos do Acordo.

1.9 **«Produtos e Software Ajax»** significa os produtos de hardware e software associado disponibilizados por Ajax ao abrigo do Acordo de Utilizador Final disponível em https://ajax.systems/end-user-agreement/.

2. FINALIDADES DO TRATAMENTO DE DADOS

2.1 O objeto do tratamento ao abrigo do presente Acordo são os Dados Pessoais gerados através de, ou no âmbito da, utilização dos Produtos e Software Ajax por parte do Responsável pelo Tratamento, os quais o Subcontratante trata em nome do Responsável pelo Tratamento para os fins previstos na presente Secção 2.

2.2 O tratamento consiste na recolha, conservação, organização, transmissão, recuperação e eliminação de Dados Pessoais através da infraestrutura em nuvem do Subcontratante, bem como em qualquer outra operação necessária para concretizar os fins previstos na cláusula 2.3 do presente Acordo.

2.3 O Subcontratante tratará os Dados Pessoais mediante Instruções documentadas do Responsável pelo Tratamento, conforme estipulado na cláusula 3.1 do presente Acordo, para os seguintes fins:

(a) operar a infraestrutura em nuvem que recebe, trata e conserva eventos, alertas e outros dados gerados pelos Produtos e Software Ajax, e transmitir as notificações correspondentes ao Responsável pelo Tratamento;

(b) permitir o acesso remoto e o controlo do Responsável pelo Tratamento aos Produtos e Software Ajax, incluindo o acesso a gravações e ao histórico de eventos gerados pelos dispositivos;

(c) prestar suporte técnico ao Responsável pelo Tratamento no âmbito da sua utilização dos Produtos e Software Ajax;

(d) permitir que o Responsável pelo Tratamento, mediante Instruções documentadas, partilhe o acesso aos Produtos e Software Ajax e aos Dados Pessoais relacionados com terceiros autorizados pelo Responsável pelo Tratamento, conforme mais detalhadamente descrito na cláusula 3.3 do presente Acordo.

2.4 O Subcontratante tratará os Dados Pessoais pelo período de duração estabelecido na Secção 9 do presente Acordo.

2.5 As categorias de titulares dos dados e as categorias de Dados Pessoais tratados ao abrigo do presente Acordo encontram-se previstas no Anexo 1.

3. OBRIGAÇÕES GERAIS RELATIVAS AO TRATAMENTO DE DADOS

3.1 **Instruções**. O Subcontratante tratará os Dados Pessoais exclusivamente:

(a) para os fins previstos na Secção 2 do presente Acordo;
(b) de acordo com as instruções documentadas do Responsável pelo Tratamento; e
(c) em conformidade com a Regulamentação de Proteção de Dados aplicável.

O Responsável pelo Tratamento não dará instruções ao Subcontratante para tratar Dados Pessoais em violação da lei aplicável. O Subcontratante não terá qualquer responsabilidade por quaisquer danos ou prejuízos resultantes do cumprimento de Instruções que o Responsável pelo Tratamento não estivesse legalmente legitimado a dar. Se o Subcontratante considerar fundamentadamente que uma Instrução viola a Regulamentação de Proteção de Dados aplicável, informará prontamente o Responsável pelo Tratamento por escrito, salvo se tal for legalmente proibido, e poderá suspender o tratamento dos Dados Pessoais afetados (com exceção da mera conservação e manutenção da segurança de tais dados) até que o Responsável pelo Tratamento forneça novas Instruções que o Subcontratante possa cumprir. Durante qualquer suspensão desta natureza, o Subcontratante não será responsável por qualquer incumprimento das obrigações que dependam do tratamento suspenso.

3.2 O Subcontratante cumprirá a Regulamentação de Proteção de Dados aplicável e implementará os sistemas e procedimentos adequados para garantir que quaisquer Dados Pessoais tratados ao abrigo do presente Acordo sejam adequados, pertinentes, não excessivos, exatos e não conservados durante mais tempo do que o necessário.

3.3 O Responsável pelo Tratamento poderá, mediante Instruções documentadas, autorizar o Subcontratante a partilhar Dados Pessoais com as seguintes categorias de terceiros, atuando cada um deles como responsável pelo tratamento independente no que respeita aos Dados Pessoais que receber:

(a) empresas de monitorização profissional e centrais recetoras de alarmes (CRA) contratadas pelo Responsável pelo Tratamento;

(b) empresas de serviços de segurança e vigilância contratadas pelo Responsável pelo Tratamento;

(c) engenheiros de instalação e manutenção a quem o Responsável pelo Tratamento tenha concedido direitos de acesso à conta PRO.

O Subcontratante apenas transferirá Dados Pessoais para tais terceiros mediante Instruções documentadas do Responsável pelo Tratamento, não assumindo qualquer responsabilidade pelo seu tratamento posterior.

3.4 O Subcontratante fica pelo presente autorizado a responder diretamente aos pedidos dos titulares dos dados relativos ao exercício dos seus direitos ao abrigo da Regulamentação de Proteção de Dados aplicável no âmbito do tratamento efetuado nos termos do presente Acordo. O Subcontratante notificará o Responsável pelo Tratamento de qualquer pedido dessa natureza, bem como da ação substantiva adotada, no prazo máximo de cinco (5) dias úteis após a resposta ao pedido. A obrigação de assistência do Subcontratante limitar-se-á às medidas tecnicamente viáveis, tendo em conta a natureza do tratamento.

3.5 O Subcontratante prestará ainda ao Responsável pelo Tratamento uma assistência comercialmente razoável para garantir o cumprimento das obrigações do Responsável pelo Tratamento no que respeita à realização de avaliações de impacto sobre a proteção de dados e de segurança, à emissão de notificações de violações de dados e à realização de consultas prévias junto da autoridade de controlo competente, nos termos previstos na legislação aplicável em matéria de proteção de dados, tendo em conta a natureza do tratamento e a informação disponível para o Subcontratante.

3.6 Tendo em conta o estado da técnica, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento efetuado pelo Subcontratante ao abrigo do presente Acordo, bem como os riscos de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares, o Subcontratante aplicará as medidas técnicas e organizativas adequadas para proteger os Dados Pessoais

contra o tratamento não autorizado e ilícito, bem como contra a perda, alteração ou destruição acidentais.

3.7 Tais medidas incluirão, sempre que adequado e relevante para cada operação de tratamento:

i. a pseudonimização e a cifragem dos Dados Pessoais;

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

iii. a capacidade de restabelecer a disponibilidade e o acesso aos Dados Pessoais em tempo útil no caso de um incidente físico ou técnico;

iv. um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

3.8 Adicionalmente, o Subcontratante deverá, e garantirá que o seu pessoal irá:

i. fornecer prontamente ao Responsável pelo Tratamento toda a informação que este possa exigir para lhe permitir cumprir as suas obrigações relativas aos direitos dos titulares dos dados, incluindo os direitos de acesso, ou a notificações e pedidos endereçados por quaisquer autoridades de proteção de dados;

ii. garantir que as pessoas autorizadas a tratar os Dados Pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a uma obrigação legal adequada de confidencialidade; e

iii. notificar prontamente o Responsável pelo Tratamento de quaisquer consultas ou pedidos da parte dos titulares dos dados, do provedor de proteção de dados ou de qualquer outra autoridade reguladora ou de aplicação da lei.

4. TRANSFERÊNCIA DE DADOS PESSOAIS PARA FORA DO EEE

4.1 Os Dados Pessoais não serão transferidos para fora do Espaço Económico Europeu sem o consentimento prévio por escrito do Responsável pelo Tratamento, a menos que o terceiro esteja vinculado ou aceite vincular-se às Cláusulas Contratuais-Tipo (CCT) ou que a transferência se enquadre nos casos especificados no presente Acordo, em particular na cláusula 4.2.

4.2 O Responsável pelo Tratamento fica igualmente informado e concede autorização para que o Subcontratante transfira Dados Pessoais para fora da União Europeia ou do Espaço Económico Europeu, com o fim de cumprir os termos e as obrigações do presente Acordo. Em tais casos, o Subcontratante compromete-se pelo presente a garantir um elevado nível de proteção para as transferências de Dados Pessoais para fora da UE/EEE, incluindo, conforme adequado, nos acordos relevantes, as cláusulas-tipo para a transferência internacional de dados estabelecidas na Decisão de Execução (UE) 2021/914 da Comissão, ou através da aplicação de outra garantia adequada nos termos da Regulamentação de Proteção de Dados.

4.3 Qualquer cláusula do presente Acordo que resulte na privação do efeito das cláusulas-tipo referidas na cláusula 4.2 supra como garantias adequadas nos termos do Artigo 46.º do RGPD não será aplicável na medida em que produza esse efeito.

5. AUDITORIAS

5.1 Nos termos da Cláusula 8.9 das CCT, as Partes acordam nas seguintes modalidades para o exercício dos direitos de auditoria ao abrigo do presente Acordo:

i. para a realização de uma auditoria ao abrigo do presente Acordo, as Partes recorrerão apenas a auditores independentes que deverão assinar um acordo de confidencialidade com o Subcontratante;

ii. a auditoria não envolverá o acesso às instalações ou aos sistemas de informação do Subcontratante e será realizada exclusivamente sob a forma documental;

iii. a auditoria poderá ser realizada no máximo uma vez por ano, mediante notificação por escrito ao Subcontratante com antecedência mínima de trinta (30) dias de calendário em relação à data de início prevista para a auditoria;

iv. todos os custos de qualquer auditoria dessa natureza serão integralmente suportados pelo Responsável pelo Tratamento; e

v. qualquer auditoria realizada pelo Responsável pelo Tratamento não limitará, de forma alguma, as obrigações e a responsabilidade do Subcontratante ao abrigo do presente Acordo.

5.2 Nada no presente Artigo será interpretado como limitando ou restringindo os direitos do Responsável pelo Tratamento ao abrigo da Cláusula 8.9 das CCT. Os procedimentos previstos no presente Artigo constituem as modalidades práticas através das quais esses direitos serão ordinariamente exercidos.

6. VIOLAÇÕES

6.1 O Subcontratante notificará o Responsável pelo Tratamento sem demora injustificada, mas o mais tardar no prazo de setenta e duas (72) horas após ter tido conhecimento de qualquer violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a Dados Pessoais tratados por conta do Responsável pelo Tratamento («**Violação**»). Sempre que o Subcontratante tiver motivos razoáveis para crer que ocorreu uma tal Violação, deverá informar o Responsável pelo Tratamento em conformidade. O Subcontratante não notificará qualquer autoridade de controlo nem qualquer titular dos dados sobre uma Violação em nome do Responsável pelo Tratamento, salvo se por este instruído por escrito ou se a tal for obrigado pela legislação aplicável.

6.2 O Subcontratante prestará ao Responsável pelo Tratamento todas as informações relevantes relacionadas com a violação. A notificação da Violação efetuada pelo Subcontratante ao Responsável pelo Tratamento incluirá, pelo menos, o seguinte:

i. uma descrição da natureza da Violação e das informações por ela afetadas;

ii. o nome e os dados de contacto do ponto de contacto do Subcontratante onde possam ser obtidas mais informações;

iii. uma descrição das medidas adotadas pelo Subcontratante para aplicar à Violação, incluindo, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

6.3 O Subcontratante documentará todas as Violações, incluindo os factos relacionados com cada Violação, os seus efeitos e as medidas corretivas adotadas.

7. RECURSO A TERCEIROS NO TRATAMENTO DE DADOS

7.1 **Autorização geral.** O Responsável pelo Tratamento concede a sua autorização geral para que o Subcontratante envolva empresas afiliadas do Subcontratante e outros subcontratados como subcontratantes ulteriores para o tratamento de Dados Pessoais no âmbito dos Serviços («**Subcontratantes Ulteriores**»), desde que tal designação não resulte no incumprimento de qualquer legislação aplicável ou das obrigações do Subcontratante ao abrigo do presente Acordo. O Subcontratante manterá uma lista dos Subcontratantes Ulteriores por si utilizados no Livro Branco do RGPD de Ajax (Perguntas Frequentes) em https://ajax.systems/gdpr-white-paper/. O Subcontratante garantirá que os Subcontratantes Ulteriores envolvidos possuem a qualificação adequada e estão contratualmente vinculados a obrigações de proteção de dados não menos protetoras do que as estipuladas no presente Acordo, seja através de um acordo de tratamento de dados ou de outra documentação contratual vinculativa.

7.2 **Alteração de Subcontratante Ulterior.** Nos termos da Cláusula 9.ª das CCT constantes do Apêndice 1, a obrigação do Subcontratante de informar o Responsável pelo Tratamento sobre a adição ou substituição de um Subcontratante Ulterior é cumprida através da atualização da lista de Subcontratantes Ulteriores publicada no Livro Branco do RGPD de Ajax (Perguntas Frequentes) em https://ajax.systems/gdpr-white-paper/, bem como mediante notificação enviada ao Responsável pelo Tratamento por correio eletrónico para o endereço registado na sua conta e/ou através de uma notificação nos Produtos e Software Ajax. A referida notificação será enviada com, pelo menos, cinco (5) dias úteis de antecedência relativamente ao início do tratamento de Dados Pessoais pelo novo Subcontratante Ulterior ou pelo seu substituto ao abrigo do presente Acordo. O Responsável pelo Tratamento poderá opor-se a essa alteração dentro desse prazo, mediante notificação por escrito ao Subcontratante. Se nenhuma oposição for recebida antes do termo desse prazo, considerar-se-á que a alteração foi aceite.

8. APAGAMENTO E DEVOLUÇÃO DE DADOS PESSOAIS

8.1 Após a cessação ou caducidade do Acordo de Utilizador Final, o encerramento da conta do Responsável pelo Tratamento ou mediante pedido deste, o Subcontratante, à escolha do Responsável pelo Tratamento, apagará ou devolverá a este todos os Dados Pessoais tratados por sua conta e apagará as cópias existentes, salvo se a legislação aplicável exigir a sua conservação posterior. O Responsável pelo Tratamento poderá alterar a sua escolha a qualquer momento antes do termo da prestação dos Serviços, mediante notificação por escrito ao Subcontratante.

8.2 Caso o Responsável pelo Tratamento não tenha comunicado a sua escolha nos termos da cláusula 8.1 no prazo de trinta (30) dias de calendário após o evento relevante, o Subcontratante apagará os Dados Pessoais.

8.3 O apagamento dos sistemas de produção em tempo real do Subcontratante será concluído no prazo de trinta (30) dias de calendário a contar da data do pedido relevante ou do evento referido na cláusula 8.1, consoante aplicável.

8.4 Os Dados Pessoais poderão permanecer em cópias de segurança encriptadas após o apagamento nos termos da cláusula 8.3 durante o ciclo de retenção de cópias de segurança do Subcontratante, o qual não excede doze (12) meses. Durante esse período, esses Dados Pessoais não serão tratados para qualquer outro fim, o acesso aos mesmos será restrito e os mesmos serão apagados definitivamente após o termo do ciclo de cópias de segurança aplicável. Em caso de restauro a partir de uma cópia de segurança, o Subcontratante removerá os Dados Pessoais dos Responsáveis pelo Tratamento cujos dados tenham sido previamente apagados antes de os dados restaurados serem utilizados em produção.

8.5 Até que o apagamento ou a devolução estejam concluídos, o Subcontratante continuará a assegurar o cumprimento do presente Acordo no que respeita aos Dados Pessoais em causa.

8.6 O Subcontratante confirmará por escrito ao Responsável pelo Tratamento, a pedido deste, que o apagamento foi concluído.

8.7 Caso a legislação aplicável exija que o Subcontratante conserve os Dados Pessoais para além dos prazos previstos na presente Secção, o Subcontratante informará o Responsável pelo Tratamento desse requisito, salvo se for proibido por lei de o fazer, e tratará os Dados Pessoais conservados apenas na medida e pelo tempo estritamente necessários.

9. CESSAÇÃO E DISPOSIÇÕES DIVERSAS

9.1 O presente Acordo entra em vigor simultaneamente com o Acordo de Utilizador Final e constitui

parte integrante do mesmo a partir da data em que o Responsável pelo Tratamento aceitar o Acordo do Utilizador Final em https://ajax.systems/end-user-agreement/. O presente Acordo manter-se-á em vigor até que o Subcontratante tenha cessado o tratamento de Dados Pessoais com base nos Serviços ou em qualquer acordo celebrado entre as Partes e tenha cumprido as obrigações relativas à conclusão do tratamento, salvo acordo em contrário por escrito entre as Partes.

9.2 A cessação ou caducidade do presente Acordo não exonera as Partes de qualquer obrigação de confidencialidade nem de quaisquer outras responsabilidades ao abrigo do mesmo.

9.3 Ajax poderá alterar o presente Acordo mediante a publicação de uma versão atualizada no sítio Web de Ajax, por notificação por correio eletrónico ou através de notificação nos Produtos e/ou aplicações móveis. A utilização continuada dos Produtos ou do Software após a referida notificação constitui aceitação do Acordo alterado. Este direito de alteração não se estende às Cláusulas Contratuais-Tipo do Apêndice 1, as quais apenas poderão ser atualizadas nos termos permitidos pelas referidas Cláusulas.

10. LEI APLICÁVEL E RESOLUÇÃO DE LITÍGIOS

10.1 O presente Acordo, incluindo todos os seus aditamentos, anexos e demais partes integrantes, será regido e interpretado de acordo com a legislação da República da Polónia.

10.2 As Partes concordam igualmente em cumprir a Legislação aplicável em matéria de proteção de dados relativa ao tratamento de Dados Pessoais.

10.3 «Legislação aplicável em matéria de proteção de dados» designa a legislação sobre o tratamento de dados pessoais em vigor a cada momento, incluindo o Regulamento Geral sobre a Proteção de Dados (UE) 2016/679; a Lei de Proteção de Dados do Reino Unido de 2018; a Diretiva relativa à Privacidade e às Comunicações Eletrónicas 2002/58/CE (conforme atualizada pela Diretiva 2009/136/CE); os Regulamentos de Privacidade e Comunicações Eletrónicas de 2003 (SI 2003/2426), conforme alterados; e qualquer outra legislação do EEE relativa a dados pessoais, bem como toda a restante legislação e requisitos regulamentares em vigor a cada momento que se apliquem às Partes no que diz respeito à utilização de Dados Pessoais (incluindo, sem limitação, a privacidade das comunicações eletrónicas), consoante o território em que os Produtos e Software são fornecidos.

10.4 Qualquer litígio, controvérsia ou reclamação decorrente do presente Acordo ou de algum modo com ele relacionado, bem como relativo à sua interpretação, exequibilidade, execução, violação, cessação ou validade, será resolvido pelos tribunais da Polónia (Varsóvia), salvo disposição em contrário da Legislação aplicável em matéria de proteção de dados. O idioma do processo será o inglês.

10.5 As Partes concordam irrevogavelmente que os tribunais da República da Polónia terão jurisdição exclusiva para resolver quaisquer litígios que possam surgir de ou em relação ao Acordo, incluindo, entre outros, litígios relativos à sua execução, existência, validade, interpretação, cessação ou consequências resultantes. Assim, qualquer ação ou processo judicial decorrente do presente Acordo ou com ele relacionado, assente em responsabilidade contratual ou extracontratual, será intentado exclusivamente perante os tribunais da República da Polónia. Caso o Responsável pelo Tratamento seja uma pessoa singular que atue como Utilizador Final Individual (conforme definido no Acordo do Utilizador Final), o Responsável pelo Tratamento poderá também intentar processos perante os tribunais do seu país de residência habitual.

CLÁUSULAS CONTRATUAIS-TIPO

SECÇÃO I

Cláusula 1

Finalidade e âmbito de aplicação

(a) As presentes cláusulas contratuais-tipo visam assegurar o cumprimento dos requisitos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados) aplicáveis às transferências de dados pessoais para países terceiros.

(b) As Partes:

(i) a(s) pessoa(s) singular(es) ou coletiva(s), a(s) autoridade(s) pública(s), a(s) agência(s) ou outro(s) organismo(s) (adiante designado(s) por «entidade(s)») que transfere(m) os dados pessoais, tal como enumerados no anexo 1 (a seguir designado(s) individualmente por «exportador de dados»), e

(ii) a(s) entidade(s) de um país terceiro que recebe(m) os dados pessoais do exportador de dados, direta ou indiretamente através de outra entidade também Parte nas presentes CCT, tal como enumeradas no anexo 1 (a seguir designada(s) individualmente por «importador de dados»)

acordaram nas presentes cláusulas contratuais-tipo (a seguir designadas por «cláusulas»).

(c) As presentes CCT são aplicáveis no que diz respeito à transferência de dados pessoais, conforme especificado no anexo 1.

(d) O apêndice das presentes CCT, que contém os anexos nelas referidos, é parte integrante das presentes CCT.

Cláusula 2

Efeito e invariabilidade das cláusulas

(a) As presentes CCT estabelecem garantias adequadas, incluindo direitos oponíveis dos titulares dos dados e medidas jurídicas corretivas eficazes, nos termos do artigo 46.°, n.° 1, e do artigo 46.°, n.° 2, alínea (c), do Regulamento (UE) 2016/679 e, no que diz respeito às transferências de dados de responsáveis pelo tratamento para subcontratantes e/ou entre subcontratantes, nos termos do artigo 28.°, n.° 7, do Regulamento (UE) 2016/679, desde que não sejam alteradas, exceto para selecionar o(s) módulo(s) adequado(s) ou para acrescentar ou atualizar informações no apêndice. Tal não impede as Partes de incluir as cláusulas contratuais-tipo estabelecidas nas presentes CCT num contrato mais abrangente e/ou de acrescentar outras cláusulas ou garantias adicionais, desde que não colidam, direta ou indiretamente, com as presentes CCT, e sem prejuízo dos direitos ou das liberdades fundamentais dos titulares dos dados.

(b) As presentes CCT não prejudicam as obrigações a que o exportador de dados está sujeito por força do Regulamento (UE) 2016/679.

Cláusula 3

Cláusula do terceiro beneficiário

(a) Os titulares dos dados podem invocar e fazer aplicar as presentes CCT, enquanto terceiros beneficiários, contra o exportador e/ou importador de dados, com as seguintes exceções:

(i) Cláusulas 1, 2, 3, 6, 7,

(ii) Cláusula 8: Cláusula 8.1, alínea (b), Cláusula 8.9, alíneas (a), (c), (d) e (e),

(iii) Cláusula 9: Cláusula 9, alíneas (a), (c), (d) e (e),

(iv) Cláusula 12: Cláusula 12, alíneas (a), (d) e (f),

(v) Cláusula 13,

(vi) Cláusula 15.1, alíneas (c), (d) e (e),

(vii) Cláusula 16, alínea (e),

(viii) Cláusula 18: Cláusula 18, alíneas (a) e (b).

(b) A alínea (a) não prejudica os direitos dos titulares dos dados ao abrigo do Regulamento (UE) 2016/679.

Cláusula 4

Interpretação

(a) Caso as presentes CCT utilizem termos que se encontram definidos no Regulamento (UE) 2016/679, esses termos têm o mesmo significado que lhes é atribuído nesse regulamento.

(b) As presentes CCT devem ser lidas e interpretadas à luz das disposições do Regulamento (UE) 2016/679.

(c) As presentes CCT não devem ser interpretadas de forma contrária aos direitos e obrigações previstos no Regulamento (UE) 2016/679.

Cláusula 5

Hierarquia

Em caso de contradição entre as presentes CCT e as disposições de acordos conexos celebrados entre as Partes que se encontrem em vigor no momento em que as presentes CCT sejam acordadas ou que sejam celebrados posteriormente, prevalecem as presentes CCT.

Cláusula 6

Descrição da(s) transferência(s)

Os pormenores da(s) transferência(s) e, em particular, as categorias de dados pessoais que são transferidos e a(s) finalidade(s) para a(s) qual(is) são transferidos, são especificados no anexo 1.

Cláusula 7

Cláusula de adesão

Na Cláusula 7, a cláusula de adesão opcional não se aplica.

SECÇÃO II — OBRIGAÇÕES DAS PARTES

Cláusula 8

Garantias em matéria de proteção de dados

O exportador de dados garante que envidou esforços razoáveis para determinar que o importador de dados tem capacidade, através da aplicação de medidas técnicas e organizativas adequadas,

para cumprir as obrigações que lhe incumbem por força das presentes CCT.

8.1. Instruções

(a) O importador de dados deve proceder ao tratamento dos dados pessoais apenas mediante instruções documentadas do exportador de dados. O exportador de dados pode dar essas instruções ao longo do período de vigência do contrato.

(b) O importador de dados deve informar imediatamente o exportador de dados se não puder seguir essas instruções.

8.2. Limitação das finalidades

O importador de dados deve proceder ao tratamento dos dados pessoais apenas para a(s) finalidade(s) específica(s) da transferência, conforme estabelecido no anexo 1, salvo se receber instruções adicionais do exportador de dados.

8.3. Transparência

Mediante pedido, o exportador de dados deve disponibilizar gratuitamente ao titular dos dados uma cópia das presentes CCT, incluindo o apêndice, conforme preenchido pelas Partes. Na medida do necessário para proteger segredos comerciais ou outras informações confidenciais, incluindo as medidas descritas no anexo 2 e dados pessoais, o exportador de dados pode editar parte do texto do apêndice das presentes CCT antes de partilhar uma cópia do mesmo, mas deve disponibilizar um resumo significativo do apêndice se, de outro modo, o titular dos dados não for capaz de compreender o seu conteúdo ou exercer os seus direitos. Mediante pedido, as Partes devem comunicar ao titular dos dados os motivos das ocultações, na medida do possível sem revelar as informações ocultadas. Esta cláusula não prejudica as obrigações do exportador de dados nos termos dos artigos 13.° e 14.° do Regulamento (UE) 2016/679.

8.4. Exatidão

Se o importador de dados tomar conhecimento de que os dados pessoais que recebeu são inexatos ou estão desatualizados, deve informar o exportador de dados sem demora injustificada. Neste caso, o importador de dados deve cooperar com o exportador de dados para apagar ou retificar os dados.

8.5. Duração do tratamento e apagamento ou devolução dos dados

O tratamento pelo importador de dados só pode ocorrer durante o período especificado no anexo 1. Depois de concluída a prestação dos serviços de tratamento, o importador de dados deve, consoante a escolha do exportador de dados, apagar todos os dados pessoais tratados por conta deste último e certificar ao exportador de dados que o fez ou devolver ao exportador de dados todos os dados pessoais tratados por sua conta e apagar as cópias existentes. Até que os dados

sejam apagados ou devolvidos, o importador de dados deve continuar a assegurar o cumprimento das presentes CCT. Caso a legislação local aplicável ao importador de dados proíba a devolução ou o apagamento dos dados pessoais, o importador de dados garante continuar a assegurar o cumprimento das presentes CCT e só proceder ao tratamento dos dados pessoais em causa na medida em que e enquanto for necessário nos termos dessa legislação local. Tal não prejudica a Cláusula 14, em particular a exigência de o importador de dados, nos termos da Cláusula 14, alínea (e), notificar o exportador de dados ao longo do período de vigência do contrato se tiver motivos para crer que está ou ficou sujeito a legislações ou práticas não conformes com os requisitos da Cláusula 14, alínea (a).

8.6. Segurança do tratamento

(a) O importador de dados e, durante a transmissão, também o exportador de dados devem aplicar medidas técnicas e organizativas adequadas para garantir a segurança dos dados, incluindo a proteção contra uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizados a esses dados (a seguir designada por «violação de dados pessoais»). Ao avaliar o nível de segurança adequado, as Partes devem ter em devida conta as técnicas mais avançadas, os custos de aplicação, a natureza, o âmbito, o contexto e a(s) finalidade(s) do tratamento e os riscos inerentes ao tratamento para os titulares dos dados. As Partes devem, em particular, ponderar o recurso à cifragem ou à pseudonimização, nomeadamente durante a transmissão, sempre que a finalidade do tratamento possa ser cumprida dessa forma. Em caso de pseudonimização, as informações adicionais para a atribuição dos dados pessoais a um titular de dados específico devem permanecer, sempre que possível, sob o controlo exclusivo do exportador de dados. No cumprimento das obrigações que lhe incumbem por força do presente número, o importador de dados deve, pelo menos, aplicar as medidas técnicas e organizativas especificadas no anexo 2. O importador de dados deve realizar controlos regulares para garantir que estas medidas continuam a proporcionar um nível de segurança adequado.

(b) O importador de dados só deve conceder acesso aos dados pessoais aos membros do seu pessoal na medida estritamente necessária para a execução, a gestão e o acompanhamento do contrato. Deve assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas às obrigações legais de confidencialidade adequadas.

(c) Em caso de violação de dados pessoais relativa a dados pessoais tratados pelo importador de dados ao abrigo das presentes CCT, o importador de dados deve tomar as medidas adequadas para reparar a violação, incluindo medidas para atenuar os seus efeitos negativos. O importador de dados deve notificar igualmente o exportador de dados, sem demora injustificada, após ter tomado conhecimento da violação. Essa notificação deve conter os dados de um ponto de contacto onde possam ser obtidas mais informações, uma descrição da natureza da violação (incluindo, se possível, as categorias e o número aproximado de titulares de dados e de registos de dados pessoais em causa), as suas consequências prováveis e as medidas adotadas ou propostas para reparar a violação, incluindo, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos. Caso, e na medida em que, não seja possível comunicar todas as informações ao mesmo tempo, a notificação inicial deve conter as informações então disponíveis, devendo outras informações, à medida que fiquem disponíveis, ser fornecidas posteriormente sem demora injustificada.

(d) O importador de dados deve cooperar com o exportador de dados e prestar-lhe assistência para que este cumpra as obrigações que lhe incumbem nos termos do Regulamento (UE) 2016/679, em particular a obrigação de notificar a autoridade de controlo competente e os titulares de dados afetados, tendo em conta a natureza do tratamento e as informações ao dispor do importador de dados.

8.7. Dados sensíveis

Sempre que a transferência envolva dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, dados genéticos ou biométricos destinados a identificar uma pessoa singular de forma inequívoca, dados relativos à saúde, à vida sexual ou à orientação sexual de uma pessoa ou dados relacionados com condenações penais e com infrações (a seguir designados por «dados sensíveis»), o importador de dados deve aplicar as limitações específicas e/ou garantias adicionais descritas no anexo 1.

8.8. Transferências ulteriores

O importador de dados só deve divulgar os dados pessoais a terceiros mediante instruções documentadas do exportador de dados. Além disso, os dados só podem ser divulgados a terceiros localizados fora da União Europeia (no mesmo país que o importador de dados ou noutro país terceiro, a seguir designada «transferência ulterior») se o terceiro estiver ou aceitar estar vinculado pelas presentes CCT, ao abrigo do módulo adequado, ou se:

(i) o destino da transferência ulterior for um país que beneficie de uma decisão de adequação nos termos do artigo 45.° do Regulamento (UE) 2016/679 que abranja a transferência ulterior,

(ii) o terceiro assegurar, de qualquer outra forma, as garantias adequadas nos termos dos artigos 46.° ou 47.° do Regulamento (UE) 2016/679 no que diz respeito ao tratamento em questão,

(iii) a transferência ulterior for necessária à declaração, ao exercício ou à defesa de um direito num processo judicial no contexto de processos administrativos, regulamentares ou judiciais específicos, ou

(iv) a transferência ulterior for necessária para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular.

Qualquer transferência ulterior está sujeita ao cumprimento, pelo importador de dados, de todas as outras garantias previstas nas presentes CCT, em particular a limitação da finalidade.

8.9. Documentação e cumprimento

(a) O importador de dados deve responder, rápida e adequadamente, aos pedidos de informação do exportador de dados relacionados com o tratamento ao abrigo das presentes CCT.

(b) As Partes devem poder demonstrar o cumprimento das presentes CCT. Em particular, o importador de dados deve conservar documentação adequada sobre as atividades de tratamento realizadas por conta do exportador de dados.

(c) O importador de dados deve disponibilizar ao exportador de dados todas as informações necessárias para demonstrar o cumprimento das obrigações previstas nas presentes CCT e, a pedido deste último, facilitar e contribuir para as auditorias das operações de tratamento abrangidas pelas presentes CCT, a intervalos razoáveis ou se houver indícios de incumprimento. Ao decidir sobre uma revisão ou auditoria, o exportador de dados pode ter em conta as certificações pertinentes detidas pelo importador de dados.

(d) O exportador de dados pode optar por realizar, ele próprio, a auditoria ou mandatar um auditor independente. As auditorias podem incluir inspeções nos edifícios ou nas instalações físicas do importador de dados, devendo, se for caso disso, ser realizadas com uma antecedência razoável.

(e) As Partes devem disponibilizar as informações referidas nas alíneas (b) e (c), incluindo os resultados de quaisquer auditorias, à autoridade de controlo competente, mediante pedido.

Cláusula 9

Recurso a subcontratantes ulteriores

(a) O importador de dados tem a autorização geral do exportador de dados para a contratação de (um) subcontratante(s) ulterior(es) a partir de uma lista acordada. O importador de dados deve informar especificamente o exportador de dados, por escrito, das alterações pretendidas a efetuar a essa lista quanto ao aumento do número ou à substituição de subcontratantes ulteriores com uma antecedência mínima de cinco (5) dias úteis, dando assim ao exportador de dados tempo suficiente para se opor a essas alterações antes da contratação do(s) subcontratante(s) ulterior(es). O importador de dados deve fornecer ao exportador de dados as informações necessárias para que este último possa exercer o seu direito de oposição.

(b) Se o importador de dados contratar um subcontratante ulterior para realizar operações específicas de tratamento (por conta do exportador de dados), deve fazê-lo através de um contrato escrito que preveja, do ponto de vista material, as mesmas obrigações em matéria de proteção de dados que as que incumbem ao importador de dados por força das presentes CCT, incluindo em termos de direitos de terceiro beneficiário para os titulares dos dados. As Partes concordam que, ao cumprir esta Cláusula, o importador de dados cumpre as obrigações que lhe incumbem por força da Cláusula 8.8. O importador de dados deve garantir que o subcontratante ulterior cumpre as obrigações a que o importador de dados está sujeito nos termos das presentes CCT.

(c) O importador de dados deve facultar ao exportador de dados, a pedido do mesmo, uma cópia do referido acordo de subcontratação e de quaisquer alterações subsequentes. Na medida do necessário para proteger segredos comerciais ou outras informações confidenciais, incluindo dados pessoais, o importador de dados pode editar o texto do acordo antes de partilhar uma cópia.

(d) O importador de dados continua a ser inteiramente responsável, perante o exportador de dados, pelo cumprimento das obrigações que incumbem ao subcontratante ulterior por força do seu contrato com o importador de dados. O importador de dados deve notificar o exportador de dados de qualquer incumprimento, pelo subcontratante ulterior, das obrigações que lhe incumbem por força desse contrato.

(e) O importador de dados deve acordar com o subcontratante ulterior uma cláusula do terceiro beneficiário nos termos da qual — em caso de desaparecimento de facto, de extinção legal ou de insolvência do importador de dados — o exportador de dados tem o direito de rescindir o contrato do subcontratante ulterior e de dar instruções ao subcontratante ulterior para apagar ou devolver os dados pessoais.

Cláusula 10

Direitos dos titulares dos dados

(a) O importador de dados deve notificar imediatamente o exportador de dados de qualquer pedido que tenha recebido de um titular de dados. Não pode responder ele próprio a esse pedido, salvo se tiver sido autorizado pelo exportador de dados.

(b) O importador de dados deve prestar assistência ao exportador de dados no cumprimento das suas obrigações de resposta aos pedidos dos titulares dos dados respeitantes ao exercício dos seus direitos ao abrigo do Regulamento (UE) 2016/679. Neste contexto, as Partes devem estabelecer, no anexo 2, as medidas técnicas e organizativas adequadas, tendo em conta a natureza do tratamento, através das quais a assistência deve ser prestada, bem como o âmbito e a amplitude da assistência necessária.

(c) No cumprimento das obrigações que lhe incumbem por força das alíneas (a) e (b), o importador de dados deve cumprir as instruções do exportador de dados.

Cláusula 11

Recurso

(a) O importador de dados deve informar os titulares dos dados, de forma transparente e de fácil acesso, através de uma notificação individual ou no seu sítio Web, de um ponto de contacto autorizado a tratar as reclamações. Deve tratar imediatamente quaisquer reclamações que receba de um titular de dados.

(b) Em caso de litígio entre um titular dos dados e uma das Partes quanto ao cumprimento das presentes CCT, essa Parte deve envidar todos os esforços para resolver a questão de forma amigável e atempada. As Partes devem manter-se mutuamente informadas sobre esses litígios e, quando adequado, cooperar na sua resolução.

(c) Se o titular dos dados invocar um direito de terceiro beneficiário nos termos da Cláusula 3, o importador de dados deve aceitar a decisão do titular dos dados de:

(i) apresentar uma reclamação à autoridade de controlo no Estado-Membro da sua residência habitual ou do seu local de trabalho ou à autoridade de controlo competente, nos termos da Cláusula 13,

(ii) submeter o litígio à apreciação dos tribunais competentes na aceção da Cláusula 18.

(d) As Partes aceitam que o titular dos dados possa ser representado por um organismo, organização ou associação sem fins lucrativos, nas condições estabelecidas no artigo 80.°, n.° 1, do Regulamento (UE) 2016/679.

(e) O importador de dados deve acatar uma decisão vinculativa nos termos do direito da UE ou dos Estados-Membros aplicável.

(f) O importador de dados acorda que a opção do titular dos dados não prejudica os direitos materiais e processuais do mesmo de obter reparação em conformidade com a legislação aplicável.

Cláusula 12

Responsabilidade

(a) Cada Parte é responsável perante a(s) outra(s) Parte(s) por quaisquer danos que lhe(s) cause decorrentes de qualquer violação das presentes CCT.

(b) O importador de dados é responsável perante o titular dos dados, tendo o titular dos dados o direito de receber uma indemnização, por quaisquer danos materiais ou imateriais que o importador de dados ou o seu subcontratante ulterior cause ao titular dos dados em consequência da violação dos direitos de terceiro beneficiário ao abrigo das presentes CCT.

(c) Não obstante o disposto na alínea (b), o exportador de dados é responsável perante o titular dos dados, tendo o titular dos dados o direito de receber uma indemnização, por quaisquer danos materiais ou imateriais que o exportador ou o importador de dados (ou o seu subcontratante ulterior) cause ao titular dos dados em consequência da violação dos direitos de terceiro beneficiário ao abrigo das presentes CCT. Tal não prejudica a responsabilidade do exportador de dados e, se este for um subcontratante que atue por conta de um responsável pelo tratamento, a responsabilidade do responsável pelo tratamento nos termos do Regulamento (UE) 2016/679 ou do Regulamento (UE) 2018/1725, consoante o caso.

(d) As Partes acordam que, se o exportador de dados for considerado responsável, nos termos da alínea (c), por danos causados pelo importador de dados (ou pelo seu subcontratante), tem o direito de reclamar ao importador de dados a parte da indemnização correspondente à responsabilidade do importador de dados pelos danos.

(e) Quando mais de uma Parte for responsável por quaisquer danos causados ao titular dos dados devido a uma violação das presentes CCT, todas as Partes responsáveis são solidariamente responsáveis e o titular dos dados tem o direito de intentar uma ação em tribunal contra qualquer uma destas Partes.

(f) As Partes acordam que, se uma Parte for considerada responsável nos termos da alínea (e), tem o direito de reclamar à(s) outra(s) Parte(s) a parte da indemnização correspondente à sua responsabilidade pelos danos.

(g) O importador de dados não pode invocar o comportamento de um subcontratante ulterior para se isentar da sua própria responsabilidade.

Cláusula 13

Controlo

(a) A autoridade de controlo com a responsabilidade de assegurar o cumprimento, pelo exportador de dados, do Regulamento (UE) 2016/679 no que diz respeito à transferência de dados, conforme indicado no anexo 1, deve agir como autoridade de controlo competente.

(b) O importador de dados aceita submeter-se à jurisdição da autoridade de controlo competente e cooperar com a mesma em quaisquer procedimentos destinados a assegurar o cumprimento das presentes CCT. Em particular, o importador de dados concorda em responder a pedidos de informação, submeter-se a auditorias e cumprir as medidas adotadas pela autoridade de controlo, incluindo medidas corretivas e compensatórias. Deve fornecer à autoridade de controlo uma confirmação escrita de que foram tomadas as medidas necessárias.

SECÇÃO III — LEGISLAÇÃO LOCAL E OBRIGAÇÕES EM CASO DE ACESSO POR PARTE DE AUTORIDADES PÚBLICAS

Cláusula 14

Legislação e práticas locais que afetam o cumprimento das CCT

(a) As Partes garantem que não têm motivos para crer que a legislação e as práticas do país terceiro de destino aplicáveis ao tratamento dos dados pessoais pelo importador de dados, incluindo quaisquer requisitos de divulgação de dados pessoais ou medidas destinadas a autorizar o acesso de autoridades públicas, impedem o importador de dados de cumprir as obrigações que lhe incumbem por força das presentes CCT. Tal baseia-se no entendimento de que a legislação e as práticas que respeitem a essência dos direitos e das liberdades fundamentais e não excedam o necessário e proporcional numa sociedade democrática para salvaguardar um dos objetivos enumerados no artigo 23.°, n.° 1, do Regulamento (UE) 2016/679 não são contrárias ao disposto nas presentes CCT.

(b) As Partes declaram que, ao apresentar a garantia referida na alínea (a), tiveram em devida conta, em especial, os seguintes elementos:

(i) as circunstâncias específicas da transferência, incluindo a extensão da cadeia de tratamento, o número de intervenientes envolvidos e os canais de transmissão utilizados; transferências ulteriores previstas; o tipo de destinatário; a finalidade do tratamento; as categorias e o formato dos dados pessoais transferidos; o setor económico em que a transferência ocorre; o local de conservação dos dados transferidos,

(ii) a legislação e as práticas do país terceiro de destino – nomeadamente as que exigem a divulgação de dados às autoridades públicas ou autorizam o acesso por parte dessas autoridades – pertinentes à luz das circunstâncias específicas da transferência e as limitações e garantias aplicáveis[1],

(iii)quaisquer garantias contratuais, técnicas ou organizativas pertinentes aplicadas para complementar as garantias previstas nas presentes CCT, incluindo as medidas aplicadas durante a transmissão e ao tratamento dos dados pessoais no país de destino.

[1] No que diz respeito ao impacto das legislações e práticas em questão no cumprimento das presentes CCT, podem ser tidos em consideração diferentes elementos no âmbito de uma avaliação global. Esses elementos podem incluir a experiência prática pertinente e documentada com casos anteriores de pedidos de divulgação por parte de autoridades públicas, ou a ausência de tais pedidos, abrangendo um intervalo de tempo suficientemente representativo. Tal refere-se, em particular, a registos internos ou outra documentação, elaborados numa base contínua de acordo com a diligência devida e certificados a nível dos quadros superiores, desde que esta informação possa ser legalmente partilhada com terceiros. Sempre que esta experiência prática seja utilizada para concluir que o importador de dados não será impedido de cumprir as presentes CCT, é necessário que seja apoiada por outros elementos pertinentes e objetivos, e cabe às Partes ponderar cuidadosamente se estes elementos, em conjunto, têm peso suficiente, em termos da sua fiabilidade e representatividade, para apoiar esta conclusão. Em particular, as Partes têm de ter em conta se a sua experiência prática é corroborada e não contrariada por informações fiáveis, acessíveis ao público ou, de outro modo, acessíveis, sobre a existência ou a ausência de pedidos no mesmo setor e/ou a aplicação da legislação na prática, como a jurisprudência e relatórios de organismos de supervisão independentes.

(c) O importador de dados garante que, ao efetuar a avaliação nos termos da alínea (b), envidou todos os esforços para fornecer ao exportador de dados informações pertinentes e acorda que continuará a cooperar com o exportador de dados no sentido de assegurar o cumprimento das presentes CCT.

(d) As Partes acordam em documentar a avaliação prevista na alínea (b) e disponibilizá-la à autoridade de controlo competente, mediante pedido.

(e) O importador de dados acorda em notificar imediatamente o exportador de dados se, depois de ter subscrito as presentes CCT e durante a vigência do contrato, tiver motivos para crer que está ou ficou sujeito a legislações ou práticas não conformes com os requisitos da alínea (a), nomeadamente na sequência de uma alteração da legislação do país terceiro ou de uma medida (como um pedido de divulgação) que indique uma aplicação dessa legislação na prática que não esteja em consonância com os requisitos da alínea (a).

(f) Na sequência de uma notificação nos termos da alínea (e), ou se o exportador de dados tiver motivos para crer que o importador de dados já não é capaz de cumprir as obrigações que lhe incumbem por força das presentes CCT, o exportador de dados deve identificar imediatamente as medidas adequadas (por exemplo, medidas técnicas ou organizativas para garantir a segurança e a confidencialidade) a adotar pelo exportador e/ou importador de dados para resolver a situação. O exportador de dados deve suspender a transferência de dados se considerar que não podem ser asseguradas garantias adequadas para essa transferência ou se receber instruções da autoridade de controlo competente nesse sentido. Neste caso, o exportador de dados tem o direito de rescindir o contrato, na medida em que este diga respeito ao tratamento de dados pessoais ao abrigo das presentes CCT. Se o contrato envolver mais de duas Partes, o exportador de dados só pode exercer este direito de rescisão em relação à Parte pertinente, salvo decisão das Partes em contrário. Se o contrato for rescindido nos termos da presente Cláusula, aplica-se a Cláusula 16, alíneas (d) e (e).

Cláusula 15

Obrigações do importador de dados em caso de acesso por parte de autoridades públicas

15.1. Notificação

(a) O importador de dados acorda em notificar imediatamente o exportador de dados e, se possível, o titular dos dados (se necessário, com a ajuda do exportador de dados) se:

(i) receber um pedido juridicamente vinculativo de uma autoridade pública, incluindo autoridades judiciárias, ao abrigo da legislação do país de destino para a divulgação dos dados pessoais transferidos nos termos das presentes CCT; esta notificação deve incluir informações sobre os dados pessoais solicitados, a autoridade requerente, o fundamento jurídico do pedido e a resposta fornecida, ou

(ii) tomar conhecimento de qualquer acesso direto das autoridades públicas aos dados pessoais transferidos nos termos das presentes CCT, em conformidade com a legislação do país terceiro de destino; esta notificação deve incluir todas as informações de que o importador disponha.

(b) Se o importador de dados estiver proibido de notificar o exportador de dados e/ou o titular dos dados por força da legislação do país de destino, o importador de dados acorda em envidar todos os esforços para obter uma derrogação da proibição com vista a comunicar, o mais rapidamente possível, o maior número possível de informações. O importador de dados aceita documentar todos os seus esforços a fim de poder comprová-los a pedido do exportador de dados.

(c) Quando tal for permitido pela legislação do país de destino, o importador de dados aceita fornecer periodicamente ao exportador de dados, durante a vigência do contrato, o maior número possível de informações pertinentes sobre os pedidos recebidos (em particular, o número de pedidos, o tipo de dados solicitados, a(s) autoridade(s)/entidade(s) requerente(s), se os pedidos foram contestados e o resultado dessas contestações, etc.).

(d) O importador de dados aceita conservar as informações nos termos das alíneas (a) a (c) durante a vigência do contrato e em disponibilizá-las à autoridade de controlo competente, mediante pedido.

(e) As alíneas (a) a (c) não prejudicam a obrigação que incumbe ao importador de dados, nos termos da Cláusula 14, alínea (e), e da Cláusula 16, de informar imediatamente o exportador de dados se não puder cumprir as presentes CCT.

15.2. Controlo da legalidade e minimização dos dados

(a) O importador de dados aceita controlar a legalidade do pedido de divulgação, em particular a questão de saber se este se mantém nos limites dos poderes concedidos à autoridade pública requerente, e em contestar o pedido se, após uma avaliação minuciosa, concluir que existem fundamentos razoáveis para considerar que o pedido é ilegal nos termos da legislação do país de destino, das obrigações aplicáveis ao abrigo do direito internacional e dos princípios de cortesia internacional. O importador de dados deve, nas mesmas condições, explorar as possibilidades de recurso. Ao contestar um pedido, o importador de dados deve procurar medidas provisórias com vista a suspender os efeitos do pedido até que a autoridade judiciária competente tenha decidido sobre o seu mérito. O importador de dados não pode divulgar os dados pessoais solicitados até que seja obrigado a fazê-lo ao abrigo das regras processuais aplicáveis. Estes requisitos não prejudicam as obrigações que incumbem ao importador de dados nos termos da Cláusula 14, alínea (e).

(b) O importador de dados aceita documentar a sua avaliação jurídica e qualquer contestação do pedido de divulgação e, na medida do permitido pela legislação do país de destino, disponibilizar a documentação ao exportador de dados. Deve igualmente disponibilizá-la à autoridade de controlo competente, mediante pedido.

(c) O importador de dados aceita fornecer a quantidade mínima de informação admissível ao responder a um pedido de divulgação, com base numa interpretação razoável do pedido.

SECÇÃO IV — DISPOSIÇÕES FINAIS

Cláusula 16

Incumprimento das CCT e rescisão

(a) O importador de dados deve informar imediatamente o exportador de dados se, por qualquer motivo, não puder cumprir as presentes CCT.

(b) Se o importador de dados violar ou não puder cumprir as presentes CCT, o exportador de dados deve suspender a transferência de dados pessoais para o importador de dados até que o cumprimento seja novamente assegurado ou o contrato seja rescindido. Esta disposição não prejudica o disposto na Cláusula 14, alínea (f).

(c) O exportador de dados tem o direito de rescindir o contrato, na medida em que este diga respeito ao tratamento de dados pessoais ao abrigo das presentes CCT, caso:

(i) o exportador de dados tenha suspendido a transferência de dados pessoais para o importador de dados nos termos da alínea (b) e o cumprimento das presentes CCT não for restabelecido num prazo razoável e, em todo o caso, no prazo de um mês a contar da suspensão,

(ii) o importador de dados viole, de forma substancial ou persistente, as presentes CCT, ou

(iii) o importador de dados não cumpra uma decisão vinculativa de um tribunal ou autoridade de controlo competente relativamente às obrigações que lhe incumbem por força das presentes CCT.

Nestes casos, deve informar a autoridade de controlo competente desse incumprimento. Se o contrato envolver mais de duas Partes, o exportador de dados só pode exercer este direito de rescisão em relação à Parte pertinente, salvo decisão das Partes em contrário.

(d) Os dados pessoais que tenham sido transferidos antes da rescisão do contrato nos termos da alínea (c) devem, consoante a escolha do exportador de dados, ser imediatamente devolvidos ao exportador de dados ou apagados na sua totalidade. O mesmo se aplica a quaisquer cópias dos dados. O importador de dados deve certificar o apagamento dos dados ao exportador de dados. Até que os dados sejam apagados ou devolvidos, o importador de dados deve continuar a assegurar o cumprimento das presentes CCT. Caso a legislação local aplicável ao importador de dados proíba a devolução ou o apagamento dos dados pessoais transferidos, o importador de dados garante continuar a assegurar o cumprimento das presentes CCT e só proceder ao tratamento dos dados na medida em que e enquanto for necessário nos termos dessa legislação local.

(e) Qualquer das Partes pode revogar o seu consentimento em ficar vinculada pelas presentes CCT se (i) a Comissão Europeia adotar uma decisão nos termos do artigo 45.°, n.° 3, do Regulamento (UE) 2016/679 que abranja a transferência de dados pessoais a que se aplicam as presentes CCT; ou (ii) o Regulamento (UE) 2016/679 se tornar parte do quadro jurídico do país para o qual os dados pessoais são transferidos. Tal não prejudica outras obrigações aplicáveis ao tratamento em questão nos termos do Regulamento (UE) 2016/679.

Cláusula 17

Direito aplicável

As presentes CCT são regidas pelo direito de um dos Estados-Membros da UE, desde que tal direito permita o exercício dos direitos de terceiros beneficiários. As Partes acordam que é aplicável o direito da Polónia.

Cláusula 18

Eleição do foro e jurisdição

(a) Qualquer litígio decorrente das presentes CCT deve ser dirimido pelos tribunais de um Estado-Membro da UE.

(b) As Partes acordam que estes são os tribunais da Polónia.

(c) Um titular de dados pode igualmente intentar uma ação judicial contra o exportador e/ou importador de dados nos tribunais do Estado-Membro em que tem a sua residência habitual.

(d) As Partes aceitam submeter-se à jurisdição dos referidos tribunais.

ANEXO 1. DESCRIÇÃO DO TRATAMENTO DE DADOS

A. LISTA DE PARTES

Exportador de dados

Função: Responsável pelo Tratamento

Identidade e dados de contacto: O Responsável pelo Tratamento, conforme identificado pelas informações de conta (nome ou denominação social, endereço e correio eletrónico de contacto) registadas pelo Responsável pelo Tratamento nos Produtos e Software Ajax no momento da criação da conta.

Atividades relevantes para os dados transferidos: Utilização dos Produtos e Software Ajax para garantir a segurança de instalações ou bens sob o controlo do Responsável pelo Tratamento.

Importador de dados

Função: Subcontratante

Nome: AJAX SYSTEMS TRADING FZE

Endereço: S3B2SR06, Jebel Ali Freezone, Dubai, Emirados Árabes Unidos

Dados de contacto: privacy@ajax.systems

Atividades relevantes para os dados transferidos: Prestação de Serviços que permitem a utilização dos Produtos e Software Ajax por parte do Responsável pelo Tratamento, em conformidade com o Acordo do Utilizador Final.

B. CATEGORIAS DE TITULARES DOS DADOS

Os Dados Pessoais transferidos ao abrigo das presentes CCT dizem respeito às seguintes categorias de titulares dos dados:

- o Responsável pelo Tratamento (titular da conta) e quaisquer pessoas a quem o Responsável pelo Tratamento conceda acesso à conta;
- membros do agregado familiar, trabalhadores, visitantes ou outras pessoas singulares presentes nas instalações ou bens protegidos pelos Produtos e Software Ajax do Responsável pelo Tratamento, cujos Dados Pessoais (incluindo imagens e gravações de vídeo) possam ser recolhidos consoante a configuração estabelecida pelo Responsável pelo Tratamento.

C. FREQUÊNCIA DA TRANSFERÊNCIA

Contínua durante o período de utilização dos Produtos e Software Ajax por parte do Responsável pelo Tratamento.

D. OBJETO, NATUREZA E FINALIDADE DO TRATAMENTO

O objeto, a natureza e as finalidades do tratamento encontram-se estabelecidos na Secção 2 do Acordo.

E. CATEGORIAS DE DADOS PESSOAIS

Para a prestação dos Serviços especificados no presente Acordo, o Subcontratante poderá tratar:

- Identificadores únicos (nome de utilizador);
- Informações sobre a utilização dos Produtos e Software Ajax (como pedidos efetuados através da aplicação);
- endereço IP;
- Nome, apelido e informações de contacto, conforme especificado no momento do registo inicial;
- O conteúdo de mensagens SMS com códigos de acesso enviadas aos utilizadores finais durante o registo ou alterações de conta;
- Informações sobre os dispositivos móveis dos utilizadores finais, incluindo o respetivo tipo, sistema operativo e idioma da interface;
- Imagens, gravações de áudio e de vídeo captadas pelos Produtos e Software Ajax;
- Outros dados e informações tratados sempre que necessário.

Categorias especiais de dados pessoais

Não recolhidas intencionalmente. As imagens e gravações de vídeo captadas pelos dispositivos do Responsável pelo Tratamento podem incluir incidentalmente dados biométricos (por exemplo, imagens de rostos). O Subcontratante aplica as salvaguardas adicionais descritas no Anexo 2 a quaisquer dados dessa natureza. Os dados de categorias especiais só podem ser tratados quando esse tratamento for compatível com a Legislação aplicável em matéria de proteção de dados e quando iniciado pelo titular dos dados ou pelo Responsável pelo Tratamento.

F. DURAÇÃO DO TRATAMENTO / CONSERVAÇÃO

Pelo período de utilização dos Produtos e Software Ajax por parte do Responsável pelo Tratamento. Após a cessação, a eliminação é efetuada no prazo estabelecido na Secção 8 do Acordo.

G. AUTORIDADE DE CONTROLO COMPETENTE

Quando se aplicar o RGPD da UE, a autoridade de controlo competente será a do Estado-Membro da UE

em que o Responsável pelo Tratamento (ou, caso o Responsável pelo Tratamento não tenha um estabelecimento na UE, o seu representante) estiver estabelecido. Caso o Responsável pelo Tratamento não tenha nem um estabelecimento nem um representante na UE, a autoridade de controlo competente será a Comissão Irlandesa de Proteção de Dados.

Quando se aplicar o RGPD do Reino Unido, a autoridade de controlo competente será o Gabinete do Comissário para a Informação do Reino Unido.

ANEXO 2. MEDIDAS TÉCNICAS E ORGANIZACIONAIS

O presente Anexo estabelece as **Medidas Técnicas e Organizacionais** (adiante também designadas por «MTO») e complementa a Secção 3 do Acordo de Tratamento de Dados entre o Subcontratante e o Responsável pelo Tratamento, nos termos do Artigo 28.º do RGPD (Regulamento Geral sobre a Proteção de Dados da UE n.º 2016/679).

Segurança da informação

Cifra de dados: Utilização de AES-256 para dados em repouso e TLS 1.2+ para dados em trânsito.
Pseudonimização: Utilização do algoritmo de hash SHA-256 para os conjuntos de dados aplicáveis.
Firewalls: Implementação de Firewalls de Aplicações Web (WAF) e firewalls ao nível da rede.
Controlo de autorização: Lógica rigorosa de acesso à informação com base em funções.
Resiliência: Proteção contra o tratamento não autorizado, perda ou destruição.
Cópia de segurança e restauração: Os sistemas principais são objeto de cópia de segurança como imagens completas do sistema para permitir uma recuperação rápida. As cópias de segurança são cifradas tanto em repouso como em trânsito, incluindo as cópias de segurança remotas e na nuvem. Os procedimentos de cópia de segurança e restauração são testados regularmente para confirmar que a recuperação se encontra totalmente operacional.
Em caso de restauração a partir de uma cópia de segurança, os Dados Pessoais anteriormente eliminados são removidos dos dados restaurados sem demora injustificada e, em qualquer caso, no prazo de 24 horas após a restauração.
Proteção contra ataques DDoS: Utilização de serviços especializados de filtragem de tráfego e ferramentas automatizadas de mitigação fornecidas pelo fornecedor de infraestrutura para proteção contra ataques à infraestrutura (Camada 3/4) e à camada de aplicação (Camada 7).
Gestão de patches: Monitorização e aplicação automatizadas de patches de segurança para todos os recursos na nuvem e sistemas operativos.

1. Confidencialidade

1.1. Controlo de acessos físicos

Medidas adequadas para impedir que pessoas não autorizadas tenham acesso aos sistemas de tratamento de dados através dos quais os Dados Pessoais são tratados ou utilizados.

1.2. Medidas técnicas

Sistema de alarme: Utilização dos sistemas de segurança avançados próprios de Ajax (hubs, detetores de movimento e sirenes) com monitorização 24/7 e alertas instantâneos.
Controlo de acessos eletrónico: Sistema seguro de cartões/comandos RFID para entrada no escritório; os registos de acesso são mantidos e revistos regularmente.
Videovigilância: Câmaras IP de alta definição que monitorizam pontos de entrada/saída e zonas críticas internas.
Segurança da infraestrutura na nuvem: O acesso físico aos servidores é gerido pela AWS em conformidade com as suas certificações de conformidade (SOC 2, ISO 27001).

1.3. Medidas organizacionais

Política de segurança da informação: Regras internas abrangentes que regem a segurança física e a proteção de ativos.
Instruções de trabalho para a segurança operacional: Procedimentos documentados para garantir a segurança do ambiente de trabalho e o manuseamento de equipamento.
Instrução de trabalho para o controlo de acessos: Protocolos rigorosos para a atribuição, revogação e auditoria de direitos de acesso físico para trabalhadores e prestadores de serviços.
Política de gestão de visitantes: Requisitos para o registo, identificação e acompanhamento de todos os visitantes nas instalações de escritório.

2. Controlo de acessos lógicos

Medidas para impedir a utilização não autorizada dos sistemas de tratamento de dados.

Autenticação multinível (MFA): Obrigatória para todo o acesso administrativo, gestão da consola na nuvem e sessões remotas.
Gestão de identidades e acessos (IAM): Gestão centralizada de permissões de utilizador com revisões regulares de acesso.
Acesso por VPN: Exigência de túneis VPN cifrados para qualquer ligação remota ao ambiente de produção ou a ferramentas de gestão interna.

3. Controlo de acesso aos dados

Medidas para garantir que as pessoas com direito de utilização de um sistema de tratamento de dados só possam ter acesso aos dados abrangidos pela sua competência.

Controlo de acessos baseado em funções (RBAC): As permissões são concedidas estritamente de acordo com as funções específicas do cargo e com base no princípio da «necessidade de saber».
Registo de auditoria: Registo abrangente de todas as atividades de acesso, alterações e eliminações nos sistemas que contenham Dados Pessoais.

4. Integridade, disponibilidade e resiliência

Controlo de transferência: Medidas para garantir que os Dados Pessoais não possam ser lidos, copiados, modificados ou removidos sem autorização durante a sua transmissão eletrónica.
Controlo de introdução: Medidas para garantir que seja possível verificar e determinar se, e por quem, os Dados Pessoais foram introduzidos, modificados ou removidos dos sistemas de tratamento de dados.
Controlo de disponibilidade: Medidas para garantir que os Dados Pessoais estejam protegidos contra a sua destruição ou perda acidentais (por exemplo, fontes de alimentação ininterrupta (UPS) em centros de dados, armazenamento redundante).
Continuidade do negócio e recuperação de desastres: Os planos documentados de continuidade do negócio e de recuperação de desastres são mantidos, testados e verificados, pelo menos, anualmente.

5. Procedimentos para testes e avaliações regulares

Gestão de incidentes: Processo documentado para deteção, comunicação e resposta a incidentes de segurança e potenciais violações de dados pessoais.
Gestão de vulnerabilidades: Análise automática e regular de vulnerabilidades e testes de penetração profissionais periódicos à infraestrutura e às aplicações.
Sensibilização dos trabalhadores: Sessões regulares de formação para o pessoal sobre proteção de dados, conformidade com o RGPD e ameaças de phishing.
Segurança do pessoal: São realizadas verificações de antecedentes, em conformidade com as boas

práticas de contratação, e todo o pessoal e prestadores de serviços assinam acordos de confidencialidade antes de acederem a Dados Pessoais.

ANEXO 3. LISTA DE SUBCONTRATANTES ULTERIORES AUTORIZADOS

A lista atualizada dos subcontratantes ulteriores envolvidos pelo Subcontratante é mantida e publicada em: https://ajax.systems/gdpr-white-paper/

O Subcontratante atualizará esta lista antes de envolver qualquer novo subcontratante ulterior, de acordo com o procedimento estabelecido na Secção 7 do presente Contrato.