Contrato de Processador de Dados
Controlador de Dados: Cliente situado dentro da UE (o "**Controlador de dados**") e o

Processador de dados:
Empresa: One.com Group AB
Reg. comercial nº 559205-2400
Cidade: Malmö
País do registo: Suécia

(o "**Processador de dados**")
(separadamente designado de "**Parte**" e coletivamente de "**Partes**")

celebrou o presente:

CONTRATO DO PROCESSADOR DE DADOS

(o "**Contrato**")
relativo ao processamento, por parte do Processador de Dados, de dados pessoais em nome do Controlador de Dados.

1. Os dados pessoais processados

1.1 O presente Contrato foi celebrado no âmbito da utilização dos Controladores de Dados dos serviços do Processador de Dados como parte da subscrição e serviços adicionais descritos nos "Termos e Condições de One.com" (o "**Contrato Principal**").

1.2 O Processador de Dados processa os tipos de dados pessoais em nome do Controlador de Dados relativamente aos titulares de dados relevantes, conforme especificado no **Anexo 1**. Os dados pessoais são relativos aos titulares de dados listados no **Anexo 1**.

1.3 O Processador de Dados pode iniciar o processamento de dados pessoais em nome do Controlador de Dados após a entrada em vigor do Contrato. O processamento tem a duração especificada nas instruções no **Anexo 1** do Contrato.

1.4 O Contrato e o Contrato Principal são interdependentes e não podem ser rescindidos em separado. No entanto, o Contrato pode ser substituído por outro Contrato de Processador de Dados válido sem rescisão do Contrato Principal.

2. Objetivo

2.1 O Processador de Dados só pode processar dados pessoais para os fins que sejam necessários para satisfazer as obrigações do Processador de Dados e, ao fazê-lo, prestar os serviços estabelecidos no Contrato Principal.

3. Obrigações do Controlador de Dados

3.1 O Controlador de Dados garante que os dados pessoais são processados para fins legítimos e objetivos e que o Processador de Dados não processa mais dados pessoais que os exigidos para atender às referidas finalidades.

3.2 O Controlador de Dados é responsável por assegurar que existe uma base jurídica válida para o processamento no ato de transferência dos dados pessoais para o Processador de Dados. Mediante pedido do Processador de Dados, o Controlador de Dados compromete-se, por escrito, a ter em consideração e/ou a prestar documentação de base para o processamento.

3.3 Além disso, o Controlador de Dados garante que os titulares de dados a que os dados pessoais pertencem receberam informações suficientes sobre o processamento dos próprios dados pessoais.

4. Obrigações do Processador de Dados

4.1 Todo o processamento pelo Processador de Dados de dados pessoais prestados pelo Controlador de Dados deve ser feito em conformidade com as instruções preparadas pelo Controlador de Dados; além disso, o Processador de Dados é ainda obrigado a cumprir com toda e qualquer legislação de proteção de dados em vigor de tempos a tempos. Se a legislação da União Europeia ou a legislação de um Estado Membro da UE à qual o Processador de Dados está sujeita estipule que o Processador de Dados é obrigado a processar os dados pessoais listados no **Anexo 1**, o Processador de Dados deve informar o Controlador de Dados desse requisito jurídico antes do processamento. No entanto, tal não se aplica se esta legislação proibir tais informações, com base em argumentos importantes de interesses públicos. O Processador de Dados deve imediatamente informar o Controlador de Dados se, no parecer do Processador de Dados, uma instrução infringir o Regulamento Geral de Proteção de Dados da UE ou as disposições de proteção de dados de um Estado-Membro da UE.

4.2 O Processador de Dados deve tomar todas as medidas de segurança técnicas e organizacionais necessárias, incluindo quaisquer medidas adicionais, exigidas para garantir que os dados pessoais não são acidental ou ilegalmente destruídos, perdidos, comprometidos ou divulgados a terceiros não autorizados, usados indevidamente ou de outra forma processados de uma maneira que seja contrária à legislação de proteção de dados em vigor num dado momento. Estas medidas são descritas em maior detalhe no **Anexo 2**.

4.3 O Processador de Dados deve garantir que os trabalhadores autorizados do processamento de dados pessoais se submeteram a compromissos de confidencialidade ou que estão sob obrigações de confidencialidade estatutárias apropriadas.

4.4 Se solicitado pelo Controlador de Dados, o Processador de Dados deve declarar e/ou documentar que o Processador de Dados cumpre os requisitos da legislação de proteção de dados aplicável, incluindo documentação relativa aos fluxos do Processador de Dados, bem como procedimentos/políticas para o processamento de dados pessoais.

4.5 Tendo em conta a natureza do processamento, o Processador de Dados deve, na medida do possível, auxiliar o controlador com as medidas técnicas e organizacionais apropriadas, para a satisfação da obrigação do Controlador de Dados de responder a pedidos de exercício dos direitos do titular de dados, conforme estabelecido no capítulo 3 do Regulamento Geral de Proteção de Dados.

4.6 O Processador de Dados, ou outro Processador de Dados (subprocessador de dados) deve enviar pedidos e objeções de titulares de dados ao Controlador de Dados, para processamento adicional por parte do Controlador de Dados dos mesmos, exceto se o Processador de Dados estiver autorizado a tratar ele próprio esse pedido. Se requerido pelo Controlador de Dados, o Processador de Dados deve auxiliar o Controlador de Dados a responder a pedidos e/ou objeções do género.

4.7 Caso o Processador de Dados processar dados pessoais noutro estado-membro da UE, o Processador de Dados deve cumprir a legislação relativa às medidas de segurança nesse estado membro.

4.8 O Processador de Dados deve notificar o Controlador de Dados se tiver havido uma interrupção na operação, uma suspeita de que regras de proteção de dados foram infringidas ou outras irregularidades relativas ao processamento dos dados pessoais. O prazo do Processador de Dados para notificação de uma violação de segurança ao Controlador de Dados é de 24 horas desde o momento em que o Processador de Dados tome conhecimento da referida violação de segurança. Se requerido pelo Controlador de Dados, o Processador de Dados deve auxiliar o Controlador de Dados a esclarecer o âmbito da violação de segurança, incluindo a preparação de qualquer notificação à Agência de Proteção de Dados relevante e/ou aos titulares de dados.

4.9 O Processador de Dados deve disponibilizar ao Controlador de Dados todas as informações necessárias para demonstrar a conformidade com o art.º 28 do Regulamento Geral de Proteção de Dados e do Contrato. Nesse sentido, o Processador de Dados permite e contribui para auditorias, incluindo inspeções, levadas a cabo pelo Controlador de Dados ou outro auditor mandatado pelo Controlador de Dados.

4.10 Além do anteriormente exposto, o Processador de Dados deve auxiliar o Controlador de Dados a garantir a conformidade com as obrigações do Controlador de Dados nos termos dos art. 32-36 do Regulamento Geral de Proteção de Dados. Este auxílio terá em consideração a natureza do processamento e as informações disponíveis para o Processador de Dados.

5. Transferência de dados para subprocessadores de dados e terceiros

5.1 O Processador de Dados deve cumprir as condições estabelecidas no art.°28, números 2 e 4 do Regulamento Geral de Proteção de Dados para contratação de outro Processador de Dados (subprocessador de dados). Isto implica que o Processador de Dados não contrata outro Processador de Dados (subprocessador de dados) para a consecução das obrigações do Contrato sem o consentimento prévio por escrito específico ou geral do Controlador de Dados.

5.2 O Controlador de Dados pelo presente concede ao Processador de Dados autoridade geral para celebrar contratos com subprocessadores de dados. O Processador de Dados deve notificar o Controlador de Dados de quaisquer alterações relativas ao acrescento ou substituições de subprocessadores de dados o mais tardar 30 dias antes do início do processamento de dados pessoais por um novo subprocessador dados. O Controlador de Dados pode emitir objeções razoáveis e relevantes face a tais alterações, no prazo de 14 dias após a receção da notificação. Se o Processador de Dados continuar a pretender usar um subprocessador de dados a que o Controlador de Dados tenha objetado, as Partes têm o direito de rescindir o Contrato, conforme na cláusula 7.

5.3 Quando o Controlador de Dados tiver aprovado que o Processador de Dados possa usar um subprocessador de dados, o Processador de Dados tem de impor as mesmas obrigações ao mesmo subprocessador de dados que as estabelecidas no Contrato. Isto é executado através de um contrato ou outro ato jurídico nos termos da legislação UE ou da legislação de um Estado-Membro. Deverá garantir-se, por ex., que o subprocessador de dados presta garantias suficientes para implementar medidas técnicas e organizacionais apropriadas de forma tal que o processamento satisfaça os requisitos do Regulamento Geral de Proteção de Dados (os termos integrais).

5.4 Se o subprocessador de dados não cumprir as suas obrigações de proteção de dados, o Processador de Dados permanece totalmente responsável perante o Controlador de Dados pelo desempenho das obrigações do subprocessador de dados.

5.5 A divulgação, transferência e uso interno dos dados pessoais do Controlador de Dados a países estrangeiros ou organizações internacionais só poderá ter lugar em conformidade com as instruções documentadas do Controlador de Dados; exceto se estipulado pela legislação da UE ou pela legislação de um Estado-Membro a que o Processador de Dados se encontre sujeito. Em caso positivo, o Processador de Dados tem de notificar o Controlador de Dados deste requisito jurídico antes do processamento, exceto se a lei proibir tal notificação por motivos importantes de interesses públicos.

5.6 Se os dados pessoais estipulados no **Anexo 1** forem transferidos para subprocessadores de dados fora da UE/EEE, tem de, no referido contrato, vir declarado que a legislação de proteção de dados aplicável no país do Controlador de Dados se aplica aos subprocessadores de dados. Além disso, se o subprocessador de dados recetor estiver sediado na UE/EEE, tem de vir declarado no referido contrato os requisitos estatutários específicos do país da UE recetor relativamente aos processadores de dados, por ex., as exigências de notificação das autoridades nacionais têm de ser cumpridas.

5.7 O Processador de Dados é obrigado a celebrar contratos escritos de processador de dados com os subprocessadores de dados na UE/EEE. No que fiz respeito aos subprocessadores de dados fora da UE/EEE, o Processador de Dados tem de garantir mecanismos de transferência suficientes e celebrar um contrato de subprocessador de dados celebrando contratos padrão, em conformidade com as Cláusulas Contratuais Padrão da Comissão Europeia ("**Contratos padrão**") com base no regulamento 21/914/UE de 4 de junho de 2021.

5.8 No momento de assinatura do presente Contrato, o Processador de Dados contrata os subprocessadores de dados listados no **Anexo 3**.

6. Responsabilidade

6.1 A responsabilidade das Partes é governada pelo Contrato Principal.

6.2 A responsabilidade por danos das Parte nos termos do presente Contrato é governada pelo Contrato Principal.

7. Data de vigência e rescisão

7.1 O presente Contrato entra em vigor no mesmo momento que o Contrato Principal. Em caso de rescisão do Contrato Principal, este Contrato também será rescindido. No entanto, o Processador de Dados permanece vinculado pelas obrigações estipuladas no presente Contrato, contanto que o Processador de Dados processe dados pessoais em nome do Controlador de Dados.

7.2 Mediante rescisão dos serviços de processamento o Processador de Dados é obrigado, mediante pedido do Controlador de Dados, a eliminar ou devolver todos os dados pessoais ao Controlador de Dados, bem como eliminar as cópias existentes, exceto se a retenção dos dados pessoais for prescrita pela legislação da UE ou nacional.

8. Legislação e jurisdição aplicáveis

8.1 Qualquer discórdia ou litígio decorrente de, ou associado ao presente Contrato deve ser resolvido por um tribunal de primeira instância competente, na mesma jurisdição e com a mesma escolha de lei que declarado no Contrato Principal.

9. Assinaturas

Em nome do Controlador de Dados:

_____
[Nome] [Título]

Em nome do Processador de Dados:

_____
Ronni Engelhardt Diretor-Geral

Anexo 1
Categorias de titulares de dados, tipos de dados pessoais e instruções

1. Categorias de titulares de dados:

- O Processador de Dados irá processar informações de contacto sobre clientes efetivos, potenciais ou anteriores e/ou membros, trabalhadores, fornecedores, empresas e parceiros de colaboração e afiliadas.
- O Processador de Dados disponibiliza o seu sistema ao Controlador de Dados enquanto serviço de alojamento, e não é possível para o Processador de Dados determinar todas as categorias de titulares de dados. Se o Controlador de Dados alojar dados em categorias adicionais de titulares de dados junto do Processador de Dados, é obrigação do Controlador de Dados registar estas informações.

2. Tipos de dados pessoais:

- Informações de contacto e identificação incluindo e-mail
- Endereços IP
- Nomes de domínio
- Nomes de utilizador
- Informações sobre filiação
- Dados analíticos e de utilização
- Histórico e informações sobre encomendas
- Contratos
- Comunicação
- Assistência
- Imagens
- Podem ocorrer tipos adicionais de dados pessoais

3. Instruções

Serviço

O Processador de Dados pode processar dados pessoais relativos aos titulares de dado a fim de fornecer, desenvolver, gerir e administrar os serviços do Contrato Principal, incluindo para garantir a estabilidade e a operatividade dos nossos servidores, e para cumprir requisitos de lei.

Período de retenção

Os dados pessoais armazenados/alojados nos nossos sistemas são eliminados ou tornados anónimos dentro de um tempo razoável após o Controlador de Dados ter rescindido por completo o Contrato Principal. É feita exceção para dados onde haja um requisito legal face ao Processador de Dados de conservação durante mais tempo. Este tipo de dados serão normalmente eliminados no prazo de oito semanas, mas podem ser eliminados mais cedo. Outros tipos de dados que são armazenados em registos, etc., serão eliminados após um período razoável, normalmente dentro de 8 semanas, após os quais são eliminados pelo Processador de Dados.

Localização do processamento

O processamento de dados pessoais coberto pelo Contrato não deve ser realizado sem o consentimento prévio por escrito do Controlador de Dados em locais que não a morada do Processador de Dados e a morada dos subprocessadores de dados, conforme listado no Anexo 3.

Inspeção do Processador de Dados

O Processador de Dados deve, uma vez ao ano e a encargo próprio, obter um relatório de auditoria/inspeção de terceiros relativamente à conformidade do Processador de Dados com o presente Contrato e Anexos. O relatório ou outro formato de auditoria tem de ser encaminhado para o Controlador de Dados ou publicado no site do Controlador de Dados o quanto antes após a sua redação.

Programa 2
Medidas de segurança

Domínio	Práticas
Organização da segurança das informações	**Propriedade de segurança**. A One.com designou um representante de segurança responsável por coordenar e monitorizar regras e procedimentos de segurança. Uma governação composta por indivíduos de nível C auxiliam e orientam o representante de segurança. **Funções e responsabilidades de segurança**. O pessoal da One.com com acesso aos dados do cliente está sujeito a obrigações de confidencialidade, que são enfatizadas no ato de contratação e por consciencialização contínua. **Gestão de risco**. A One.com realiza continuamente avaliações de risco, como parte da Gestão do Risco, antes de processar os dados do cliente ou de lançar serviços. O rastreamento da Gestão de Risco permite um enfoque em ameaças relevantes através do estabelecimento de prioridades, estruturação e mitigação dos riscos acima do que é aceite. São implementadas cópias de segurança. O Processador de Dados retém os seus documentos de segurança em virtude dos seus requisitos de retenção após deixarem de estar em vigor.
Administração de ativos	**Inventário de bens**. O Processador de Dados mantém um inventário de todos os suportes nos quais os dados do cliente estão armazenados. O acesso aos inventários de tais suportes encontra-se limitado aos trabalhadores do Processador de Dados autorizados por escrito para acesso aos mesmos. **Manuseamento de bens**

Domínio	Práticas
	- A One.com classifica os dados dos clientes para ajudar a quantificá-los e permitir que o acesso aos mesmos seja devidamente restringido. - Os trabalhadores do Processador de Dados tem de obter a autorização do Processador de Dados antes de armazenarem dados dos clientes em serviços portáteis, aceder remotamente aos dados dos clientes ou a processar dados dos clientes fora das instalações do Processador de Dados.
Segurança dos Recursos humanos	**Formação sobre segurança**. A One.com informa os próprios trabalhadores sobre procedimentos de segurança relevante e respetivas funções, aborda novas ameaças, etc., na medida em que os trabalhadores desempenham um papel fundamental para a mesma.
Segurança física e ambiental	**Acesso físico às instalações**. A One.com limita o acesso às instalações onde sistemas de informação que processam dados do cliente se localizam a indivíduos autorizados identificados. **Acesso físico aos componentes**. A One.com garante restrições suficientes nos suportes que contêm dados do cliente. **Proteção contra perturbações**. A One.com usa uma série de sistemas padrão da indústria para proteger contra a perda de dados decorrente de falhas de alimentação, inundações, incêndios ou interferência da linha. **Eliminação de componentes**. A One.com utiliza processos padrão da indústria para eliminar dados do cliente quando deixam de ser necessários.
Gestão das comunicações e operações	**Política operacional**. A One.com mantém documentos de segurança que descrevem as suas medidas de segurança e os procedimentos e as responsabilidades relevantes dos próprios trabalhadores que têm acesso aos dados dos clientes. **Procedimento de recuperação de dados** - A One.com armazena cópias de dados de clientes e procedimentos de recuperação de dados num local diferente do equipamento computorizado primário para o processamento dos dados dos clientes. - A One.com possui procedimentos implementados específicos que regem o acesso às cópias dos dados dos clientes. **Software malicioso**. A One.com possui controlos anti-malware que ajudam a evitar que software malicioso obtenha acesso não autorizado aos dados dos clientes, incluindo software malicioso originário de redes públicas. Também foi implementado um antivírus. **Registo de eventos**. A One.com regista, ou permite ao cliente registar, aceder e utilizar sistemas de informação que contêm dados dos clientes, registando o ID de acesso, a hora, a autorização concedida ou negada e a atividade relevante. **Encriptação**. As comunicações via Internet entre o sistema que tratam dados pessoais são encriptadas.
Controlo do acesso	**Política de acesso**. A One.com mantém um registo de privilégios de segurança dos indivíduos que têm acesso aos dados dos clientes. **Autorização de acesso**

Domínio	Práticas
	- A One.com desativa as credenciais de autenticação que não foram usadas durante um período de tempo para não exceder os seis meses. - A One.com identifica os trabalhadores que podem conceder, alterar ou cancelar o acesso autorizado aos dados e recursos. - A One.com certifica-se de que nos casos em que mais do que um indivíduo tenha acesso a sistemas que contêm dados dos clientes, os indivíduos possuem identificadores/inícios de sessão separados. **O menor privilégio** - A One.com limita o acesso aos dados dos clientes aos indivíduos que necessitem de aceder aos mesmos para desempenhar a sua função profissional. **Integridade e confidencialidade** - A One.com instrui o próprio pessoal a desativar sessões administrativas quando abandonam as instalações ou quando os computadores são deixados sem supervisão. - A One.com armazena palavras-passe de uma forma que as torna ininteligíveis quando estão em vigor. **Autenticação** - A One.com usa práticas padrão da indústria para identificar e autenticar utilizadores que tentam aceder aos sistemas de informação. - Nos casos em que os mecanismos de autenticação se baseiam em palavras-passe, o Processador de Dados exige que as palavras-passe sejam renovadas com regularidade. - A One.com garante que os identificadores desativados ou expirados não são concedidos a outros indivíduos. - A One.com monitoriza ou permite ao cliente monitorizar tentativas repetidas de obter acesso ao sistema de informação usando uma palavra-passe inválida. - A One.com mantém procedimentos padrão da indústria para desativar palavras-passe que tenham sido corrompidas ou acidentalmente divulgadas. - A One.com usa práticas de proteção de palavras-passe padrão da indústria, incluindo práticas destinadas a manter a confidencialidade e a integridade de palavras-passe quando estas são atribuídas e distribuídas, e durante o seu armazenamento. **Design da rede**. A One.com tem controlos implementados para evitar que indivíduos obtenham direitos de acesso que não lhes tenham sido atribuídos e de aceder a dados dos clientes quando não têm autorização de acesso aos mesmos.
Gestão de incidentes de segurança das informações	**Processo de resposta a incidentes** - A One.com mantém um registo de violações de segurança com uma descrição da violação, do período de tempo, das consequências da violação, do nome do denunciante, a quem a violação foi comunicada, e o procedimento para recuperação de dados. - Para cada violação de segurança que seja um Incidente de Segurança, a One.com enviará uma notificação sem demoras indevidas e, em todo o caso, dentro de 72 horas.

Domínio	Práticas
	- A One.com monitoriza ou permite que o Cliente monitorize, divulgue os dados do cliente, incluindo quais os dados divulgados, a quem e em que altura.
Gestão da continuidade empresarial	- A One.com mantém planos de emergência e contingência para as instalações nas quais os sistemas de informação do Processador de Dados que processa os dados dos clientes se situam. - O armazenamento redundante da One.com e os seus procedimentos para recuperação de dados foram idealizados para procurar reconstruir os dados dos clientes no seu estado original ou da última cópia de segurança, antes de terem sido perdidos ou destruídos.

Programa 3
Lista de subprocessadores de dados

Fornecedor	Localização	Função	Atualizado
Global Connect A/S	DK	Datacenter	20.02.2021
Interxion	DK	Datacenter	12.04.2021
Interxion	DK/UK/NL/FR/DE	PoP (Ponto de presença)	12.04.2021
Equinix	SE	PoP (Ponto de presença)	12.04.2021