Datenverarbeitungsvertrag

Datenverantwortlicher: Kunde mit Sitz in der EU (der „Datenverantwortliche“)

und

Datenverarbeiter:

Unternehmen:	One.com Gruppe AB
Reg.-Nr.	559205-2400
Stadt:	Malmö
Land der Registrierung:	Schweden

(der „**Datenverarbeiter**“)

(einzeln als „**Partei**“ und gemeinsam als „**Parteien**“ bezeichnet)

haben dies beschlossen:

Datenverarbeitungsvertrag

(der „**Vertrag**“)

in Bezug auf die Verarbeitung personenbezogener Daten durch den Datenverarbeiter im Auftrag des Datenverantwortlichen.

1. Die verarbeiteten personenbezogenen Daten

1.1 Dieser Vertrag wurde im Zusammenhang mit der Nutzung der Dienste des Datenverarbeiters durch den Datenverantwortlichen im Rahmen des Abonnements und der zusätzlichen Dienste, wie in den „One.com Geschäftsbedingungen“ (der „**Hauptvertrag**“) beschrieben, geschlossen.

1.2 Der Datenverarbeiter verarbeitet die Arten von personenbezogenen Daten im Auftrag des Datenverantwortlichen im Hinblick auf die relevanten Daten der betroffenen Personen wie in **Anhang** 1 beschrieben. Die personenbezogenen Daten beziehen sich auf die in Anhang 1 aufgeführten betroffenen Personen.

1.3 Der Datenverarbeiter kann nach Inkrafttreten des Vertrags im Auftrag des Datenverantwortlichen mit der Verarbeitung personenbezogener Daten beginnen. Die Dauer der Verarbeitung ist in den Angaben in **Anhang 1** des Vertrags festgelegt.

1.4 Der Vertrag und der Hauptvertrag ergänzen sich gegenseitig und können nicht separat gekündigt werden. Der Vertrag kann jedoch durch einen anderen gültigen Vertrag mit dem Datenverarbeiter ersetzt werden, ohne den Hauptvertrag zu beenden.

2. Zweck

2.1 Der Datenverarbeiter darf personenbezogene Daten ausschließlich zu Zwecken verarbeiten, die für die Erfüllung seiner Pflichten und damit für die Erbringung der im Hauptvertrag festgelegten Dienstleistungen erforderlich sind.

3. Pflichten des Datenverantwortlichen

3.1 Der Datenverantwortliche garantiert, dass die personenbezogenen Daten für legitime und objektive Zwecke verarbeitet werden und dass der Datenverarbeiter nicht mehr personenbezogene Daten verarbeitet, als für die Erfüllung dieser Zwecke erforderlich sind.

3.2 Der Datenverantwortliche trägt die Verantwortung dafür, dass zum Zeitpunkt der Übermittlung der personenbezogenen Daten an den Datenverarbeiter eine gültige Rechtsgrundlage für die Verarbeitung besteht. Auf Verlangen des Datenverarbeiters verpflichtet sich der Datenverantwortliche, schriftlich Rechenschaft abzulegen und/oder die Grundlage für die Verarbeitung zu dokumentieren.

3.3 Darüber hinaus garantiert der Datenverantwortliche, dass die betroffenen Personen, auf die sich die personenbezogenen Daten beziehen, hinreichend über die Verarbeitung ihrer personenbezogenen Daten informiert worden sind.

4. Pflichten des Datenverarbeiters

4.1 Jedwede Verarbeitung der vom Datenverantwortlichen zur Verfügung gestellten personenbezogenen Daten durch den Datenverarbeiter muss in Übereinstimmung mit den vom Datenverantwortlichen vorbereiteten Anweisungen erfolgen. Der Datenverarbeiter ist darüber hinaus verpflichtet, alle jeweils geltenden Datenschutzgesetze einzuhalten. Wenn das EU-Recht oder das Recht eines EU-Mitgliedstaates, dem der Datenverarbeiter unterliegt, vorschreibt, dass der Datenverarbeiter verpflichtet ist, die in **Anhang 1** aufgeführten personenbezogenen Daten zu verarbeiten, muss der Datenverarbeiter den Datenverantwortlichen vor der Verarbeitung über diese rechtliche Verpflichtung informieren. Dies trifft jedoch nicht zu, wenn diese Gesetzgebung derartige Informationen aus wichtigen Gründen des öffentlichen Interesses verbietet. Der Datenverarbeiter ist verpflichtet, den Datenverantwortlichen unverzüglich zu informieren, wenn eine Anweisung nach Ansicht des Datenverarbeiters gegen die EU-Datenschutzgrundverordnung oder die Datenschutzbestimmungen eines EU-Mitgliedstaates verstößt.

4.2 Der Datenverarbeiter ist verpflichtet, alle notwendigen technischen und organisatorischen Sicherheitsmaßnahmen zu treffen, einschließlich aller zusätzlichen Maßnahmen, die gewährleisten, dass die personenbezogenen Daten nicht versehentlich oder unrechtmäßig zerstört werden, verloren gehen oder beeinträchtigt werden oder unbefugten Dritten zugänglich gemacht werden, missbraucht werden oder auf andere Weise in einer Weise verarbeitet werden, die zu irgendeinem Zeitpunkt gegen die geltenden Datenschutzvorschriften verstößt. Diese Maßnahmen werden in **Anhang 2** ausführlicher beschrieben.

4.3 Der Datenverarbeiter ist verpflichtet sicherzustellen, dass die zur Verarbeitung der personenbezogenen Daten befugten Mitarbeiter sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Verpflichtung zur Vertraulichkeit unterliegen.

4.4 Auf Verlangen des Datenverantwortlichen ist der Datenverantwortliche verpflichtet, zu erklären und/oder zu dokumentieren, dass der Datenverantwortliche die Anforderungen der geltenden Datenschutzgesetze einhält, einschließlich der Dokumentation der Datenflüsse des Datenverantwortlichen sowie der Verfahren/Richtlinien für die Verarbeitung personenbezogener Daten.

4.5 Unter Berücksichtigung der Art der Verarbeitung muss der Datenverarbeiter den Datenverantwortlichen nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung seiner Verpflichtung unterstützen, auf Anfragen zur Ausübung der Rechte der betroffenen Person wie in Kapitel 3 der Allgemeinen Datenschutzverordnung festgelegt zu reagieren.

4.6 Der Datenverarbeiter oder ein anderer Datenverarbeiter (unterbeauftragter Datenverarbeiter) muss Anfragen und Einwände von betroffenen Personen an den Datenverantwortlichen weiterleiten, damit der Datenverantwortliche diese weiterverarbeiten kann, sofern der Datenverarbeiter nicht berechtigt ist, diese Anfragen selbst zu bearbeiten. Auf Verlangen des Datenverantwortlichen ist der Datenverarbeiter verpflichtet, den Datenverantwortlichen bei der Beantwortung solcher Anfragen und/oder Einwände zu unterstützen.

4.7 Wenn der Datenverarbeiter personenbezogene Daten in einem anderen EU-Mitgliedsstaat verarbeitet, ist er verpflichtet, die Rechtsvorschriften bezüglich der Sicherheitsmaßnahmen in diesem Mitgliedsstaat einzuhalten.

4.8 Der Datenverarbeiter ist verpflichtet, den Datenverantwortlichen zu benachrichtigen, wenn eine Unterbrechung des Betriebs, ein Verdacht auf einen Verstoß gegen die Datenschutzbestimmungen oder andere Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung der personenbezogenen Daten auftreten. Die Frist des Datenverarbeiters zur Benachrichtigung des Datenverantwortlichen über eine Sicherheitsverletzung beträgt 24 Stunden ab dem Zeitpunkt, an dem der Datenverarbeiter von einer Sicherheitsverletzung Kenntnis erhält. Auf Verlangen des Datenverantwortlichen ist der Datenverarbeiter verpflichtet, den Datenverantwortlichen bei der Klärung des Ausmaßes der Sicherheitsverletzung zu unterstützen. Dies schließt die Vorbereitung von Benachrichtigungen an die zuständige Datenschutzbehörde und/oder die betroffenen Personen ein.

4.9 Der Datenverarbeiter ist verpflichtet, dem Datenverantwortlichen alle erforderlichen Informationen zur Verfügung zu stellen, um die Einhaltung von Artikel 28 der Allgemeinen Datenschutzverordnung und des Vertrags nachzuweisen. In diesem Zusammenhang genehmigt der Datenverarbeiter Audits, einschließlich Inspektionen, die von dem Datenverantwortlichen oder einem anderen von dem Datenverantwortlichen beauftragten Prüfer durchgeführt werden, und beteiligt sich an diesen.

4.10 Zusätzlich zu den oben genannten Punkten ist der Datenverarbeiter verpflichtet, den Datenverantwortlichen dabei zu unterstützen, die Einhaltung der Verpflichtungen des Datenverantwortlichen gemäß Artikel 32-36 der Allgemeinen Datenschutzverordnung sicherzustellen. Im Rahmen dieser Unterstützung werden die Art der Verarbeitung sowie die dem Datenverarbeiter zur Verfügung stehenden Informationen berücksichtigt.

5. Übermittlung von Daten an Sub-Datenverarbeiter oder Dritte

5.1 Der Datenverarbeiter ist verpflichtet, die in Artikel 28, Absatz 2 und 4 der Allgemeinen Datenschutzverordnung festgelegten Bedingungen einzuhalten, wenn er einen anderen

Datenverarbeiter (Sub-Datenverarbeiter) beauftragt. Dies bedeutet, dass der Datenverarbeiter keinen anderen Datenverarbeiter (Sub-Datenverarbeiter) mit der Durchführung des Vertrags beauftragt, ohne dass der Datenverantwortliche zuvor eine spezifische oder allgemeine schriftliche Genehmigung erteilt hat.

5.2 Der Datenverantwortliche erteilt dem Datenverarbeiter hiermit eine allgemeine Vollmacht zum Abschluss von Vereinbarungen mit Sub-Datenverarbeitern. Der Datenverarbeiter ist verpflichtet, den Datenverantwortlichen spätestens 30 Tage vor dem Beginn der Verarbeitung der personenbezogenen Daten durch einen neuen Sub-Datenverarbeiter über alle Änderungen bezüglich der Hinzufügung oder des Austauschs von Sub-Datenverarbeitern zu informieren. Der Datenverantwortliche kann gegen derartige Änderungen innerhalb von 14 Tagen nach Erhalt der Mitteilung angemessene und relevante Einwände erheben. Möchte der Datenverarbeiter weiterhin einen Sub-Datenverarbeiter einsetzen, gegen den der Datenverantwortliche Einspruch erhoben hat, haben die Parteien das Recht, den Vertrag zu kündigen, vgl. Artikel 7.

5.3 Hat der Datenverantwortliche zugestimmt, dass der Datenverarbeiter einen Sub-Datenverarbeiter einsetzen kann, muss der Datenverarbeiter dem Sub-Datenverarbeiter die gleichen Verpflichtungen auferlegen, wie sie in dem Vertrag festgelegt sind. Dies geschieht durch einen Vertrag oder einen anderen Rechtsakt gemäß EU-Recht oder dem Recht eines Mitgliedstaates. Es muss beispielsweise sichergestellt werden, dass der Sub-Datenverarbeiter ausreichende Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen zu ergreifen, damit die Verarbeitung den Anforderungen der Datenschutzgrundverordnung entspricht („Back-to-Back“-Bedingungen).

5.4 Sollte der Sub-Datenverarbeiter seinen Datenschutzpflichten nicht nachkommen, so haftet der Datenverarbeiter gegenüber dem Datenverantwortlichen weiterhin in vollem Umfang für die Erfüllung der Pflichten des Sub-Datenverarbeiters.

5.5 Die Offenlegung, Übermittlung und interne Nutzung der personenbezogenen Daten der verantwortlichen Stelle an Drittländer oder internationale Organisationen darf nur in Übereinstimmung mit schriftlichen Anweisungen der verantwortlichen Stelle erfolgen, sofern dies nicht durch EU-Recht oder das Recht eines Mitgliedstaates, dem der Datenverarbeiter unterliegt, vorgeschrieben ist. In diesem Fall muss der Datenverarbeiter den Datenverantwortlichen vor der Verarbeitung über diese gesetzliche Verpflichtung informieren, sofern das Gesetz eine solche Benachrichtigung nicht aus wichtigen Gründen des öffentlichen Interesses verbietet.

5.6 Sollten die in **Anhang 1** genannten personenbezogenen Daten an Sub-Datenverarbeiter außerhalb der EU/des EWR übermittelt werden, muss in dem genannten Vertrag festgehalten werden, dass die im Land des für die Datenverarbeitung Verantwortlichen geltenden Datenschutzgesetze für die Sub-Datenverarbeiter gelten. Ist der empfangende Sub-Datenverarbeiter in der EU/EWR ansässig, muss in diesem Vertrag mit dem Datenverarbeiter zudem festgehalten werden, dass die spezifischen gesetzlichen Anforderungen des empfangenden EU-Landes in Bezug auf Datenverarbeiter, beispielsweise hinsichtlich der Meldepflicht gegenüber nationalen Behörden, eingehalten werden müssen.

5.7 Der Datenverarbeiter ist verpflichtet, schriftliche Verträge mit Sub-Datenverarbeitern innerhalb der EU/EWR abzuschließen. Bei Sub-Datenverarbeitern außerhalb der EU/des EWR muss der Datenverarbeiter für ausreichende Übermittlungsmechanismen sorgen und einen Vertrag mit dem Sub-Datenverarbeiter abschließen. Dies geschieht durch den Abschluss von Standardverträgen in Übereinstimmung mit den Standardvertragsklauseln der EU-Kommission („Standardverträge“) auf der Grundlage der Richtlinie 2021/914/EU vom 4. Juni 2021.

5.8 Zum Zeitpunkt der Unterzeichnung dieses Vertrags beauftragt der Datenverarbeiter die in **Anhang 3** aufgeführten Sub-Datenverarbeiter.

6. Haftung

6.1 Die Haftung der Parteien wird durch den Hauptvertrag geregelt.

6.2 Die Haftung der Parteien in Bezug auf Schadenersatz im Rahmen dieses Vertrags wird durch den Hauptvertrag geregelt.

7. Datum des Inkrafttretens und Beendigung

7.1 Dieser Vertrag tritt zeitgleich mit dem Hauptvertrag in Kraft. Im Falle der Beendigung des Hauptvertrags endet auch der vorliegende Vertrag. Der Datenverarbeiter unterliegt jedoch weiterhin den in diesem Vertrag festgeschriebenen Verpflichtungen, solange der Datenverarbeiter personenbezogene Daten im Auftrag des Datenverantwortlichen verarbeitet.

7.2 Nach Beendigung der Verarbeitungsdienstleistungen ist der Datenverarbeiter verpflichtet, auf Verlangen des Datenverantwortlichen alle personenbezogenen Daten zu löschen oder an den Datenverantwortlichen zurückzugeben sowie vorhandene Kopien zu löschen, sofern die Aufbewahrung der personenbezogenen Daten nicht durch EU- oder nationales Recht vorgeschrieben ist.

8. Geltendes Recht und Gerichtsbarkeit

8.1 Jegliche Ansprüche oder Streitigkeiten, die sich aus oder im Zusammenhang mit diesem Vertrag ergeben, müssen von einem zuständigen Gericht in erster Instanz in derselben Rechtsordnung und mit derselben Rechtswahl wie im Hauptvertrag festgelegt geregelt werden.

9. Unterschriften

Im Namen des
Datenverantwortlichen:

_____

[Name] [Titel]

Im Namen des Datenverarbeiters:

_____

Ronni Engelhardt CEO

Anhang 1

Kategorien von betroffenen Personen, Arten von personenbezogenen Daten und Anweisungen

1. Kategorien von betroffenen Personen:

- Der Datenverarbeiter verarbeitet Kontaktinformationen über aktuelle, potenzielle oder ehemalige Kunden und/oder Mitglieder, Mitarbeiter, Lieferanten, Geschäfts- und Kooperationspartner und Affiliates des Datenverantwortlichen.
- Der Datenverarbeiter stellt sein System zur Verwaltung der Daten des Datenverantwortlichen als gehosteten Dienst zur Verfügung, und es ist dem Datenverarbeiter nicht möglich, alle Kategorien von betroffenen Personen zu bestimmen. Wenn der Datenverantwortliche Daten über weitere Kategorien von betroffenen Personen bei dem Datenverarbeiter hostet, ist der Datenverantwortliche verpflichtet, diese Informationen zu erfassen.

2. Arten von personenbezogenen Daten:

- Kontakt- und Identifikationsinformationen einschließlich E-Mail-Adressen
- IP-Adressen
- Domainnamen
- Benutzernamen
- Informationen zur Mitgliedschaft
- Analysen und Nutzungsdaten
- Auftragsgeschichte und Informationen
- Verträge
- Kommunikation
- Support
- Bilder
- Es können weitere Arten von personenbezogenen Daten erhoben werden

3. Anweisungen

Service

Der Datenverarbeiter kann personenbezogene Daten der betroffenen Personen zu dem Zweck verarbeiten, die Dienstleistungen des Hauptvertrags zu erbringen, weiterzuentwickeln, zu verwalten und zu managen. Dazu gehört auch die Sicherstellung der Stabilität und der Betriebszeit unserer Server sowie die Erfüllung gesetzlicher Anforderungen.

Aufbewahrungszeitraum

Die in unseren Systemen gespeicherten/gehosteten personenbezogenen Daten werden innerhalb eines angemessenen Zeitraums nach vollständiger Beendigung des Hauptvertrags durch den Datenverantwortlichen gelöscht oder anonymisiert. Ausnahmen bilden Daten, bei denen der Datenverarbeiter gesetzlich verpflichtet ist, sie länger zu speichern. Diese Art von Daten wird in der Regel innerhalb von acht Wochen gelöscht, kann aber auch früher gelöscht werden. Andere Arten von Daten, die beispielsweise in Logdateien gespeichert sind, werden nach einer angemessenen Zeit, in der Regel innerhalb von 8 Wochen, beim Datenverarbeiter gelöscht.

Ort der Verarbeitung

Die Verarbeitung personenbezogener Daten im Rahmen dieses Vertrags darf nur mit vorheriger schriftlicher Zustimmung des Datenverantwortlichen an anderen Orten als der Adresse des Datenverarbeiters und der Adresse der Sub-Datenverarbeiter, wie in **Anhang 3** aufgeführt, erfolgen.

Inspektion des Datenverarbeiters

Der Datenverarbeiter ist verpflichtet, einmal pro Jahr auf eigene Kosten einen Audit-/Inspektionsbericht von einer dritten Partei einzuholen, der die Einhaltung dieses Vertrags und der Anhänge durch den Datenverarbeiter überprüft. Der Bericht oder ein anderes Audit-Format muss so schnell wie möglich nach der Erstellung an den Datenverantwortlichen weitergeleitet oder auf der Website des Datenverantwortlichen veröffentlicht werden.

Anhang 2
Sicherheitsvorkehrungen

Domain	Praktiken
Organisation der Informationssicherheit	**Verantwortlicher für die Sicherheit.** One.com hat einen Sicherheitsbeauftragten ernannt, der für die Koordinierung und Überwachung der Sicherheitsvorschriften und -verfahren verantwortlich ist. Der Sicherheitsbeauftragte wird von einer Gruppe von Führungskräften unterstützt und angewiesen. **Sicherheitsrollen und Verantwortlichkeiten.** Mitarbeiter von One.com, die Zugang zu Kundendaten haben, unterliegen einer Geheimhaltungspflicht, die bei der Einstellung ausdrücklich betont wird und die auch weiterhin beachtet werden muss. **Risikomanagement** One.com führt im Rahmen des Risikomanagements eine kontinuierliche Risikobewertung durch, bevor es die Kundendaten verarbeitet oder Dienstleistungen anbietet. Der Bereich des Risikomanagements ermöglicht es, sich auf relevante Bedrohungen zu konzentrieren, indem die Risiken über das akzeptierte Maß hinaus priorisiert, strukturiert und reduziert werden. Ein Backup ist implementiert. Der Datenverarbeiter speichert seine Sicherheitsdokumente nach Ablauf der Gültigkeit gemäß seinen Aufbewahrungsvorschriften.
Anlagenverwaltung	**Inventarisierung der Assets.** Der Datenverarbeiter führt ein Verzeichnis aller Medien, auf denen Kundendaten gespeichert sind. Der Zugang zu den Verzeichnissen dieser Medien ist auf das Personal des Datenverarbeiters beschränkt, das schriftlich autorisiert wurde, diesen Zugang zu erhalten. **Asset-Handling** - One.com führt eine Klassifizierung der Kundendaten durch, um sie zu identifizieren und den Zugang zu ihnen angemessen zu beschränken. - Die Mitarbeiter des Datenverarbeiters müssen die Genehmigung des Datenverarbeiters einholen, bevor sie Kundendaten auf mobilen Endgeräten speichern, remote auf Kundendaten zugreifen oder Kundendaten außerhalb der Einrichtungen des Datenverarbeiters verarbeiten.
Sicherheit im Bereich Human Resources	**Sicherheitstraining.** One.com informiert seine Mitarbeiter über relevante Sicherheitsverfahren und ihre jeweilige Rolle sowie über neue Bedrohungen usw., bei denen die Mitarbeiter eine wichtige Rolle spielen.
Physische Sicherheit und Umweltsicherheit	**Physischer Zugang zu den Einrichtungen**. One.com beschränkt den Zugang zu Einrichtungen, in denen sich Informationssysteme zur Verarbeitung von Kundendaten befinden, auf bestimmte autorisierte Personen. **Physischer Zugang zu den Komponenten.** One.com gewährleistet einen ausreichenden Schutz der Datenträger mit Kundendaten. **Schutz vor Störungen.** One.com setzt eine Vielzahl von Industriestandardsystemen ein, um sich gegen Datenverluste aufgrund von Stromausfällen, Überschwemmungen, Feuer oder Leitungsstörungen zu schützen.

Domain	Praktiken
	Komponentenentsorgung. One.com setzt branchenübliche Verfahren ein, um Kundendaten zu löschen, wenn diese nicht mehr benötigt werden.
Kommunikation und Betriebsmanagement	**Unternehmenspolitik.** One.com pflegt Sicherheitsdokumente, in denen die Sicherheitsmaßnahmen sowie die entsprechenden Verfahren und Verantwortlichkeiten der Mitarbeiter, die Zugang zu den Kundendaten haben, beschrieben werden. **Verfahren zur Datenwiederherstellung** - One.com speichert Kopien von Kundendaten und Datenwiederherstellungsverfahren an einem anderen Ort als dem Ort, an dem sich die primäre EDV-Anlage zur Verarbeitung der Kundendaten befindet. - One.com verfügt über spezielle Verfahren für den Zugriff auf Kopien von Kundendaten. **Schadsoftware.** One.com setzt Anti-Malware-Kontrollen ein, um zu verhindern, dass Schadsoftware unbefugten Zugriff auf Kundendaten erhält. Dies schließt auch Schadsoftware ein, die aus öffentlichen Netzwerken stammt. Auch ein Virenschutz wurde implementiert. **Aufzeichnung von Ereignissen.** One.com protokolliert den Zugriff auf und die Nutzung von Informationssystemen, die Kundendaten enthalten, oder ermöglicht es dem Kunden, diese zu protokollieren. Dabei werden die Zugriffs-ID, der Zeitpunkt, die erteilte oder verweigerte Genehmigung und die entsprechende Aktivität registriert. **Verschlüsselung.** Die Kommunikation über das Internet zwischen Systemen, die persönliche Daten verarbeiten, erfolgt verschlüsselt.
Zugriffskontrolle	**Zugriffspolitik.** One.com pflegt ein Verzeichnis der Sicherheitsrechte von Personen, die Zugang zu Kundendaten haben. **Zugangsberechtigung** - One.com deaktiviert Authentifizierungsnachweise, die über einen Zeitraum von maximal sechs Monaten nicht verwendet wurden. - One.com identifiziert die Personen, die autorisierten Zugriff auf Daten und Ressourcen erteilen, ändern oder löschen dürfen. - One.com gewährleistet, dass für den Fall, dass mehr als eine Person Zugang zu Systemen mit Kundendaten hat, die einzelnen Personen getrennte Kennungen/Logins haben. **Geringste Rechte** - One.com beschränkt den Zugang zu Kundendaten auf die Personen, die einen solchen Zugang benötigen, um ihre Aufgabe zu erfüllen. **Integrität und Vertraulichkeit**

Domain	Praktiken
	- One.com weist seine Mitarbeiter an, administrative Sitzungen beim Verlassen des Firmengeländes zu deaktivieren oder wenn Computer anderweitig unbeaufsichtigt gelassen werden. - One.com speichert Passwörter derart, dass sie während ihrer Gültigkeit nicht lesbar sind. **Authentifizierung** - One.com setzt branchenübliche Verfahren zur Identifizierung und Authentifizierung von Benutzern ein, die versuchen, auf Informationssysteme zuzugreifen. - Basieren die Authentifizierungsmechanismen auf Passwörtern, verlangt der Datenverarbeiter, dass die Passwörter regelmäßig erneuert werden. - One.com gewährleistet, dass deaktivierte oder abgelaufene Kennungen nicht an andere Personen vergeben werden. - One.com überwacht bzw. ermöglicht dem Kunden die Überwachung wiederholter Versuche, sich mit einem ungültigen Passwort Zugang zum Informationssystem zu verschaffen. - One.com wendet branchenübliche Verfahren zur Deaktivierung von beschädigten oder versehentlich preisgegebenen Passwörtern an. - One.com wendet zum Schutz von Passwörtern branchenübliche Verfahren an, einschließlich Verfahren zur Wahrung der Vertraulichkeit und Integrität von Passwörtern bei der Vergabe und Verteilung sowie bei der Speicherung. **Netzwerkdesign.** One.com verfügt über Kontrollen, die verhindern, dass Personen Zugriffsrechte nutzen, die ihnen nicht zugewiesen wurden, um sich dadurch Zugang zu Kundendaten zu verschaffen, für die sie keine Zugriffsberechtigung haben.
Management von Informationssicherheitsvorfällen	**Prozess zur Reaktion auf Vorfälle** - One.com führt ein Protokoll über Sicherheitsverletzungen mit einer Beschreibung der Verletzung, dem Zeitraum, den Folgen der Verletzung, dem Namen des Meldenden und demjenigen, dem die Verletzung gemeldet wurde, sowie dem Verfahren zur Wiederherstellung der Daten. - Bei jeder Sicherheitsverletzung, die einen Sicherheitsvorfall darstellt, erfolgt die Benachrichtigung durch One.com ohne unangemessene Verzögerung und in jedem Fall innerhalb von 72 Stunden. - One.com erfasst die Weitergabe von Kundendaten oder ermöglicht es dem Kunden, diese zu erfassen. Dies beinhaltet auch, welche Daten weitergegeben wurden, an wen und zu welchem Zeitpunkt.
Management der Geschäftskontinuität	- One.com verfügt über Notfall- und Krisenpläne für die Einrichtungen, in denen sich die Informationssysteme der Datenverarbeiter befinden, mit denen Kundendaten verarbeitet werden.

Domain	Praktiken
	- Der redundante Speicher von One.com und die Verfahren zur Wiederherstellung von Daten sind derart konzipiert, dass der Versuch unternommen wird, die Kundendaten in ihrem ursprünglichen oder zuletzt replizierten Zustand vor dem Zeitpunkt ihres Verlusts oder ihrer Zerstörung zu rekonstruieren.

Anhang 3
Liste von Sub-Datenverarbeitern

Lieferant	Standort	Funktion	Aktualisiert
Global Connect A/S	DK	Rechenzentrum	20.02.2021
Interxion	DK	Rechenzentrum	12.04.2021
Interxion	DK/UK/NL/FR/DE	PoP (Point of Presence)	12.04.2021
Equinix	SE	PoP (Point of Presence)	12.04.2021