Table of Contents

# Artikel 1: Definitionen

1. \*\* PERSÖNLICHE DATEN \*\*: Alle Informationen zu tun zu einer identifizierten oder identifizierbaren natürlichen Person (“Person betroffen “), wie durch die allgemeinen Vorschriften auf Datenschutz (DSGVO).
2. \*\* Behandlungsmanager \*\*: die natürliche oder juristische Person, öffentliche Autorität, Dienst oder eine andere Organisation, die allein oder gemeinsam mit anderen die Zwecke und die Mittel bestimmt Verarbeitung personenbezogener Daten.
3. \*\* Subunternehmer \*\*: Die natürliche oder juristische Person, die Behörde Öffentlichkeit, Dienst oder andere Organisation, die Daten verarbeitet persönlich im Namen des Controllers.
4. \*\* Behandlung \*\*: Jeder Betrieb oder jede Reihe von Operationen durchgeführt oder nicht automatisierte Prozesse verwenden und auf Daten angewendet werden oder Sätze personenbezogener Daten.
5. \*\* Datenverletzung \*\*: Ein Sicherheitsverstoß, der dazu führt versehentlich oder illegal zerstören, Verlust, Veränderung, nicht authorisierte Offenlegung von Daten Mitarbeiter übertragen, erhalten oder auf andere Weise verarbeitet oder zugreifen Nicht zu solchen Daten autorisiert.
6. \*\* Datenübertragung \*\*: Jede Übertragung von Daten eines Zeichens Mitarbeiter außerhalb des europäischen Wirtschaftsbereichs (EEE), einschließlich an ein Drittland oder eine internationale Organisation.
7. \*\* Cloud -Service \*\*: Jede Behandlung, Speicher- oder Management -Service personenbezogene Daten vom Subunternehmer übertragen Wolkeninfrastruktur.

# Artikel 2: Objekt

Der Zweck dieses Anhangs besteht darin, die Bedingungen und Methoden zu definieren Verarbeitung personenbezogener Daten im Rahmen des Vertrags Main, einschließlich der Nutzung von Cloud -Diensten.Sie zielt darauf ab garantieren die Konformität der Parteien mit den Verpflichtungen, die sich aus der DSGVO ergeben und Französische Gesetze im Zusammenhang mit dem Schutz personenbezogener Daten.

# Artikel 3: Verpflichtungen des Controllers

1. \*\* Licuity der Behandlung \*\*: Der Controller verpflichtet sich an Verarbeitung personenbezogener Daten rechtmäßig, loyal und transparent gemäß den Artikeln 5 und 6 der DSGVO.
2. \*\* Ermittelte Zwecke \*\*: Persönliche Daten nicht muss nur für bestimmte Zwecke gesammelt werden, explizit und legitim und dürfen nicht behandelt werden anschließend mit diesen Zwecken nicht kompatibel.
3. \*\* Datenminimierung \*\*: Der Controller muss Stellen Sie sicher, dass die gesammelten Daten angemessen sind, relevant und beschränkt auf das, was in Bezug auf notwendig ist Zwecke, für die sie verarbeitet werden.
4. \*\* Datengenauigkeit \*\*: Es liegt in der Verantwortung des Controllers Um sicherzustellen, dass personenbezogene Daten genau sind und, Gegebenenfalls auf dem neuesten Stand.
5. \*\* Datensicherheit \*\*: Der Controller muss eingesetzt werden In Betrieb die entsprechenden technischen und organisatorischen Maßnahmen Um ein an das Risiko angepasster Sicherheitsniveau in Übereinstimmung mit dem Risiko zu gewährleisten Artikel 32 der DSGVO.Dies schließt die regelmäßige Bewertung von Maßnahmen ein Wolkensicherheit verwendet.

# Artikel 4: Verpflichtungen des Subunternehmers

1. \*\* Behandlung gemäß den Anweisungen \*\*: Der Subunternehmer beginnt personenbezogene Daten nur unter Anweisungen zu verarbeiten von den Behandlungsmanagern dokumentiert, einschließlich in Bedenken von personenbezogenen Daten zu a Dritte Länder oder eine internationale Organisation, es sei denn a Die gesetzliche Anforderung erfordert dies.
2. **Confidentialité** : Le Sous-traitant doit veiller à ce que les personnes autorisées à traiter les données à caractère personnel s’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.
3. **Sécurité des traitements** : Le Sous-traitant s’engage à mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir la sécurité des données à caractère personnel qu’il traite, einschließlich derjenigen, die über Cloud -Dienste verarbeitet werden, gemäß den Artikel 32 der DSGVO.
4. \*\* nachfolgende Subunternehmer \*\*: Der Subunternehmer darf nicht Verwenden Sie einen anderen Subunternehmer ohne vorherige Genehmigung geschrieben und spezifisch für den Controller.Bei Der Subunternehmer muss autorisierte Unteraufträge sicherstellen, dass der nachfolgende Subunternehmer die gleichen Verpflichtungen respektiert Datenschutz.
5. \*\* Unterstützung für den Behandlungsmanager \*\*: Der Subunternehmer muss Unterstützung des Controllers so weit wie möglich, seine Verpflichtungen in Bezug auf die Sicherheit von zu zahlen Daten, Benachrichtigung über Datenverstöße, Realisierung Auswirkungsanalyse zum Datenschutz und Vorherige Konsultationen mit den Kontrollbehörden.
6. \*\* Datenort \*\*: Der Subunternehmer muss bereitstellen Löschen Sie Informationen zu Speicher- und Verarbeitungsorten Daten in der Cloud -Infrastruktur und stellen Sie sicher, dass diese Stellen entsprechen den geltenden Schutzvorschriften Daten.

# Artikel 5: Beschreibung der Behandlungen

Der Subunternehmer ist berechtigt, im Namen des Managers von zu behandeln Verarbeitung, personenbezogene Daten erforderlich, um bereitzustellen Dienstleistungen.Die Art und Kategorie der Operationen, die durchgeführt werden Persönliche Daten werden vom Manager von definiert Behandlung gemäß den spezifischen Bedürfnissen jedes Dienstes.DER Die Behandlungszwecke werden vom Manager von bestimmt Behandlung und dem Subunternehmer mitgeteilt.Natur und Kategorie Persönliche Daten verarbeitet werden von der angegeben Behandlungsleiter.Die Kategorien der betroffenen Personen sind vom Controller identifiziert.Für die Ausführung von Dienste, die der Controller zur Verfügung stellt Unterauftragung der erforderlichen Informationen.Die Dauer der Behandlung ist vom Behandlungsmanager gemäß den Anforderungen von festgelegt Dienstleistungen zur Verfügung gestellt.

# Artikel 6: Rechte der betroffenen Personen

1. \*\* Zugriff und Berichtigung \*\*: Der Controller und der Der Subunternehmer muss den betroffenen Personen erlauben, Sport zu treiben ihr Recht, auf ihre Daten zuzugreifen und sie zu korrigieren Persönlicher Charakter gemäß den Artikeln 15 und 16 der DSGVO.
2. \*\* Löschung und Begrenzung der Behandlung \*\*: Menschen besorgt muss in der Lage sein, ihre Rechte an der Löschung von auszuüben ihre Daten (Recht auf vergessen werden) oder die Verarbeitung begrenzen, Gemäß den Artikeln 17 und 18 der DSGVO.
3. \*\* Datenportabilität \*\*: Der Controller muss Stellen Sie gegebenenfalls sicher persönlicher Charakter der betroffenen Personen gemäß den Begriffen Artikel 20 der DSGVO.
4. \*\* Opposition \*\*: Die betroffenen Personen müssen in der Lage sein, trainieren zu können Ihr Recht, sich der Verarbeitung ihrer personenbezogenen Daten zu widersetzen Gemäß Artikel 21 der DSGVO.

# Artikel 7: Sicherheitsmessung und Vertraulichkeitsmessung

Der Subunternehmer verpflichtet sich insbesondere, die Maßnahmen einzuführen ausreichend, um die Sicherheit und Vertraulichkeit von Daten zu gewährleisten Persönliche betraut und verarbeitet im Rahmen von Diensten, nämlich insbesondere:

* Implementieren Sie geeignete technische und organisatorische Maßnahmen Personenbezogene Daten vor Zerstörung zu schützen Zufälliger oder illegaler, zufälliger Verlust, Veränderung, Entführten Gebrauch, nicht autorisierte Verbreitung oder Zugang sowie das gegen eine andere Form einer illegalen Behandlung;
* Verwenden Sie keine personenbezogenen Daten für Ihre eigenen Konto oder im Namen von Dritten und nicht ohne übertragen die vorherige schriftliche Genehmigung des Controllers oder Endkunde;
* Stellen Sie sicher, dass Personen, die zur Verarbeitung von Daten zu verarbeiten sind Persönlicher Charakter unterliegen angemessene Verpflichtungen von Vertraulichkeiten;
* Machen Sie keine Kopien oder Duplikationen von Daten von Natur Mitarbeiter ohne vorherige schriftliche Genehmigung des Managers von Behandlungs- oder Endkunde (es sei denn, dies ist erforderlich die Erbringung der vom Dienstleister in der erbrachten Dienstleistungen Rahmen des Vertrags);
* Informieren Sie den Controller über einen versehentlichen Zugang oder nicht über autorisiert an personenbezogenen Daten, von einem Verstoß von Vorschriften für personenbezogene Daten oder irgendwelche Verdacht auf einen solchen Verstoß, so bald wie möglich und wenn, wenn Möglicherweise 48 Stunden nach dem Lesen nach dem Lesen.
* Abhängig von der Auswahl der Behandlungsmanager löschen oder kehren Sie zurück Personenbezogene Daten oder senden Sie sie bis zum Ende des Vertrags zurück, und Zerstören Sie bestehende Kopien, es sei denn, eine gesetzliche Verpflichtung zu halten;
* Implementieren Sie eine Sicherheitsrichtlinie für Informationssysteme und Management von logischen und physischen Zugangsberechtigten insbesondere, dass er während der gesamten Dauer von aufrechterhalten und weiterentwickeln muss VERTRAG.

# Artikel 8: Benachrichtigung von Datenverstößen

En cas de violation de données à caractère personnel, le Sous-traitant doit notifier cette violation au Responsable de traitement sans délai indu après en avoir pris connaissance. Cette notification doit inclure toutes les informations pertinentes permettant au Responsable de traitement de notifier cette violation à l’autorité de contrôle compétente et, le cas échéant, aux personnes concernées conformément à l’article 33 du RGPD. La notification doit préciser l’impact potentiel auf den in der Cloud gehosteten Daten und den Maßnahmen für die ergriffenen Maßnahmen für Abhilfe.

# Artikel 9: Datenübertragungen außerhalb der Europäischen Union

Jede Übertragung personenbezogener Daten in ein Drittland oder Eine internationale Organisation kann nur unterliegen Einhaltung der Bedingungen der DSGVO, insbesondere in Artikeln 44 bis 50. Der Controller muss sicherstellen, dass diese Garantien garantiert werden Angemessen sind vorhanden, wie z. B. Standard -Vertragsklauseln genehmigt von der Europäischen Kommission oder der Existenz einer Entscheidung Angemessenheit.

# Artikel 10: Dauer und Ende der Behandlung

Am Ende des Hauptvertrags verfolgt der Subunternehmer gemäß dem Anweisungen vom Controller, um alle zu löschen personenbezogene Daten oder zurück zum Manager von Behandlung und zu zerstören bestehende Kopien, es sei denn, eine gesetzliche Verpflichtung Gegenteil.Diese Verpflichtung enthält auch Daten, die gespeichert sind Backup unterstützt in der Cloud -Infrastruktur, es sei denn a Die gesetzliche Verpflichtung erfordert ihre Erhaltung.

# Artikel 11: Dokumentation und Audits

Der Subunternehmer wird den Behandlungsmanager anbieten Alle Informationen, die erforderlich sind, um die Einhaltung der Einhaltung der Einhaltung Verpflichtungen in diesem Anhang vorgesehen und werden die Audits genehmigen. einschließlich Inspektionen, durch den oder einen anderen Controller Der von letzteren vorgeschriebene Zuhörer, um die Einhaltung der Einhaltung Dieser Anhang und die DSGVO.Der Subunternehmer muss auch a halten Register der Verarbeitungsaktivitäten gemäß Artikel 30 der DSGVO und geben Sie Compliance -Berichte zur Cloud -Infrastruktur an gebraucht.

# Artikel 12: Register der Behandlungsaktivitäten

Der Subunternehmer muss auch ein Aktivitätenregister von behalten Behandlung gemäß Artikel 30 der DSGVO und Berichte Einhaltung der verwendeten Cloud -Infrastruktur.Dieses Register Enthält mindestens: - Name und Kontaktdaten des Controllers und gegebenenfalls die mit Verantwortung für die Behandlung verantwortlich, die Vertreterin von Verantwortlich für Datenschutz- und Datenschutzdelegierter;- - Die Beschreibung der Kategorien der betroffenen Personen und der Kategorien personenbezogene Daten;- Behandlungszwecke;- DER Kategorien von Empfängern, zu denen personenbezogene Daten waren oder wird kommuniziert, einschließlich Empfänger in Drittländern oder internationale Organisationen;- Die Haltbarkeit von Daten;- die allgemeine Beschreibung der technischen Maßnahmen und organisatorische Sicherheit implementiert.

Auf schriftliche Anfrage vom Controller, der Endkunde oder Jede zuständige Behörde, der Subunternehmer, hat 15 Arbeitstage zur Kommunikation einer Kopie des genannten Registers aus dem Empfangsdelate -Anfrage. # Artikel 13: nachfolgende Subunternehmer

Der Subunternehmer muss möglicherweise einen (oder) Anbieter verwenden (en) / externe Lieferant für die Verwaltung von Dienstleistungen spezifisch für den Vertrag.Zu diesem Zweck kann der Subunternehmer sein führte unter seiner Verantwortung zu einem Rekrut, einen (oder) Subunternehmer (en) Zweitens in dem einzigen Zweck, einen Teil der Dienste bereitzustellen notwendig für das infogierte System. Der Subunternehmer verpflichtet sich, eine verbindliche Rechtsgesetze mit abzuschließen Jeder nachfolgende Subunternehmer, den er für die Behandlung initiiert Daten, um die Einhaltung der Anforderungen der DSGVO und der Gleiche Verpflichtungen wie in Artikel 20.2 vorgesehen.Besonders, Der Subunternehmer muss sicherstellen, dass der Subtrahierer, den er hat Rekrutierte präsentiert ausreichende Garantien für die Umsetzung von notwendige Sicherheitsmaßnahmen. En cas de défaillance du sous-traitant ultérieur dans le respect de ses obligations en matière de protection des Données personnelles, le Sous-traitant demeurera pleinement responsable à l’égard du Responsable de traitement, sans préjudice des droits des Personnes concernées prévus aux articles 79 et 82 du RGPD.

La liste des sous-traitants subséquents autorisés est la suivante:

1. Interxion
2. Data4
3. Telehouse
4. Iron Mountain

Während der Vertragsausführung kann der Controller Zu jederzeit mit dem Subunternehmer zugreifen, um zu aktualisieren besagte Liste.Ungeachtet der oben genannten wird der Subunternehmer durch benachrichtigen geschrieben an den Behandlungsmanager Die Liste der Subunternehmer später regelmäßig Update mit Ausnahme einer Änderung Haupt Subunternehmer.

# Artikel 14: Verantwortung

Der Controller und der Subunternehmer erkennen, dass sie kann für den durch a verursachten Schaden verantwortlich gemacht werden Verarbeitung personenbezogener Daten nicht gemäß DSGVO und anwendbare französische Gesetze.Der Subunternehmer ist verantwortlich für durch die Behandlung verursachte Schäden, wenn sie den Verpflichtungen nicht eingehalten haben DSGVO speziell für Subunternehmer anwendbar oder wenn es in wirkte außerhalb der rechtlichen Anweisungen des Controllers oder Im Gegensatz zu diesen.

# Artikel 15: Änderungen

Jede Änderung dieses Anhangs muss Gegenstand einer Bestätigung sein geschrieben von beiden Parteien.Änderungen müssen sein gemäß den Anforderungen der DSGVO und den französischen Gesetzen in Bezug auf die Schutz personenbezogener Daten.

# Artikel 16: anwendbares Recht und kompetente Gerichtsbarkeit

Dieser Anhang unterliegt dem französischen Recht.Jeder relative Streit zu seiner Interpretation oder seiner Ausführung wird eine ausschließliche Kompetenz sein Französische Gerichte.Im Falle von Divergenz zwischen den Versionen Linguistik dieses Anhangs, die französische Version wird sich durchsetzen.