Anlage – Gemeinsame Bestimmungen für die Verarbeitung personenbezogener Daten

1. Definitionen

Für die Zwecke dieser Anlage gelten alle Definitionen, die in der Verordnung (EU) 2016/679 (DSGVO) festgelegt sind.

„**Datenschutzgesetze**“ bezeichnet alle Gesetze oder Vorschriften in Bezug auf Datenschutz und Cybersicherheit, die die Verarbeitung personenbezogener Daten im Rahmen des Vertrags regeln, einschließlich der EU-Verordnung 2016/679 (DSGVO) und spezifischer nationaler Datenschutzgesetze, die für den Kunden und Expensya gelten.

2. Gegenstand

Das vorliegende Dokument ist Teil der Anlagen zu den Allgemeinen Geschäftsbedingungen und bildet zwischen dem Dienstanbieter und dem Kunden vereinbarten „Gemeinsamen Bestimmungen für die Verarbeitung personenbezogener Daten”.

3. Auslegung

Ein Verweis auf ein Gesetz oder eine Rechtsvorschrift schließt einen Verweis auf eine untergeordnete Gesetzgebung ein und stellt ebenfalls einen Verweis auf dieses Gesetz, diese Rechtsvorschrift oder diese untergeordnete Gesetzgebung im Zusammenhang mit einer Änderung, Vereinheitlichung, Umnummerierung, Wiederinkraftsetzung oder Ersetzung (mit oder ohne Änderung) derselben nach dem Datum der Anlage sowie auf ein Gesetz, eine Rechtsvorschrift oder eine untergeordnete Gesetzgebung, die sie (mit oder ohne Änderung) vereinheitlichen, wieder in Kraft setzen oder ersetzen sollen, dar.

Verweise im Singular schließen den Plural ein und umgekehrt.

Begriffe, die auf die Begriffe/Ausdrücke „inbegriffen“, „insbesondere“ und „im Besonderen“ folgen oder ähnliche Begriffe oder Ausdrücke werden uneingeschränkt ausgelegt und beschränken folglich nicht die Bedeutung der ihnen vorausgehenden Ausdrücke.

4. Verpflichtung des Dienstanbieters als Daten-Subunternehmer

Sofern zwischen den Parteien schriftlich nicht anders vereinbart, verarbeitet der Dienstanbieter die personenbezogenen Daten unter der Aufsicht des Kunden in seiner Eigenschaft als für die Datenverarbeitung Verantwortlicher ausschließlich zum Zweck der Erfüllung seiner Verpflichtungen aus diesen Allgemeinen Geschäftsbedingungen oder zu einem anderen im Vertrag ausdrücklich genehmigten Zweck und in Übereinstimmung mit den geltenden Datenschutzgesetzen.

Der Dienstanbieter verarbeitet personenbezogene Daten nicht in einer Weise, die mit den für den Dienstanbieter und/oder den Kunden geltenden Datenschutzgesetzen unvereinbar ist.

Insbesondere verpflichtet sich der Dienstanbieter:

- die personenbezogenen Daten nur für den Zweck/die Zwecke, der/die Gegenstand des Vertrags ist/sind zu verarbeiten;

- die personenbezogenen Daten in Übereinstimmung mit den dokumentierten Anweisungen des Kunden zu verarbeiten;
- die Vertraulichkeit der im Rahmen des Vertrags verarbeiteten personenbezogenen Daten zu garantieren;
- sicherzustellen, dass die Personen, die gemäß dem Vertrag zur Verarbeitung der personenbezogenen Daten berechtigt sind:
    - sich zur Wahrung der Vertraulichkeit verpflichten oder einer entsprechenden gesetzlichen Vertraulichkeitsverpflichtung unterliegen,
    - die notwendige Schulung im Bereich des Schutzes personenbezogener Daten erhalten.
- bei seinen Werkzeugen, Produkten, Anwendungen oder Diensten von Anfang an standardmäßig die Grundprinzipien des Datenschutzes zu berücksichtigen;
- den Kunden vor jedweder Verarbeitung zu informieren, wenn der Dienstanbieter gesetzlich verpflichtet ist, die personenbezogenen Daten anders als in Übereinstimmung mit den Anweisungen des Kunden zu verarbeiten, es sei denn, das entsprechende Gesetz verbietet eine solche Verarbeitung aus Gründen des öffentlichen Interesses; in diesem Fall wird der Dienstanbieter den Kunden informieren, sobald es das Gesetz erlaubt;
- den Kunden bei der Erfüllung seiner Verpflichtungen gemäß den Datenschutzgesetzen, einschließlich seiner Verpflichtung, Aufforderungen zur Ausübung der Rechte der betroffenen Personen nachzukommen, zu unterstützen. Diese Hilfe ist in einer Weise zu leisten, die es dem Kunden ermöglicht, seinen Verpflichtungen rechtzeitig und vollständig nachzukommen;
- mit dem Kunden bei der Ausarbeitung und der Aktualisierung des Verzeichnisses der Datenverarbeitungsaktivitäten des Kunden zusammenzuarbeiten, aber nur hinsichtlich vom Dienstanbieter durchgeführter Datenverarbeitungsaktivitäten für den Kunden im Rahmen der vorliegenden Allgemeinen Geschäftsbedingungen.

Ist der Dienstanbieter der Ansicht, dass eine Anweisung des Kunden einen Verstoß gegen die geltenden Datenschutzgesetze darstellt, wird er den Kunden gemäß den oben genannten Verpflichtungen unverzüglich über diesen Sachverhalt informieren.

Darüber hinaus muss der Dienstanbieter, wenn er verpflichtet ist, Daten in ein Drittland oder an eine internationale Organisation zu übermitteln, den Kunden gemäß geltender Datenschutzgesetze vor der Verarbeitung über diese gesetzliche Verpflichtung informieren, es sei denn, das entsprechende Gesetz verbietet diese Inkenntnissetzung aus wichtigen Gründen des öffentlichen Interesses.

Der Dienstanbieter versichert ferner, keinen Grund zu der Annahme zu haben, dass ihn die ihn oder seine Aktivitäten betreffende Gesetzgebung daran hindert, die vom Kunden erteilten Anweisungen zu befolgen oder seine aus diesem Vertrag erwachsenden Verpflichtungen zu erfüllen. Ist zu erwarten, dass eine Gesetzesänderung erhebliche negative Auswirkungen auf die in dieser Anlage aufgeführten Gewährleistungen und Verpflichtungen haben wird oder ist der Dienstanbieter der Ansicht, dass die Anweisungen des Kunden einen Verstoß gegen Datenschutzgesetze oder Entscheidungen einer Aufsichtsbehörde darstellen, unterrichtet der Dienstanbieter den Kunden, sobald er von einer solchen Änderung Kenntnis erhält.

Der Dienstanbieter führt ein Verzeichnis des Personals und der Dienstleister, die zur Verarbeitung personenbezogener Daten befugt sind, und stellt sicher, dass dieses Personal und seine Subunternehmer:

- an Vertraulichkeitsverpflichtungen gebunden sind, die mit denen identisch sind, an die der Kunde und der Dienstanbieter gebunden sind und die in den vorliegenden Allgemeinen Geschäftsbedingungen genannt wurden;

- eine angemessene Schulung erhalten haben und hinsichtlich der Verarbeitung personenbezogener Daten angemessenen beaufsichtigt werden;
- einen Zugang zu den personenbezogenen Daten haben, der streng auf das beschränkt ist, was für die Erbringung der Dienstleistungen und/oder die Erfüllung der Verpflichtungen von Expensya im Rahmen der vorliegenden Allgemeinen Geschäftsbedingungen erforderlich ist.

5. Sicherheitsmaßnahmen

Der Dienstanbieter hat angemessene technische, physische und organisatorische Maßnahmen ergriffen und wird diese aufrechterhalten (einschließlich einer obligatorischen Vertraulichkeitsklausel für seine Mitarbeitenden, Vertreter und Subunternehmer), um die personenbezogenen Daten vor versehentlicher oder illegaler Zerstörung, versehentlichem Verlust, Änderung oder unbefugter Offenlegung oder unbefugtem Zugriff zu schützen.

Der Dienstanbieter informiert den Kunden unverzüglich, wenn er in seiner Eigenschaft als Daten-Subunternehmer von einem Sicherheitsvorfall, unbefugtem Zugriff, Veruntreuung, Verlust, Schaden oder einer anderen tatsächlichen oder vermuteten Beeinträchtigung in Bezug auf die Sicherheit, Vertraulichkeit oder Integrität der von seinen Mitarbeitenden verarbeiteten personenbezogenen Daten erfährt.

Wird eine Sicherheitsverletzung festgestellt, ergreift der Dienstanbieter alle erforderlichen Maßnahmen, um eine mögliche neue Verletzung zu verhindern, und gewährt dem Kunden unverzüglich jede erforderliche Unterstützung, damit dieser als für die Datenverarbeitung Verantwortlicher seiner Informationspflicht nachkommen kann.

Darüber hinaus hat der Dienstanbieter einen Datenschutzbeauftragten (DSB) ernannt und stellt sicher, dass dieser DSB in der Lage ist, seine Aufgaben in Übereinstimmung mit den Datenschutzgesetzen zu erfüllen.

Kontaktdaten des DSB des Anbieters:
Virtual DPO SAS
42 Rue Manin 75019 Paris
Handels- und Gesellschaftsregister (RCS) 830 490 603 Paris
E-Mail: contact@virtual-dpo.fr

6. Zusammenarbeit

6.1. Allgemeine Bestimmungen

Auf schriftliche Anfrage des Kunden stellt der Dienstanbieter dem Kunden unverzüglich alle in seinem Besitz befindlichen nützlichen Informationen zur Verfügung, um es ihm zu ermöglichen, die Anforderungen der Datenschutzgesetze zu erfüllen.

Die vom DSB des Dienstanbieters durchgeführte Konformitätsprüfung des Dienstanbieters enthält eine detaillierte Beschreibung der vom Dienstanbieter ergriffenen technischen, physischen und organisatorischen Maßnahmen, um personenbezogene Daten vor versehentlicher oder unrechtmäßiger Zerstörung oder versehentlichem Verlust, vor Änderung, unbefugter Offenlegung oder unbefugtem Zugriff zu schützen, sowie die Aufzeichnung der Datenverarbeitungsaktivitäten des Dienstanbieters für den Kunden.

Auf schriftliche Anfrage des Kunden stellt der Dienstanbieter spätestens binnen zehn (10) Arbeitstagen eine elektronische Kopie der Konformitätsprüfung zur Verfügung.

Die Merkmale und Besonderheiten seiner Lösung betreffend hat sich der Dienstanbieter dafür entschieden, keine Datenschutzfolgenabschätzung (Privacy Impact Assessment, PIA) durchzuführen. Verlangt der Kunde die Durchführung einer Datenschutzfolgenabschätzung über die vom Dienstanbieter in seiner Eigenschaft als Daten-Subunternehmer durchgeführten Verarbeitungsvorgänge, muss der Dienstanbieter dennoch die entsprechende Ausrüstung und technische Unterstützung zur Verfügung stellen. Die Parteien vereinbaren, dass die Kosten der Datenschutzfolgenabschätzung ausschließlich vom Kunden in seiner Eigenschaft als für die Datenverarbeitung Verantwortlicher getragen werden. Falls erforderlich, kann der Dienstanbieter dem Kunden die für die Durchführung einer solchen Analyse aufgewendete Zeit sowie das Personal und die Ausrüstung in Rechnung stellen, was der Kunde versteht und akzeptiert.

6.2. Anfragen von betroffenen Personen

Gemäß den Anweisungen des Kunden beantwortet der Dienstanbieter Anfragen von Datensubjekten nach ihren persönlichen Daten:

Hat der Kunde darum gebeten, dass alle Anfragen an seine eigenen Abteilungen weitergeleitet werden, wird der Dienstanbieter davon absehen, den betroffenen Personen direkt zu antworten, und diese Anfragen an die Kontaktperson unter der vom Kunden im Vertrag angegebenen Adresse weiterleiten;

Hat der Kunde den Dienstanbieter gebeten, alle Anfragen in seinem Namen zu beantworten, wird sich der Dienstanbieter bemühen, nach bestem Wissen präzise Antworten zu geben. Sollte es aufgrund fehlender Informationen nicht möglich sein, die Fragen zu beantworten, wird der Dienstanbieter die Anfragen an die vom Kunden im Vertrag angegebene Kontaktperson unter der vom Kunden angegebenen Adresse weiterleiten.

Der Dienstanbieter informiert den Kunden unverzüglich über Anfragen von betroffenen Personen zur Ausübung ihrer Rechte gemäß den Datenschutzgesetzen.

6.3. Datenschutzverletzung

Im Falle einer Verletzung von persönlichen Daten informiert der Dienstanbieter den Kunden so schnell wie möglich, spätestens jedoch sechsunddreißig (36) Stunden nach Bekanntwerden einer solchen Verletzung, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unerlaubten Offenlegung von übertragenen, gespeicherten oder anderweitig verarbeiteten persönlichen Daten oder zum unberechtigten Zugriff auf solche Daten führt.

Der Dienstanbieter stellt dem Kunden so bald wie möglich nach erfolgter Benachrichtigung über die Verletzung von personenbezogenen Daten und im Rahmen des Möglichen die folgenden Informationen zur Verfügung:

Die Kategorien und die ungefähre Anzahl der von der Datenschutzverletzung betroffenen Personen;

Die Kategorien und die ungefähre Anzahl der betroffenen Datensätze mit personenbezogenen Daten;

Eine Beschreibung der wahrscheinlichen Folgen der Verletzung von personenbezogenen Daten;

Eine Beschreibung der Schritte, die der Dienstanbieter zur Behebung der Verletzung von personenbezogenen Daten unternommen hat oder vorschlägt, einschließlich gegebenenfalls der Maßnahmen zur Milderung nachteiliger Folgen.

Verfügt der Dienstanbieter zum Zeitpunkt der ursprünglichen Mitteilung nicht über alle im vorstehenden Absatz vorgesehenen Informationen, nimmt er die Informationen, über die er zum Zeitpunkt der Mitteilung verfügt, in die ursprüngliche Mitteilung auf und übermittelt die fehlenden Informationen schnellstmöglich.

7. Zugang Dritter zu Daten – Spätere Subunternehmer

Der Dienstanbieter stellt sicher, dass seine Mitarbeitenden, Vertreter und Subunternehmer die Integrität, Vertraulichkeit und Sicherheit der personenbezogenen Daten achten und bewahren.

Im Falle der Vergabe von Unteraufträgen verpflichtet sich der Dienstanbieter, seinen Subunternehmern vertraglich ein Maß an Verpflichtungen aufzuerlegen, das hinsichtlich des Datenschutzes dem in dieser Anlage und in den Datenschutzgesetzen vorgesehenen mindestens gleichwertig ist. Der Dienstanbieter bleibt gegenüber dem Kunden allein für die Erfüllung seiner Verpflichtungen durch seine Subunternehmer haftbar.

Der Dienstanbieter stellt dem Kunden in der Anlage **Verzeichnis der Datenverarbeitungsaktivitäten** eine Liste seiner derzeitigen Subunternehmer zur Verfügung, die direkt oder indirekt Datenverarbeitungstätigkeiten an allen oder einem Teil der Kundendaten durchführen dürfen, wobei der Kunde dem Dienstanbieter erlaubt, die Dienste dieser Subunternehmer in Anspruch zu nehmen.

Der Dienstanbieter verpflichtet sich, die Dienste von Subunternehmern nur dann in Anspruch zu nehmen, wenn diese für die Erfüllung des Vertrags unbedingt erforderlich sind.

Der Dienstanbieter verpflichtet sich, nur Subunternehmer in Anspruch zu nehmen, die die folgenden Kriterien erfüllen:

- Ihr Sitz befindet sich in einem Mitgliedsland der Europäischen Union oder des Europäischen Wirtschaftsraums; oder
- Sie sind in einem Land niedergelassen, das nach Ansicht der Europäischen Kommission ein angemessenes Schutzniveau im Rahmen der Datenschutzgesetze bietet; oder
- Sie sind einem den Sicherheitsregeln der europäischen Kommission entsprechenden Prozess zertifiziert; oder
- Sie bieten entsprechende Garantien nach Artikel 46 der DSGVO.

8. Internationale Transfers von personenbezogenen Daten

Wenn der Dienstanbieter direkt oder indirekt personenbezogene Daten in Länder außerhalb der Europäischen Union übermittelt oder wenn ein vom Dienstanbieter vorgesehener Subunternehmer die personenbezogenen Daten in Länder außerhalb der Europäischen Union oder in ein Land übermitteln könnte, das kein angemessenes Schutzniveau im Sinne der Datenschutzgesetze gewährleistet, ist der Zugang zu diesen Daten nur nach Einholung der Zustimmung des Kunden und der Umsetzung der in Artikel 46 der DSGVO vorgesehenen angemessenen Garantien möglich.

Die Tochtergesellschaft des Dienstanbieters, SARL Expensya Tunisie ((Pepinotech Tunisia), zu 99,92 % im Besitz von SA Expensya, hat ihren Sitz in Tunesien. Die für die IT-Entwicklung und -Unterstützung zuständige Tochtergesellschaft kann im Rahmen der spezifischen Dienstleistungen, die sie im Zusammenhang mit der Lösung erbringt, auf personenbezogene Daten zugreifen. Expensya SA und Expensya Tunisia haben Standardvertragsklauseln unterzeichnet, die gewährleisten, dass personenbezogene Daten in Übereinstimmung mit den Datenschutzgesetzen übermittelt werden können.

Der Kunde bestätigt, darüber informiert worden zu sein, und ist einverstanden, dass sich die Tochtergesellschaft von Expensya in Tunesien befindet und Zugang zu persönlichen Daten haben kann.

Auf schriftliche Anfrage des Kunden stellt der Dienstleister spätestens innerhalb von zehn (10) Arbeitstagen eine elektronische Kopie der mit dem Subunternehmen SARL Expensya Tunisie (Pepinotech Tunisia) unterzeichneten Vertragsklauseln zur Verfügung.

9. Prüfung

Auf Anfrage stellt der Dienstanbieter dem Kunden auf elektronischem Weg alle Dokumente zur Verfügung, die erforderlich sind, um die Einhaltung seiner Verpflichtungen als Subunternehmer im Rahmen der vorliegenden Allgemeinen Geschäftsbedingungen nachzuweisen. Die Kosten für eine Übermittlung dieser Unterlagen auf einem anderen Weg gehen zu Lasten des Kunden.

Der Kunde kann vom Dienstanbieter zusätzliche Erklärungen verlangen, wenn die zur Verfügung gestellten Dokumente es ihm nicht ermöglichen, die Einhaltung der Verpflichtungen eines Subunternehmers im Rahmen der vorliegenden Allgemeinen Geschäftsbedingungen oder dieser Anlage zu überprüfen.

Der Kunde sendet in diesem Fall per Einschreiben mit Empfangsbestätigung einen Antrag an den Dienstanbieter, in dem er seinen Antrag auf zusätzliche Erklärungen begründet und dokumentiert. Der Dienstanbieter verpflichtet sich, dem Kunden so schnell wie möglich zu antworten.

Sollte der Kunde die Vollständigkeit der bereitgestellten Informationen trotz der Antwort des Dienstanbieters anfechten oder falls eine unmittelbare Gefahr für die Sicherheit von personenbezogenen Daten besteht, kann der Kunde auf seine Kosten und gemäß den zwischen dem Dienstanbieter und dem Kunden vereinbaren Modalitäten eine Vor-Ort-Prüfung durchführen.

Anlage – Verzeichnis der Datenverarbeitungsaktivitäten

1. Gegenstand

Das vorliegende Dokument ist Teil der Anlagen zu den Allgemeinen Geschäftsbedingungen und bildet das „Verzeichnis der Datenverarbeitungsaktivitäten".

2. Beschreibung der Datenverarbeitung

Zweck der Verarbeitung

☒ Der Zweck der Datenverarbeitung durch den Subunternehmer ist insbesondere in der Anlage **Dienstleistungsbroschüre** dargelegt

☐ Andere: ……

Einstufung der von der Verarbeitung ausgehenden Risiken

Risiken	Auswirkungen auf Personen	Hauptrisikoquellen	Hauptbedrohungen	Bestehende oder geplante Maßnahmen	Schwe
Illegitimer Datenzugriff	Zugriff auf Reisekostenabrechnungen:	Zugangsbetrug / Passwortdiebstahl	Benutzer / Passwortoffenlegung	SSO	Mäßig
Unerwünschte Datenänderung	Betrug bei Reisekostenabrechnungen	Zugangsbetrug / Passwortdiebstahl	Benutzer / Passwortoffenlegung	SSO / Audit der Änderungen	Mäßig
Datenverlust	Datenverlust auf Reisekostenabrechnungen, Auswirkungen auf die Buchhaltung	Vernichtung von Expensya-Daten	Bedrohungen von außerhalb des Anbieters	Redundanz, beweiskräftige Archivierung	Stark

Dauer der Verarbeitung:

☒ Die Verarbeitungsdauer entspricht der Vertragslaufzeit,

☐ Andere: ……

Die vom Subunternehmer im Rahmen des Vertrags durchgeführte Verarbeitung umfasst:

☒ Datensammlung oder -aufzeichnung

☒ Organisieren oder Strukturieren der Daten

☒ Hosting oder Speicherung der Daten

☒ Anpassung oder Änderung der Daten

☒ Extraktion oder Aufrufen der Daten

☐ Verwendung der Daten

☒ Weitergabe der Daten durch Übertragung, Verbreitung oder jede andere Form von Bereitstellung

☐ Abgleich oder Verknüpfung von Daten

☒ Beschränkung (Sperrung) der Daten

☒ Löschung oder Zerstörung der Daten

☐ Andere Verarbeitung:……...……

Zweck der Verarbeitung

☒ Der Zweck der Datenverarbeitung ist im Vertrag, insbesondere in der Anlage Dienstleistungsbroschüre, dargelegt.

☐ Andere: ……

Daten-Kategorien

☒ Name, Titel, Funktionen	☒Identifikationsnummer (n)
☐Fotos oder Aufzeichnungen wie Video- oder Telefongesprächsaufnahmen	☐Vertragsbezogene Informationen (vertragliche Beziehungen, Interesse an Produkten, Dienstleistungen oder Verträgen)
☐Persönliche Kontaktdaten (z.B. Telefon, E-Mail)	☐Historie Begünstigte(r)
☒Geschäftliche Kontaktdaten (z.B. Firma, Adresse, Telefon, E-Mail)	☐Bankverbindung (Bankverbindung, IBAN, Kreditkartennummer, Transaktionen)
☐Daten zum Privatleben (Lebensgewohnheiten, Familienstand, etc.)	☒Rechnungs- oder Zahlungsdaten
☒Daten zum Berufsleben (Lebenslauf, Berufsausbildung, Auszeichnungen usw.)	☐Bewertungs- oder Ratingdaten
☐Wirtschafts- und Finanzinformationen (Einkommen, Finanzen, Steuern, usw.)	☐Verbindungsdaten (IP-Adresse, Protokolle usw.)

☒Standortdaten (Bewegungen, GPS-Daten, GSM etc.)

☐ Andere: …… ……

Spezielle Daten-Kategorien

☐ Daten, die Aufschluss über ethnische Herkunft geben

☐ Daten, die Aufschluss über politische Meinungen geben

☐ Daten, die Aufschluss über religiöse oder philosophische Überzeugungen geben

☐ Daten, die Aufschluss über Gewerkschaftszugehörigkeit geben

☐ Genetische Daten

☐ Biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person

☐ Gesundheitsdaten

☐ Daten zum Sexualleben oder zur sexuellen Orientierung

☐ Daten im Zusammenhang mit strafrechtlichen Verurteilungen oder Straftaten

☐ Eindeutige nationale Identifikationsnummer (NIR für Frankreich)

Kategorien von betroffenen Personen:

☒ Mitarbeitende und ehemalige Mitarbeitende (Arbeitnehmer, Auszubildende)

☐Besucher

☐Interessenten

☐Begünstigte

☐ Abonnenten

☒ Lieferanten, Berater

☐ Handelsvertreter

☐Ansprechpartner

☐ Andere: …….....

3. Liste der autorisierten Subunternehmer

#	Firmenname	Adresse	Land	Durchgeführte Verarbeitung
1.	Microsoft Azure	Amsterdam	Niederlande	Speicherung und Hosting der Lösung Expensya
2.	Expensya Tunesien	Les Berges du Lac 2, Tunis	Tunesien	Kunden-Support
3.	CDC Arkhineo	122-120 Rue Réaumur – 75002 PARIS	Frankreich	Beweiskräftige Archivierung

4. Abbildung der Datenströme außerhalb des Europäischen Wirtschaftsraums oder in das Vereinigte Königreich

Ein Datenfluss außerhalb des Europäischen Wirtschaftsraums findet nur dann statt, wenn der Kunde eine Anfrage an den in Tunesien ansässigen Support des Dienstanbieters stellt. Das für die Bearbeitung der Anfrage zuständige Mitglied des Support-Teams des Dienstanbieters greift in einem solchen Fall auf die spezifisch erwähnten Daten auf den in Amsterdam gehosteten Microsoft Azure-Servern zu. Während dieser Support-Tätigkeit findet kein effektiver Datentransfer oder Backup statt.

5. Maßnahmen zur Gewährleistung der Übereinstimmung der Verarbeitung mit den Datenschutzbestimmungen

5.1. Sicherheit

IT-Sicherheitspolitik des Subunternehmens: auf Anfrage erhältlich

Verschlüsselung:

☒ Verfahren zur Verwaltung von Schlüsseln und Zertifikaten

☒Datenverschlüsselung

☒Verschlüsselung der Datenübertragung

☒Hashfunktion: SHA-256, SHA-512 oder SHA-3

☒Speicherung von Passwörtern: HMAC Verwendung von SHA-256, bcrypt, scrypt oder PBKDF2

☐ Andere: …… ……

☐ Symmetrische Verschlüsselung: AES oder AES-CBC mit 128-Bit-Schlüsseln

☐ Unterschriften: RSA-SSA-PSS wie in PKCS#1 v2.1 angegeben mit Modulen und geheimen Exponenten von mindestens 2048 Bit oder 3072 Bits mit öffentlichen Exponenten, zur Verschlüsselung, größer als 65536

Schutz des IT-Netzes des Subunternehmers:

☐Beschränkung des Internetzugangs

☒Verwaltung von WLan-Netzwerken

☐Obligatorische Nutzung eines VPN für den Fernzugriff

☒Die Verwaltungsschnittstellen sind nicht direkt über das Internet zugänglich.

☒Begrenzung der Netzwerkflüsse

☒Umsetzung der ANSSI-Empfehlungen in Bezug auf Website-Sicherheit, TLS und WLan

☐Automatische Geräteerkennung

☒Einrichtung von Einbruchserkennungssystemen

☒Netzwerk-Unterteilung

☐ Andere:
……
..

Rückverfolgbarkeit:

☒Einrichtung von Protokollsystemen

☒Einrichtung eines Verfahrens zur Überwachung der Verwendung der Verarbeitung

☒Einrichtung eines spezifischen Schutzes für Protokollierungsausrüstung und protokollierte Daten

☒Periodische Überprüfung der Ereignisprotokolle

☒Einrichtung eines Verfahrens zur Meldung von Anomalien oder Sicherheitsvorkommnissen

☐ Andere: ……

Verwaltung der Berechtigungen:

☒ Festlegen von Berechtigungsprofilen

☒ Durchführung einer jährlichen Überprüfung der Berechtigungen

☒ Löschung der Zugriffsberechtigungen für Benutzer, sobald sie nicht mehr berechtigt sind, auf einen Raum oder eine Computerressource zuzugreifen, sowie nach Ende ihres Vertrags

☒Einrichtung von Richtlinien zur Zugangskontrolle

☐ Andere:
……

Verwaltung der Authentifizierung:

☒ Einrichtung einer eindeutigen Benutzeridentifizierung pro Benutzer

☐ Verwendung von Passwortmanagern, um für jede Abteilung über andere Passwörter zu verfügen

☒ Verbot von Gemeinschaftskonten

☒ Befolgen der Empfehlung „Passwortauthentifizierung: Die zusätzlichen Sicherheitsmaßnahmen“ der frz. Datenschutzbehörde (CNIL) vom 4. September 2017

☒Sichere Speicherung von Passwörtern

☒ Starke Authentifizierung

☒ Bezugnahme auf die von der ANSSI veröffentlichten Regeln und Empfehlungen zu Authentifizierungsmechanismen, wenn starke Authentifizierungsmechanismen implementiert werden, insbesondere in Bezug auf die Anlagen B36 und B17, die jeweils von Authentifizierungsmechanismen bzw. kryptographische Mechanismen handeln

☒ Begrenzung der Anzahl der Zugriffsversuche

☒ Obligatorische Passwort-Erneuerung

☒ Sperrung des Kontos bei ausbleibender Passwort-Erneuerung
☐ Andere:
……

Sicherheitsmaßnahmen:

☒ Verwendung von regelmäßig aktualisierter Anti-Virus-Software
☒ Automatische Sicherheitsaktualisierung
☒ Suche nach Ursprung und Spuren eines Einbruchs, wenn die Sicherheit eines Rechners beeinträchtigt wurde
☒ Sicherheitsüberwachung
☒ Verschlüsselung von mobilen Endgeräten und mobilen Speichermedien
☒ Implementierung von Mechanismen zum Schutz vor Diebstahl und zur Begrenzung seiner Auswirkungen
☐Obligatorische Nutzung eines VPN für den Fernzugriff
☒ Anwendung der ANSSI-Empfehlungen in Bezug auf die Sicherung von Websites, TLS und WLan
☒Einrichtung von Einbruchserkennungssystemen
☒ Anwendung der ANSSI-Empfehlungen in Bezug auf die Absicherung der Verwaltung von IT-Systemen und bewährte Praktiken in Bezug auf die Sicherung des zentralen Verzeichnisdienstes Active Directory
☒ Einrichtung eines IT-Wiederherstellungs- und Geschäftskontinuitätsplans
☒ Test der Backup-Wiederherstellung und der Anwendung des Geschäftskontinuitäts- oder Wiederherstellungsplans
☒ Einrichtung eines sicheren Verfahrens zur Datenlöschung
☐ Verwendung von Software zur Löschung von Daten, die von der ANSSI (frz. nationale Agentur für Sicherheit der Informationssysteme) zertifiziert ist
☐ Andere: …….

5.2. Privacy by design/Privacy by default

☒ Standard- und Mindesteinstellungen durch Benutzer von Datenerfassungsvorgängen
☒ Nicht-obligatorisches Ausfüllen eines optionalen Felds
☒ Es werden nur Daten gesammelt, die für den Zweck der Verarbeitung erforderlich sind
☒ Automatische und selektive Löschung von Daten am Ende der Verarbeitung
☒ Verwaltung von IT-Berechtigungen und Zugriffsrechten nach „Einzeldaten“ oder auf Anfrage
☐ Andere: …….

5.3. Daten-Governance

☒ Anwendung der 25 Bezugsrahmen der CNIL-Beratung Nr. 2017-219 vom 13. Juli 2017
☒ Ernennung eines Datenschutzbeauftragten
☒Einrichtung von geeigneten Datenschutzrichtlinien
☐ Andere: ……..

5.4. Schulung

☒ Regelmäßige Schulung über die DSGVO-Grundprinzipien für die an der Verarbeitung Beteiligten

☐ Andere: ……..