

Anlage Nr. 1:

Einbeziehungsvertrag zur Anwendung der EU-Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Art. 28 Abs. 7 DSGVO

zwischen



- im Folgenden „Verantwortlicher“ genannt -


und

RUBICON IT GmbH
gesetzlich vertreten durch Markus Leimhofer (Prokurist)
Gonzagagasse 16, 1010 Wien, Österreich

- im Folgenden „Auftragsverarbeiter“ genannt -

gemeinsam auch die „Parteien“ genannt.

Präambel

Im Rahmen der Leistungserbringung nach dem am  zwischen den Parteien geschlossenen EVB-IT Cloudvertrag (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragsverarbeiter mit personenbezogenen Daten umgeht. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang mit personenbezogenen Daten durch den Auftragsverarbeiter zur Durchführung des Hauptvertrags, insbesondere durch die Vereinbarung der EU-Standardvertragsklauseln.

1. Vertragsgegenstand

1.1 Mit diesem Vertrag vereinbaren die Parteien die Geltung der EU-Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates (**Anlage „EU-**

Standardvertragsklauseln“, im Folgenden kurz „EU-Standardvertragsklauseln“)¹. Die EU-Standardvertragsklauseln sind auch dann wirksam einbezogen, sollten sie dem vorliegenden Vertrag nicht als Anlage beigelegt sein.

- 1.2 Zudem fügen die Parteien den EU-Standardvertragsklauseln mit diesem Vertrag gemäß Klausel 2 lit. b der EU-Standardvertragsklauseln („Unabänderbarkeit der Klauseln“) ergänzende Regelungen hinzu.
- 1.3 Die Bestimmungen dieses Vertrags finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragsverarbeiter, seine Mitarbeiter, Subunternehmer gleich welchen Grades, deren Mitarbeiter bzw. die sonstigen Erfüllungsgehilfen des Auftragsverarbeiters mit personenbezogenen Daten in Berührung kommen oder in Berührung kommen können.

2. Geltung der EU-Standardvertragsklauseln

- 2.1 Die Parteien vereinbaren die Geltung der EU-Standardvertragsklauseln mit nachfolgenden Optionen.
- 2.2 Soweit in den EU-Standardvertragsklauseln entweder auf die DSGVO (OPTION 1) oder auf die Verordnung (EU) 2018/1725 (OPTION 2) verwiesen wird, gilt vorliegend OPTION 1, also die Bezugnahme auf die hier einschlägige DSGVO.
- 2.3 Die fakultative Klausel 5 der EU-Standardvertragsklauseln („Kopplungsklausel“) kommt nicht zur Anwendung.
- 2.4 Klausel 7.7 lit. a) der EU-Standardvertragsklauseln („Einsatz von Unterauftragsverarbeitern“) wird dahingehend konkretisiert, dass OPTION 1 („VORHERIGE GESONDERTE GENEHMIGUNG“) mit einem Zeitraum für die Einreichung des Antrags auf gesonderte Genehmigung von mindestens vier Wochen vor Beauftragung des Unterauftragsverarbeiters gilt.

3. Vergütung und Aufwendungen

Soweit der Auftragsverarbeiter im Zusammenhang mit der Durchführung der Pflichten nach den EU-Standardvertragsklauseln Leistungen erbringt oder ihm Aufwendungen entstehen, sind diese mit der laufenden pauschalen Vergütung aus dem Hauptvertrag abgegolten. Insbesondere hat der Auftragsverarbeiter auch keinen gesonderten Anspruch auf Zahlung einer

¹ Abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021D0915> (zuletzt abgerufen am 15.08.2022). Bitte drucken Sie das Dokument aus und fügen Sie es als Anlage bei. Die dort mit aufgeführten Anhänge I bis IV sind ebenfalls auszufüllen und dem Einbeziehungsvertrag beizufügen.

Vergütung nach Aufwand für die im Zusammenhang mit Klausel 7.6. („Dokumentation und Einhaltung der Klauseln“) zu erbringenden Leistungen.

4. Haftung, Vertragsstrafe

- 4.1 Für Schäden des Verantwortlichen im Zusammenhang mit einer Verletzung von Pflichten aus diesem Vertrag bzw. einem Verstoß gegen die gesetzlichen Datenschutzbestimmungen durch den Auftragsverarbeiter gelten die gesetzlichen Haftungsregelungen. Etwaige zwischen den Parteien an anderer Stelle (z.B. im Hauptvertrag) vereinbarte Haftungsbeschränkungen finden insoweit keine Anwendung.
- 4.2 Macht ein Dritter gegen den Verantwortlichen wegen der Verletzung datenschutzrechtlicher Vorschriften Ansprüche geltend, ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen durch Bereitstellung von Informationen und Unterlagen bei der Rechtsverteidigung gegenüber dem Dritten zu unterstützen. Soweit die Ansprüche begründet sind und ihre Ursache im Verantwortungsbereich des Auftragsverarbeiters haben, wird der Auftragsverarbeiter den Verantwortlichen von den Ansprüchen freistellen. Darüber hinaus wird der Auftragsverarbeiter dem Verantwortlichen die aus der Rechtsverletzung resultierenden weitergehenden Schäden ersetzen und insbesondere den Verantwortlichen von den Kosten einer angemessenen Rechtsverteidigung freistellen, es sei denn, der Auftragsverarbeiter hat diese Schäden nicht zu vertreten.
- 4.3 Der Auftragsverarbeiter verpflichtet sich für den Fall eines schuldhaften Verstoßes des Auftragsverarbeiters oder eines seiner Erfüllungsgehilfen gegen eine wesentliche Verpflichtung aus den EU-Standardvertragsklauseln zur Zahlung einer vom Verantwortlichen im Einzelfall nach billigem Ermessen zu bestimmenden und im Fall des Streits über die Angemessenheit vom zuständigen Gericht zu überprüfenden Vertragsstrafe. Wesentliche Verpflichtungen im Sinne von Satz 1 sind insbesondere die Verpflichtungen aus folgenden Klauseln der EU-Standardvertragsklauseln:
- 4.3.1 Klausel 7.1 lit. a) Satz 1 (Verarbeitung personenbezogener Daten nur auf dokumentierte Weisung des Verantwortlichen);
- 4.3.2 Klausel 7.2 („Zweckbindung“);
- 4.3.3 Klausel 7.3. („Dauer der Verarbeitung personenbezogener Daten“);
- 4.3.4 Klausel 7.4. („Sicherheit der Verarbeitung“);
- 4.3.5 Klausel 7.5. („Sensible Daten“);

- 4.3.6 Klausel 7.6. („Dokumentation und Einhaltung der Klauseln“);
 - 4.3.7 Klausel 7.7. („Einsatz von Unterauftragsverarbeitern“);
 - 4.3.8 Klausel 7.8. („Internationale Datenübermittlungen“);
 - 4.3.9 Klausel 8 („Unterstützung des Verantwortlichen“);
 - 4.3.10 Klausel 9 („Meldung von Verletzungen des Schutzes personenbezogener Daten“).
- 4.4 Die Vertragsstrafen werden auf Schadensersatzansprüche angerechnet. Die Anwendbarkeit des § 341 Absatz 3 BGB ist ausgeschlossen.
- 4.5 Weitergehende Ansprüche und Rechte des Verantwortlichen nach dem Gesetz bleiben hiervon unberührt.

5. Vertraulichkeit

Der Auftragsverarbeiter ist verpflichtet, auch über das Ende des vorliegenden Vertrags hinaus die ihm im Zusammenhang mit dem vorliegenden Vertrag bekannt gewordenen personenbezogenen Daten vertraulich zu behandeln. Weitergehende Verpflichtungen des Auftragsverarbeiters aus dem Hauptvertrag, einer gegebenenfalls geschlossenen Vertraulichkeitsvereinbarung, sonstigen Vereinbarungen und dem Gesetz bleiben hiervon unberührt.

6. Rangfolge und Widersprüche

Die Vereinbarungen zwischen den Vertragsparteien stehen in folgender Rangfolge, wobei Bestimmungen der zuerst genannten Vereinbarungen bei Widersprüchen Vorrang vor den danach genannten besitzen:

- die EU-Standardvertragsklauseln,
- die Bestimmungen dieses Einbeziehungsvertrags nebst der Anhänge I bis IV und
- die Bestimmungen des Hauptvertrags.

7. Schlussbestimmungen

- 7.1 Dieser Vertrag unterliegt ausschließlich dem Recht der Bundesrepublik Deutschland.

- 7.2 Ausschließlicher Gerichtsstand für alle Streitigkeiten im Zusammenhang mit diesem Vertrag ist der Geschäftssitz des Verantwortlichen. Für Klagen des Verantwortlichen gegen den Auftragsverarbeiter gilt zudem jeder weitere gesetzliche Gerichtsstand. Zwingende gesetzliche Bestimmungen über ausschließliche Gerichtsstände bleiben von dieser Regelung unberührt.
- 7.3 Die Gerichtsstandsvereinbarungen nach Ziffer 7.2 bestimmen sich ausschließlich nach dem Recht der Bundesrepublik Deutschland.
- 7.4 Sollte eine Bestimmung oder ein Teil einer Bestimmung dieses Vertrags unwirksam sein oder werden, so wird die Gültigkeit des Vertrags im Übrigen nicht berührt. Die Parteien verpflichten sich, die unwirksame Regelung durch eine solche zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Regelung möglichst nahe kommt bzw. entspricht und den Anforderungen des Art. 28 DSGVO gerecht wird. Die vorstehenden Sätze gelten für die Ausfüllung einer sich ergebenden Regelungslücke entsprechend.

8. Anlagen und Anhänge

Folgende Anlage und Anhänge sind mit allen Bestandteilen Gegenstand des vorliegenden Vertrags:

Anlage 11: „EU-Standardvertragsklauseln“²

9. Sonstige Informationen zur Verarbeitung

9.1 Beschreibung der Verarbeitung

9.1.1 Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Bürger (Finder und Verlierer, Empfänger von Fundgegenständen)
- Mitarbeiter des Verantwortlichen

9.1.2 Kategorien personenbezogener Daten, die verarbeitet werden:

- Daten des Finders (Anrede/Geschlecht, Name, Anschrift, Telefonnummern, E-Mail-Adresse, Ausweisdaten, Datum der Anzeige, Abgabestelle, Funddatum, Fundort)
- Daten des Verlierers (Anrede/Geschlecht, Name, Anschrift, Geburtsdatum, Telefonnummern, E-Mail-Adresse, Ausweisdaten, Datum der Meldung, Meldestelle, Verlustdatum, Verlustort, bevorzugte Sprache)

² Abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021D0915> (zuletzt abgerufen am 15.08.2022). Bitte drucken Sie das Dokument aus und fügen Sie es als Anlage bei. Die dort mit aufgeführten Anhänge I bis IV sind ebenfalls auszufüllen und dem Einbeziehungsvertrag beizufügen.

- Allfällige am Fundgegenstand befindliche personenbezogene Daten (z.B. Name des Verlierers, Geburtsdatum/-jahr, Ausweisnummer, Bankomatkartenummer, Sozialversicherungsnummer, ...)
- Daten des vom Verlierer bzw. vom Finder bevollmächtigten Empfängers von Fundgegenständen (Anrede/Geschlecht, Name, Anschrift, Telefonnummern, E-Mail-Adresse, Ausweisdaten)
- Anwenderdaten (Benutzername, Rolle/Berechtigung, Änderungshistorie)

9.1.3 Arten der Verarbeitung

- Speicherung, Anpassung, Veränderung, Auslesen, Abfragen, Abgleich, Verknüpfung, Einschränkung, Löschen oder Vernichtung;

9.1.4 Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

- Die Zwecke der Verarbeitung sind Hosting und Betrieb der Fundservicesoftware Nova Find und gegebenenfalls damit zusammenhängenden Support- und Migrationsleistungen

9.1.5 Dauer der Verarbeitung

- Die Dauer der Verarbeitung richtet sich nach dem Hauptvertrag

9.2 Technische und organisatorische Maßnahmen gemäß Art 32 DSGVO

9.2.1 Zutrittskontrolle

Ein unbefugter Zutritt wird verhindert, wobei der Begriff räumlich zu verstehen ist.

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- Zutrittskontrollsystem: Ausweisleser, Chipkarte
- Schlüssel / Schlüsselvergabe
- Türsicherung (Stand der Technik)
- Zutrittsberechtigung richtet sich nach der Funktion und dem Aufgabenbereich der Mitarbeiter
- Genehmigungsprozess für Zutrittsberechtigung
- Videoüberwachung an neuralgischen Stellen
- Alarmanlage
- Besucher werden am Betriebsgelände nicht unbeaufsichtigt gelassen

9.2.2 Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme, sowie deren unbefugte Inbetriebnahme wird verhindert.

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- Kennwortrichtlinien (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)

- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- Einrichtung eines Benutzerstammsatzes (Domänenverzeichnis – AD) pro User; administrative Konten sind benannt
- Datenschutzgerechtes Löschen und Wiederverwenden von Speichermedien
- Trennung von Administration- und Produktionsbereich

9.2.3 Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen, sowie Zugriffe auf Daten und Programme außerhalb eingeräumter Berechtigungen werden verhindert.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Genehmigungsprozess für Berechtigungen
- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Auswertungen (im Bedarfs- und Verletzungsfall)
- Netzwerksegmentierung

9.2.4 Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten werden geregelt.

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Transportverschlüsselung mit Hilfe von sicheren Transportprotokollen
- Tunnelverbindung (VPN = Virtual Private Network)
- Protokollierung

9.2.5 Eingabekontrolle / Protokollierungspflicht

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege wird gewährleistet, insbesondere um Änderungen, Abfragen und Übermittlungen nachvollziehen zu können.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- Protokollierungs- und Protokollauswertungssysteme
- Zentrales Logging auf einem vom Produktivsystem getrennten Loggingsystem
- Auswertungen (im Bedarfs- und Verletzungsfall)

9.2.6 Auftragskontrolle

Die weisungsgemäße Auftragsverarbeitung wird gewährleistet.

Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer

- Eindeutige Vertragsgestaltung
- Kriterien zur Auswahl des Auftragnehmers
- Kontrolle der Vertragsausführung

9.2.7 Verfügbarkeitskontrolle

Die Daten werden gegen zufällige Zerstörung oder Verlust geschützt, um insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Daten, Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

Maßnahmen zur Datensicherung (physikalisch / logisch):

- Prozesse, die sicherstellen, dass die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann
- Backup-Verfahren
- Unterbrechungsfreie Stromversorgung (USV)
- getrennte Aufbewahrung
- Virenschutz / Firewall
- Notfallplan
- Monitoring

9.2.8 Trennungskontrolle / Aufgabenverteilung

Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden auch getrennt verarbeitet.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- Funktionstrennung
 - Produktion
 - Test
 - Entwicklung

9.2.9 Organisationskontrolle

Die Organisation hat Personen und Prozesse implementiert, die eine nachhaltig dem Datenschutz verpflichtete Struktur sicherstellen.

Maßnahmen, die sicherstellen, dass die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird:

- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung
- Datenschutzkonzept und Datensicherheitspolicies
- Regelmäßige Datenschutzeschulungen der Mitarbeiter
- Verpflichtung auf das Datengeheimnis nach § 6 DSGVO 2018 bzw Art 28 Abs 3b DSGVO

9.2.10 Dokumentationspflicht

Sämtliche technische und organisatorische Maßnahmen sind in einer geeigneten Form zu dokumentieren, um die Kontrolle und Beweissicherung zu gewährleisten.

Maßnahmen, die sicherstellen, dass der Auftraggeber die Ausgestaltung und Einhaltung der Datensicherheitsmaßnahmen kontrollieren kann:

- Nachvollziehbare, schriftliche Dokumentation der Sicherheitsmaßnahmen
- Regelmäßige Aktualisierung

Verantwortlicher

_____, den

Auftragsverarbeiter

Wien, den

(Name des Unterzeichnenden)

(Position des Unterzeichnenden)

Laura Thürauer
(Name des Unterzeichnenden)

Head of Sales „lost & found“
(Position des Unterzeichnenden)