VERTRAG ÜBER DIE VERARBEITUNG PERSONENBEZOGENER DATEN IM AUFTRAG

Zwischen

CRIF GmbH, Ndl. Karlsruhe
Kaiserstraße 217
76133 Karlsruhe

(nachfolgend AUFTRAGNEHMER genannt)

und

Musterfirma GmbH
slaksjdlaksjdlaskdj
slaksjdlaksjdlaskdj

(nachfolgend AUFTRAGGEBER genannt)

(gemeinsam auch VERTRAGSPARTNER genannt)

Präambel

Der AUFTRAGNEHMER ist ein Unternehmen, das u.a. auf die Erhebung, Zusammenführung, Verwaltung und Pflege von adress- und bonitätsbezogenen Daten über natürliche Personen und Unternehmen spezialisiert ist.

Der AUFTRAGGEBER wünscht im Rahmen des vorliegenden Vertrages eine Auftragsverarbeitung durch den AUFTRAGNEHMER und erteilt hierzu nachfolgenden, schriftlichen Auftrag, welcher die Rechte und Pflichten der Parteien im Zusammenhang mit der gewünschten Auftragsverarbeitung im Einzelnen regelt.

1. Gegenstand, Dauer, Art und Zweck des Auftrags

1.1. Gegenstand

Der Gegenstand, die Art und der Zweck des Auftrags, die Art der Daten und die Kategorien der betroffenen Personen sind in Anlage 1 beschrieben. Im Übrigen gelten die Bestimmungen des zwischen den VERTRAGSPARTNERN bestehenden / zeitgleich abzuschließenden Datenlieferungsvertrages inkl. Anlagen (nachstehend „Hauptvertrag“ genannt).

Der AUFTRAGNEHMER darf die Daten ausschließlich im Rahmen der Weisung des Verantwortlichen verarbeiten. Die Weisungen des AUFTRAGGEBERS können schriftlich oder elektronisch erteilt werden.

Anfragen, die nicht verarbeitbar sind oder offenkundig nicht zu einem Ergebnis führen werden, können vom AUFTRAGNEHMER verworfen oder angepasst werden. Die Anpassung kann auch derart geschehen, dass ein aufgrund seiner Unvollständigkeit irreführender oder mehrdeutiger Feldinhalt vor der Verarbeitung der Anfrage entfernt wird.

1.2. Dauer/Kündigung

Die Dauer des Auftrags richtet sich nach der Laufzeit des DIENSTLEISTUNGSVERTRAGES (Hauptvertrag).

Die fristlosen Kündigungsrechte der VERTRAGSPARTNER bleiben hiervon unberührt. Die VERTRAGSPARTNER sind u.a. berechtigt diesen Vertrag fristlos zu kündigen, wenn ein schwerwiegender Verstoß gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, bspw. wenn der AUFTRAGNEHMER eine Weisung des AUFTRAGGEBERS nicht ausführen kann oder will oder die Wahrnehmung von Kontrollrechten durch den AUFTRAGGEBER oder die zuständige Aufsichtsbehörde verweigert.

Jede Kündigung bedarf zur ihrer Wirksamkeit der Textform.

2. Ort der Datenverarbeitung

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Jede Verlagerung der Datenverarbeitung in ein Drittland bedarf der vorherigen Zustimmung des AUFTRAGGEBERS. Sofern die Zustimmung gegeben wird, sind sämtliche Anforderungen der DSGVO zu wahren, v.a. diejenigen der Art. 44 ff. DSGVO.

3. Technisch-organisatorische Maßnahmen

3.1. Der AUFTRAGNEHMER hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung in Anlage 2 dokumentiert und dem AUFTRAGGEBER zur Prüfung übergeben. Bei Akzeptanz durch den AUFTRAGGEBER werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des AUFTRAGGEBERS einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.2. Der AUFTRAGNEHMER hat die Sicherheit gemäß Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (Einzelheiten in Anlage 2).

3.3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem AUFTRAGNEHMER gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

4.1. Der AUFTRAGNEHMER darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des AUFTRAGGEBERS berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den AUFTRAGNEHMER wendet, wird der AUFTRAGNEHMER dieses Ersuchen unverzüglich an den AUFTRAGGEBER weiterleiten.

4.2. Der AUFTRAGNEHMER hat den AUFTRAGGEBER bei dessen Verpflichtung zur Wahrung der Betroffenenrechte, insbesondere der Art. 15, 16, 17, 18 DSGVO zu unterstützen. Direkte Auskünfte an Dritte oder die betroffene Person darf der AUFTRAGNEHMER nur erteilen, sofern der AUFTRAGGEBER zuvor ausdrücklich schriftlich oder elektronisch seine Zustimmung erteilt hat; etwas anderes gilt, falls der AUFTRAGNEHMER zur Auskunft gesetzlich oder behördlich verpflichtet ist.

4.3. Für Aufwände des AUFTRAGNEHMERS bei der Erfüllung der Pflichten nach dieser Ziffer, die über den üblichen Leistungsumfang des Auftrags hinausgehen, kann der AUFTRAGNEHMER eine Vergütung nach seinen üblichen Sätzen beanspruchen.

5. Qualitätssicherung und sonstige Pflichten des AUFTRAGNEHMERS

Der AUFTRAGNEHMER hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

5.1. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen Kontaktdaten werden dem AUFTRAGGEBER zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem AUFTRAGGEBER unverzüglich mitgeteilt.

5.2. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der AUFTRAGNEHMER setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der AUFTRAGNEHMER und jede dem AUFTRAGNEHMER unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des AUFTRAGGEBERS verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

5.3. Der AUFTRAGGEBER und der AUFTRAGNEHMER arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5.4. Die unverzügliche Information des AUFTRAGGEBERS über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim AUFTRAGNEHMER ermittelt.

5.5. Soweit der AUFTRAGGEBER seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim AUFTRAGNEHMER ausgesetzt ist, hat ihn der AUFTRAGNEHMER nach besten Kräften zu unterstützen. Für Aufwände des AUFTRAGNEHMERS bei der Erfüllung der Pflichten nach dieser Ziffer, die über den üblichen Leistungsumfang des Auftrags hinausgehen, kann der AUFTRAGNEHMER eine Vergütung nach seinen üblichen Sätzen beanspruchen.

5.6. Der AUFTRAGNEHMER kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

5.7. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem AUFTRAGGEBER im Rahmen seiner Kontrollbefugnisse.

6. Unterauftragsverhältnisse

6.1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der AUFTRAGNEHMER z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

6.2. Der AUFTRAGNEHMER ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des AUFTRAGGEBERS auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.3. Die Auslagerung auf Unterauftragnehmer oder der Wechsel eines bestehenden Unterauftragnehmers sind zulässig, soweit:

- der AUFTRAGNEHMER eine solche Auslagerung auf Unterauftragnehmer eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der AUFTRAGGEBER nicht innerhalb einer angemessenen Frist vor dem Zeitpunkt der Übergabe der Daten gegenüber dem AUFTRAGNEHMER wenigstens in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung mit dem Unterauftragnehmer nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

6.4. Der AUFTRAGGEBER erteilt mit Wirksamwerden dieses Vertrags die Zustimmung für die in Anlage 3 aufgeführten Unterauftragnehmer.

6.5. Die Weitergabe von personenbezogenen Daten des AUFTRAGGEBERS an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.6. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der AUFTRAGNEHMER die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Ziffer 6.1 Satz 2 eingesetzt werden sollen.

6.7. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform).

7. Vergütung

Die Vergütung ist im DIENSTLEISTUNGSVERTRAG geregelt.

8. Kontrollrechte des AUFTRAGGEBERS

8.1. Der AUFTRAGGEBER hat das Recht, im Benehmen mit dem AUFTRAGNEHMER Überprüfungen durchzuführen oder durch im Einzelfall zu benennende, nachweislich zur Verschwiegenheit verpflichtete Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den AUFTRAGNEHMER in dessen Geschäftsbetrieb zu überzeugen.

8.2. Der AUFTRAGNEHMER stellt sicher, dass sich der AUFTRAGGEBER von der Einhaltung der Pflichten des AUFTRAGNEHMERS nach Art. 28, 32 DSGVO überzeugen kann. Der AUFTRAGNEHMER verpflichtet sich, dem AUFTRAGGEBER auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen mit geeigneten Mitteln nachzuweisen.

9. Mitteilung bei Verstößen des AUFTRAGNEHMERS

Der AUFTRAGNEHMER unterstützt den AUFTRAGGEBER bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den AUFTRAGGEBER zu melden;
- die Verpflichtung, dem AUFTRAGGEBER im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
- die Unterstützung des AUFTRAGGEBERS für dessen Datenschutz-Folgenabschätzung;
- die Unterstützung des AUFTRAGGEBERS im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

10. Weisungsbefugnis und Verantwortlichkeit des AUFTRAGGEBERS

10.1. Die weisungsberechtigten Personen sind vom AUFTRAGGEBER festzulegen.

10.2. Mündliche Weisungen bestätigt der AUFTRAGGEBER unverzüglich (mind. Textform).

10.3. Der AUFTRAGNEHMER hat den AUFTRAGGEBER unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der AUFTRAGNEHMER ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den AUFTRAGGEBER bestätigt oder geändert wird.

10.4. Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt.

10.5. Der AUFTRAGGEBER als Verantwortlicher ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der der Datenweitergabe an den AUFTRAGNEHMER verantwortlich.

11.Haftung

Der AUFTRAGNEHMER haftet nach Art. 82 DSGVO. Die Haftung des AUFTRAGNEHMERS gegenüber dem AUFTRAGGEBER ist im Innenverhältnis auf 50% des Auftragsvolumens der letzten 12 Monate vor dem schädigenden Ereignis begrenzt. Dies gilt nicht bei vorsätzlich oder grob fahrlässig verursachten Vermögensschäden, bei Verletzung von Körper und Leben oder bei einer fahrlässigen Verletzung einer wesentlichen Vertragspflicht. Im letzteren Fall ist die Haftung begrenzt auf den typischerweise vorhersehbaren Schaden.

12. Löschung und Rückgabe von personenbezogenen Daten

12.1. Kopien oder Duplikate der Daten werden ohne Wissen des AUFTRAGGEBERS nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

12.2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den AUFTRAGGEBER – spätestens mit Beendigung dieses Vertrags – hat der AUFTRAGNEHMER sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem AUFTRAGGEBER auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Datensicherungen wie E-Mail-Backups werden im Rahmen des ordentlichen Geschäftsgangs gelöscht. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

12.3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den AUFTRAGNEHMER entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem AUFTRAGGEBER übergeben.

13. Schlussbestimmungen

13.1. Unbenommen von etwaigen gesetzlichen Vorgaben behält sich der AUFTRAGNEHMER das Recht vor, mit einer Ankündigungszeit von mindestens 3 Monaten und nicht öfter als 1-mal pro Kalenderjahr technische Anpassungen, insbesondere hinsichtlich der Schnittstelle, vorzunehmen.

13.2. Andere als in diesem Vertrag getroffene Vereinbarungen bestehen nicht. Mündliche Nebenabreden sind nicht getroffen. Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform.

13.3. Zur Ausübung eines Zurückbehaltungsrechtes an den Daten und Datenstrukturen des AUFTRAGGEBERS ist der AUFTRAGNEHMER nicht berechtigt.

13.4. Sollte eine Bestimmung dieses Vertrags unwirksam oder undurchführbar sein oder werden, so berührt dies nicht die Wirksamkeit der übrigen Bestimmungen und des Vertrags als solcher. Die VERTRAGSPARTNER sollen in einem solchen Fall die unwirksame oder undurchführbare Bestimmung durch eine wirksame Regelung zu ersetzen, die dem wirtschaftlichen Willen der VERTRAGSPARTNER unter Berücksichtigung der Interessen beider Parteien möglichst nahekommt. Das Gleiche gilt im Falle einer Regelungslücke.

13.5. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist München. Die VERTRAGSPARTNER vereinbaren die Anwendbarkeit deutschen Rechts unter Ausschluss des UN-Kaufrechts.

Folgende Anlagen sind integraler Bestandteil dieser Vereinbarung:

☒	**Anlage 1**	Gegenstand, Art und Zweck der Datenverarbeitung / Art der Daten / Kategorien der betroffenen Personen
☒	**Anlage 2**	Technische und organisatorische Maßnahmen des Auftragnehmers
☒	**Anlage 3**	Liste der Unterauftragnehmer

Anlage 1

Gegenstand, Art und Zweck der Datenverarbeitung / Art der Daten / Kategorien der betroffenen Personen

SYNESGY	
Gegenstand der Auftragsverarbeitung (AV)	1. Speichern von Daten der (potenziellen) Geschäftspartner des AUFTRAGGEBERS im Synesgy-Portal. 2. Abgleich mit bereits gespeicherten ESG-Daten. 3. Versand von E-Mails an (potenzielle) Geschäftspartner des AUFTRAGGEBERS (z.B. zwecks Einladung, Erinnerung, Rückfragen zur Plausibilisierung der Antworten).
Art der AV	Mit dem Synesgy-Portal stellt der AUFTRAGNEHMER seinem AUFTRAGGEBER eine Datenbank zur Verfügung, in die der AUFTRAGGEBER Daten seiner (potenziellen) Geschäftspartner hochlädt. Dort werden die Daten mit bereits im Portal vorhandenen und gültigen Synesgy-Zertifikaten abgeglichen und der jeweils neue ESG Performance Index nebst Informationen aus dem Fragebogen und Handlungsempfehlungen gespeichert. Sind bereits Synesgy-Zertifikate der (potenziellen) Geschäftspartner vorhanden und noch gültig (nicht älter als 12 Monate), kann der AUFTRAGGEBER die dem Zertifikat zugrundeliegenden Antworten, hochgeladenen Dokumente, CRIF ESG Indizes und Handlungsempfehlungen einsehen. Das Synesgy-Zertifkat (PDF) kann der AUFTRAGGEBER nicht abrufen, da dieses nur dem Geschäftspartner über das Synesgy Portal zur Verfügung gestellt wird. Geschäftspartner, zu denen entweder noch kein Synesgy-Zertifikat vorliegt oder deren Zertifikat zeitlich bereits abgelaufen ist (>12 Monate), werden vom AUFTRAGNEHMER mit einer automatisierten Standard-E-Mail von CRIF angeschrieben und gebeten, einen Fragebogen auszufüllen. Der AUFTRAGNEHMER versendet die E-Mails im Namen des AUFTRAGGEBERS über (i) ein vom AUFTRAGGEBER zur Verfügung gestelltes Konto oder (ii) eigene E-Mailkonten. Die Daten werden im Synesgy-Portal für die Dauer der Auftragsverarbeitung gespeichert. Löschung der Daten aus dem für den AUFTRAGGEBERS unterhaltenen Datenpool im Auftrag des AUFTRAGGEBERS nach dessen Vorgaben. Werden seitens des AUFTRAGGEBERS keine Löschroutinen vorgegeben, löscht der AUFTRAGNEHMER wie folgt: Kundenlisten, ESG Performance Index, Informationen aus dem Fragebogen und Handlungsempfehlungen werden 18 Monate nach Ausstellung des ESG Performance Index gelöscht.
Zweck der AV	Die Informationen aus dem Fragebogen inkl. evtl. hochgeladener Dokumente, die von CRIF berechneten ESG Performance Indizes sowie die unverbindlichen Handlungsempfehlungen können vom AUFTRAGGEBER verwendet werden, um sich einen Eindruck zu verschaffen, wie gut oder schlecht der (potenzielle) Geschäftspartner beim Thema Nachhaltigkeit aufgestellt ist, konkret bei Umwelt-, Sozial- und Governance-Themen („ESG-Themen").
Art der Daten	1. Kontaktdaten (insbesondere Firma, Anschrift, Telefon, E-Mail) und weitere Identifier (Ust.-ID, Ländercode und ggfs. Kunden- oder Referenz-Nr., Funktion) der (potenziellen) Geschäftspartner des AUFTRAGGEBERS aus dem eigenen Datenuniversum des AUFTRAGGEBERS werden vom AUFTRAGGEBER im Synesgy-Portal hochgeladen. 2. Daten aus dem Fragebogen. 3. Umweltdaten. 4. Personalmanagement. 5. Beziehungen zu Dritten. 6. Unternehmensführung.
Kreis der Betroffenen	(Potenzielle) Geschäftspartner des AUFTRAGGEBERS.

Anlage 2

Technische und organisatorische Maßnahmen (TOM)

Information Datenschutz

Stand November 2021

TOMs_20211104_v1.0.1

Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen entsprechend dieser Anlage zu. Insbesondere wird der Auftragnehmer seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Der Auftragnehmer wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers gegen Missbrauch und Verlust treffen, die den Forderungen der DSGVO entsprechen.

Dies beinhaltet insbesondere:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Ziel: Verwehrung des Zutritts zu Datenverarbeitungsanlagen für Unbefugte

Für den Zutritt zu den Bürogebäuden von CRIF ist ein Schlüssel erforderlich, der Zutritt zu den Büros selbst ist zusätzlich zur Schließung durch eine Chipkarte oder einen Passivtransponder gesichert. Vereinzelungsanlage, Alarmanlage, Wachdienst und Videoüberwachung sind weitere Komponenten zur Sicherung von Haupteingängen und Technikräumen.

Besucher werden an der Rezeption in Empfang genommen und dort von dem jeweiligen Fachbereich abgeholt. Die weitere Begehung ist betriebsfremden Personen nicht bzw. nur in Begleitung eines Mitarbeiters gestattet. Die einzelnen Bürobereiche sind nach Aufgabenbereichen strukturiert.

Zutritt zu Technikräumen

In den Bürogebäuden liegende Technikräume sind zusätzlich durch Chipkarte und/oder PIN-Schlösser gesichert.

Zutritt zum Rechenzentrum

Das Gebäude des Rechenzentrums ist von einem Sicherheitszaun umgeben, dessen Torschleuse sich nur mittels eines Chipkartenlesers/ einer Chipkarte öffnen lässt. Das Gebäude wird außerdem durch Kameras und einen Wachdienst geschützt.

Der Zutritt zum Gebäude ist durch eine Alarmanlage und ein elektronisches Chipkartenschloss gesichert. Zutritt zu beiden Systemen ermöglichen eine gültige Chipkarte und zwei sechsstellige PINs (Schließ- und Alarmanlage). Die Chipkarte befindet sich in einem Tresor, zu dem nur bestimmte Mitarbeiter der IT-Infrastruktur Zugang haben. Jede Entnahme der Chipkarte wird dokumentiert. Die Liste der zutrittsberechtigten Personen wird regelmäßig überprüft und zeitnah aktualisiert, externes Wartungspersonal hat nur in Begleitung von berechtigten Personen Zutritt.

Systemzugangskontrolle

Ziel: keine Nutzung der Datenverarbeitungsanlagen durch Unbefugte.

Im gesamten CRIF System ist keine Transaktion ohne gültige Authentifizierung und Autorisierung möglich. Der Zugang zu den Systemen wird durch mehrere Sicherheitsmechanismen abgesichert.

Der Zugang zu Systemen erfolgt durch Eingabe von Benutzername und Passwort, wobei das Passwort Restriktionen bzgl. Länge, Sonderzeichen etc. unterliegt.

Die Vergabe der Nutzerzugangsdaten erfolgt auf schriftlichen Antrag durch den HelpDesk. Nach erstmaligem Login muss das Passwort vom Nutzer geändert werden.

Das Passwort muss außerdem durch den Benutzer regelmäßig geändert werden, eine wiederholte Verwendung desselben Passwortes wird durch das System unterbunden. Fehlerhafte Anmeldeversuche führen zur Sperrung des Benutzers, der nur nach Prüfung und durch den HelpDesk bei gleichzeitiger Vergabe eines neuen Passwortes wieder freigeschaltet wird.

Das interne Netz (LAN) ist durch Virtual-Local-Area-Network-(VLAN-) Technologie in mehrere Segmente eingeteilt. Die Segmente sind u. a. Produktionssysteme, Testsysteme und Bürosysteme.

Die Netzübergänge sind durch Firewallsysteme geschützt und werden überwacht. Unbenutzte LAN-Ports sind technisch gesperrt und werden nur kontrolliert in Betrieb gesetzt.

Der Übergang vom internen Netz zu Fremdnetzen (Internet, Partner- und Kundennetze) ist nur an zentralen Stellen möglich, die durch ein mehrstufiges Firewallsystem gesichert sind und sowohl von CRIF als auch durch Dritte überwacht und regelmäßig geprüft werden (z. B. PEN-Test).

Zugriffskontrolle

Ziel: Zugriffsbeschränkung für Berechtigte, Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Löschen von Daten

Allen Nutzern sind entsprechend Ihren Tätigkeiten bestimmte erforderliche Funktionen zugeordnet, die über den Benutzernamen gesteuert werden. Die Einrichtung von Nutzern wird durch den Help-Desk durchgeführt. Die Nutzer erhalten vom HelpDesk Passwörter für den Zugang zu den Anwendungen, mit denen personenbezogene Daten verarbeitet werden. Im gesamten CRIF System ist keine Transaktion ohne gültige Authentifizierung und Autorisierung möglich.

Die Nutzer der Anwendungen haben nur in dem für die konkrete Rolle erforderlichen Umfang Zugriff auf personenbezogene Daten (Need-to-know-Prinzip). Ergänzend werden Daten und Dokumente, soweit geboten und technisch möglich, verschlüsselt gespeichert und übertragen.

Damit sind unerlaubte Tätigkeiten in CRIF-Systemen außerhalb eingeräumter Berechtigungen verhindert und eine bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung ist gegeben.

Trennungskontrolle

Ziel: Zweckgebundenheit der Datenverarbeitung sicherstellen

Der Datenzugriff ist nur anhand von Berechtigungskonzepten möglich. Datenzugriff ist nur für die jeweils erforderlichen Zwecke möglich. Die Datenbestände der betriebenen Anwendungen werden getrennt voneinander betrieben, sodass aus einer Anwendung kein Zugriff auf andere Anwendungen möglich ist.

Jeder Einmelder und jeder eingelesene Datensatz ist eindeutig über eine Referenznummer identifizierbar. Jeder Zugriff über die Produkte auf die Daten ist eindeutig identifizierbar und nachvollziehbar. Transaktionen werden separat geloggt.

Kundendatenbestände werden auf der Basis jeweils eigener Kunden-Accounts logisch voneinander getrennt. Dabei ist die Mandantenfähigkeit der eingesetzten IT-Systeme gegeben. Die zu unterschiedlichen Zwecken erhobenen Daten werden auch getrennt verarbeitet.

Bei Betrieb einer Multiauskunfteistrategie des Kunden auf der CRIF CSP Plattform:

a) CRIF kann eine Anfrage jederzeit bedienen, auch wenn eine Quelle abgeschaltet ist.
b) CRIF kann jede genutzte Datenquelle auch getrennt beauskunften, weil jede Quelle und/oder Anfrage eindeutig referenziert wird.
c) Die Herkunft der Daten ist jederzeit nachvollziehbar, d. h. wann von wem zu welchem Zweck Daten erhoben und gespeichert wurden.
d) Transaktionsdaten sind vom eigenen Datenbestand separiert und werden nicht verändert oder zu einem anderen Zweck verwendet.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Ziel: Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Löschen sowie Nachvollziehbarkeit erfolgter Übertragungen von Daten

Der Zugriff auf die Datenbanken erfolgt durch die Nutzer zum einen via FTP mit Tunnel/SFTP, zum anderen via Webservices, die über HTTPS abgesichert sind. Dabei wird nicht nur die Authentifizierung, sondern auch die Übertragung der Daten gesichert. In Absprache mit den Kunden und je nach Schutzbedarf der Daten wird eine Vielzahl von aktuellen Verschlüsselungsverfahren angeboten.

Jede Auskunftsanforderung wird im System registriert, sodass jederzeit geprüft werden kann, welche Daten von wem gespeichert, verarbeitet oder übermittelt worden sind. Ebenso kann der Empfänger einer Datenübermittlung ermittelt werden. Die Weitergabe von personenbezogenen Daten erfolgt bei direkter Anbindung prinzipiell verschlüsselt. Im Standard erfolgt die Kommunikation mit externen Clients immer verschlüsselt über HTTPS (HyperText Transfer Protocol Secure, sicheres Hypertext-Übertragungsprotokoll) und/oder VPN (Virtual Private Network). Die Übermittlung der Daten per E-Mail (SMTP) erfolgt PGP-verschlüsselt.

Für den Transfer von Dateien ist SFTP (Secure File Transfer Protocol) oder eine Dateiverschlüsselung notwendig.

Ausrangierte Computerhardware, Datenträger und nicht mehr benötigte Unterlagen und Listenausdrucke werden durch einen Entsorgungsfachbetrieb zerstört. Die Geräte werden in einem abschließbaren, dedizierten Datenbehälter abtransportiert und fachgerecht entsorgt. Die Vernichtung wird protokolliert. Das Protokoll wird CRIF zur Verfügung gestellt.

Eingabekontrolle

Ziel: Nachvollziehbarkeit von Eingaben, Änderungen oder Löschung von Daten

Die Eingabe von Daten erfolgt in automatisierten Prozessen. Diese werden vorab in Testsystemen überprüft und unterliegen einem standardisierten Freigabeprozess. In diesen Prozessen wird jede automatisierte Eingabe protokolliert und ist jederzeit durch die eindeutige Prozess- und Transaktions-ID nachvollziehbar.

Durch die Protokollierung der Eingabedaten ist es jederzeit möglich, den ursprünglichen Zustand wiederherzustellen.

Auf Basis eines Rollen- und Rechtekonzepts werden den Mitarbeitern von CRIF in Abhängigkeit ihrer Funktion und der zu bearbeitenden Datenbestände differenzierte Berechtigungen zugewiesen. Die Verarbeitung von Daten durch die Mitarbeiter wird protokolliert.

Manuelle Einzeleingaben erfolgen über eine Programmebene, die ebenfalls benutzerbezogen die einzelnen Schritte und Aktivitäten des Anwenders protokolliert. Das Eingabeprogramm unterliegt ebenfalls dem standardisierten Freigabeprozess von CRIF.

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist gewährleistet. Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, sind im Einsatz.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

Ziel: Schutz vor Datenverlust und Datenwiederherstellung in angemessener Zeit

Die Verfügbarkeit der produktiven Daten wird durch die eingesetzten Betriebstechniken (u. a. Storage Area Network [SAN], Virtualisierung und Spiegelung) und die Datensicherung gewährleistet.

Netzwerkkomponenten (z. B. NIC, Switches) und Carrier-Verbindungen (WAN) sind redundant ausgelegt und mit Servicevereinbarungen (SLA/UC) gestützt. Komponenten und Verbindungen werden durch CRIF und durch Dritte (z. B. Provider) überwacht.

In der Produktion sind alle Server doppelt oder mehrfach vorhanden. Im Falle eines Ausfalls wird (automatisiert) der jeweils andere Server eingesetzt. Durch Virtualisierung ist eine schnelle Bereitstellung gewährleistet. Das Transaktionslog der produktiven Datenbanken erlaubt auch im Falle eines Ausfalls mit Datenverlust eine Wiederherstellung des Produktionssystems.

Die Datensicherung erfolgt zusätzlich mehrfach über Magnetbandlaufwerke. Die Magnetbänder werden sowohl onsite vorgehalten als auch ausgelagert. Rücksicherungen auf Band werden regelmäßig getestet (Stichproben, automatisiert).

CRIF betreibt zusätzlich ein Notfallrechenzentrum (Geo-Redundanz), in dem alle produktiven Daten vorgehalten werden.

Maßnahmen zum Schutz vor Schäden durch Feuer und Wasser sind in den dezentralen Technikräumen installiert. Alle für die Produktion relevanten Datenbestände werden zentral im Rechenzentrum vorgehalten.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

Auftragskontrolle

Ziel: ausschließliche auftragsbezogene Verarbeitung der Daten

Auftragserteilung und Auftragsbearbeitung erfolgen bei CRIF mittels Standardprozessen. Die für die Geschäftsfelder „Risk“, „Solutions“ und „Recovery“ einschlägige Auftragsverarbeitung wird durch CRIF als Auftragsverarbeiter schriftlich dokumentiert.

Datenerhebung

Im Rahmen der automatisierten Datenerhebung werden die Aufträge (Einmeldungen) mit einem sogenannten Bearbeitungsstatus per Datei eingeliefert. Der Einmelder ist eindeutig per Referenz identifizierbar. Jede Datei und jede Einmeldung erhält eine eindeutige ID.

Entsprechend des Bearbeitungsstatus des Einmelders handelt es sich um

a) eine Neuanlage,
b) einen Löschauftrag oder
c) eine Aktualisierung.

Die einzelnen Aufträge werden historisiert abgelegt. Daten werden immer in den für den Zweck vorgesehenen Tabellen gespeichert.

Beauskunftung

Anfragen des Kunden werden über Produkte durchgeführt. Die Produkte werden entsprechend dem Vertrag mit dem Kunden zweckgebunden konfiguriert. Jede Anfrage durch den Kunden wird nur im Kundenkontext durchgeführt.

Die dabei übermittelten Daten von externen Auskunfteien werden nicht für etwaige andere Beauskunftungen erneut verwendet. Es ist über eine eindeutige Referenzierung in den Logs immer nachvollziehbar, welche Daten für welche Anfrageaufträge beauskunftet wurden.

Die weisungsgemäße Auftragsverarbeitung ist gewährleistet und Maßnahmen (technisch/ organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer sind gegeben.

5. Sonstiges

Überwachung durch die Aufsichtsbehörde

CRIF unterliegt aufgrund seiner Tätigkeit als Auskunftei der regelmäßigen Überprüfung der zuständigen Aufsichtsbehörde. Für CRIF ist das Bayerische Landesamt für Datenschutzaufsicht zuständig.

Verpflichtung der Mitarbeiter auf das Datengeheimnis, Sicherheitsrichtlinie

Der Datenschutzbeauftragte schult und überwacht die Mitarbeiter auf die Einhaltung der datenschutzrechtlichen Vorschriften. Sämtliche an der Datenverarbeitung beteiligten Mitarbeiter sind über die datenschutzrechtlichen Anforderungen unterrichtet. Eine Verpflichtungserklärung über das Datengeheimnis liegt für jeden Mitarbeiter vor.

Des Weiteren werden die Mitarbeiter von CRIF durch eine interne Sicherheitsrichtlinie, die verbindlich zu unterzeichnen und einzuhalten ist, an interne Sicherheitsstandards gebunden.

Anlage 3

Der AUFTRAGGEBER erteilt mit Wirksamwerden dieses Vertrags die Zustimmung für folgende Unterauftragnehmer (Ziffer 6):

UNTERAUFTRAGNEHMER	Leistung
CRIF S.p.A. Via della Beverara 21 40131 Bologna Italien	Bereitstellung, Betrieb und Monitoring von IT-Infrastruktur und Software inkl. Beratung, Fehleranalyse und -behebung, Trainings und IT-Projektmanagement, Customizing bestehender Software und Anpassung von Software as a Service, Betrieb Desaster Recovery Unterstützung bei Datenmanagement und Betrieb der Datenbank
einschließlich der Zweigstelle **CRIF S.p.A. Podružnica Koper** Pristaniška ulica 4 6000 Koper – Capodistria Slowenien	Unterstützung bei Recherchetätigkeiten und in der Buchhaltung
CRIF Sp. z o.o. Ul. Lublańska 38 31476 Kraków Polen	Anwendungsentwicklung, Betrieb und Monitoring von IT-Infrastruktur und Software inkl. Beratung, Fehleranalyse und -behebung, Trainings und IT-Projektmanagement, Customizing bestehender Software und Anpassung von Software as a Service, Betrieb Desaster Recovery und Backup