dacuro
die datenschutz-experten

Auftragsverarbeitungsvertrag
nach Art. 28 Abs. 3 DSGVO

Auftragsverarbeitungsvertrag

nach Art. 28 Abs. 3 DSGVO

zwischen

dem Nutzer des FlyingLess Monitoringtools

als Verantwortlicher

(hier bezeichnet als „Auftraggeber")

und

ifeu – Institut für Energie- und Umweltforschung Heidelberg gGmbH

als Auftragsverarbeiter

(hier bezeichnet als „Auftragnehmer")

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 2 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art.28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

In diesem Vertrag verwendete Begriffe, die in Art. 4, 9 und 10 DSGVO definiert werden, sind im Sinne dieser gesetzlichen Definition zu verstehen.

§ 2 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber nachfolgende Leistungen im Bereich der Analyse und Auswertung von Flugreise- und Emissionsdaten. Dabei erhält der Auftragnehmer Zugriff auf pseudonymisierte personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist.

(2) Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus der **Anlage 1** zu diesem Vertrag. Dem Auftraggeber obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO.

(3) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung.

(4) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Auftrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet werden.

(5) Der vorliegende Vertrag ist für einen unbefristeten Zeitraum gültig, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechteergeben.

(6) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der europäischen Union oder einem anderen Vertragsstaat des Abkommens über den europäischen Vertragsraum (Beschluss 94/1/EG) statt. Jede Verlagerung von Teilleistungen oder der gesamten Dienstleistung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers in Schriftform oder dokumentiertem elektronischen Format und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 3 Art der verarbeiteten Daten, Kreis der betroffenen Personen

Im Rahmen der Durchführung des Auftrages erhält der Auftragnehmer Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten der ebenfalls in **Anlage 1** näher spezifizierten betroffenen Personen. Diese Daten umfassen keine besonderen Kategorien personenbezogener Daten.

§ 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in dokumentiertem elektronischem Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in **Anlage 2** aufgeführten Maßnahmen getroffen hat. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu nutzen oder auf sonstige Weise zu verarbeiten. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden „Beschäftigte" genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 6 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder dokumentiertem elektronischen Format informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält soweit möglich folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und

c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den Auftraggeber und ersucht diesen um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Der Auftragnehmer unterstützt den Auftraggeber erforderlichenfalls bei der Erfüllung der Pflichten des Auftraggebers nach Art. 33 und 34 DSGVO in angemessener Weise (Art. 28 Abs. 3 S. 2 lit. f DSGVO). Meldungen für den Auftraggeber nach Art. 33 oder 34 DSGVO darf der Auftragnehmer nur nach vorheriger Weisung seitens des Auftraggebers gem. § 4 dieses Vertrags durchführen.

(5) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem" im Sinne der DSGVO liegen.

(6) Über wesentliche Änderungen der Sicherheitsmaßnahmen hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(7) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DSGVO hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach §5 Abs.3 auf Verlangen nach.

§ 8 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 3** genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis") befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Subunternehmers vorab schriftlich oder in dokumentiertem elektronischem Format zugestimmt hat. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 9 Anfragen und Rechte betroffener Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art.12 - 22 sowie 32 und 36 DSGVO.

(2) Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 10 Haftung

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn / soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Absatz 5 DSGVO.

§ 11 Außerordentliches Kündigungsrecht

Der Auftraggeber kann diesen Vertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO oder sonstige anwendbare Datenschutzvorschriftenvorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer sich den Kontrollrechten des Auftraggebers auf vertragswidrige Weise widersetzt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 12 Beendigung des Vertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Abschluss der vertraglich vereinbarten Arbeiten oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen.

(2) Dem Auftragnehmer wird daneben die Befugnis eingeräumt, die erhaltenen Datensätze zu anonymisieren, um diese anonymisierten Daten anschließend in stark aggregierter Form weiterzuverwenden, und sie bspw. interessierten akademischen Institutionen (z. B. über die Website von FlyingLess oder eine Publikation) zur Verfügung zu stellen.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende dieses Vertrags hinaus die ihm im Zusammenhang mit der Erfüllung des Auftrages bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über den Abschluss der vertraglich vereinbarten Arbeiten hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 13 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Heidelberg.

Anlagen:

Anlage 1 – Beschreibung der betroffenen Personen/ Betroffenengruppen sowie der verarbeiteten Daten

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3 – Genehmigte Subunternehmer

Für den Auftraggeber	Für den Auftragnehmer
[Vorname, Name, Funktion]	ifeu INSTITUT FÜR ENERGIE- UND UMWELTFORSCHUNG HEIDELBERG gGMBH Wilckensstr. 3 · 69120 Heidelberg Tel. 06221-47670 · Fax 06221-476719
(Ort, Datum, Unterschrift)	(Heidelberg, 23.01.2023)
	Lothar Eisenmann (Geschäftsführer)
	Dr. Martin Pehnt (Geschäftsführer)

Anlage 1:

(1) Betroffene Personen

Die übermittelten personenbezogenen Daten beziehen sich auf folgende Kategorien von betroffenen Personen:

An Hochschulen und Forschungseinrichtungen beschäftigte Personen, z. B.:

- Professor:innen
- Post-Docs
- Senios Scientists
- Doktorand:innen
- Verwaltungsmitarbeiter:innen
- Masterstudent:innen
- Bachlorstudent:innen
- Austauschstudent:innen
- Gäste

(2) Kategorie der verarbeiteten Daten

Die verarbeiteten personenbezogenen Daten gehören zu folgenden Datenkategorien:

Informationen zu den im Rahmen der akademischen Tätigkeit durchgeführten Reisen wie

- Reisezweck
- Anstellungsgrad
- Universitätszugehörigkeit
- Zugehörigkeit zu bestimmten Organisationseinheiten
- Flugstrecke (Start- und Zielflughafen)
- Flugklasse
- Flugnummer
- Fluggesellschaft
- verursachte Kosten

(3) Umfang, Art und Zweck der Verarbeitung

Im Rahmen der Nutzung des FlyingLess-Tools stellt der Auftraggeber dem Auftragnehmer bestimmte Informationen zum Reiseverhalten seiner Hochschulangehörigen zur Verfügung. Der Auftraggeber übermittelt die Informationen unter Nennung eines Personencodes (pseudonymisiert), wobei der Zuordnungsschlüssel (Code = Hochschulangehöriger) beim Auftraggeber verbleibt.

Die Daten werden vom Auftragnehmer zum Zwecke der Ermittlung der Flugemissionen ausgewertet und die Ergebnisse an den Auftraggeber zurückgesandt.

Anlage 2: Technisch-organisatorische Maßnahmen

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Daten-verarbeitungsanlagen, mit denen personen-bezogene Daten verarbeitet werden, zu verwehren. (z. B. Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte, Schlüssel, Schlüssel-vergabe, Werkschutz, Pförtner, Überwachungs-einrichtung, Alarmanlage, Türsicherung)	**Tech. Maßnahmen** • Automatisches Schließsystem • Zugang mit individuellen Keyfobs • Sicherheitsschlösser **Org. Maßnahmen** • Schlüsselregelung • Empfang • Reinigungsarbeiten erfolgen nur durch direkt beim ifeu angestellte Personen. Jede Reinigungskraft hat, wie alle anderen Mitarbeiter, eine Geheimhaltungsvereinbarung unterzeichnet und ist auf das BDSG (§53) verpflichtet. Alle ifeu-Mitarbeiter werden in regelmäßigen Abständen über für uns relevante Anforderungen des BDSG (§53) informiert.
2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbei-tungssysteme von Unbefugten genutzt werden können. *(z.B. Technische [Kennwort-/Passwortschutz] und organisatorische [Benutzerstammsatz] Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungs-verfahren [Beispiele: Kennwortverfahren, auto-matisches Sperren, Einrichtung eines Benutzer-stammsatzes pro User, Verschlüsselung von Datenträgern])*	**Tech. Maßnahmen** • Absicherung Zugang zu den Kommunikationsstrukturen des Unternehmens aus dem Internet durch starke Authentisierungsmechanismen • Konzept zur Absicherung der Netze (DMZ / Firewall etc.) • Anti-Viren-Software für Server und Clients • Nutzung von Verschlüsselungssystemen für Clients und Kommunikation • Sicheres Anmeldeverfahren mit sicheren Passwörtern für alle Clients. Gesondertes Verfahren für Administrationsdienste der Server **Org. Maßnahmen** • Regelungen zur Zugangsbeschränkung auf nur notwendige Systeme • Regelungen zu Gruppentrennung und Nutzung von gemeinsamen Netzen • Regelmäßige Unterweisung der MitarbeiterInnen zu den Themen Datenschutz und IT-Sicherheit

3.	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. *(z. B. Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.* *[Beispiele: differenzierte Berechtigungen wie Profile, Rollen etc., Auswertungen, Kenntnisnahme, Veränderung, Löschung])*	**Tech. Maßnahmen** • Festplatten und Datenträger werden vor der Entsorgung formatiert. • Dokumente: Entsorgung von vertraulichen Dokumenten (Schreddern). • Externer Daten- und Aktenvernichter (DIN 32757) • Nutzung von Verschlüsselungssystemen für Clients und Kommunikation **Org. Maßnahmen** • Vergabe, Entzug und Kontrolle von Berechtigungen im Netzwerk • Genehmigung, Freigabe und regelmäßige Überprüfung durch Administratoren • Mobile Systeme (Home-Office / mobile), sowie deren Datensicherung unterliegen Verfahrensanweisung. Dies beinhaltet insbesondere die Passwortsicherung des Systems und die separate Verschlüsselung von lokalen Daten.
Nr.	**Maßnahme**	**Umsetzung der Maßnahme**
4.	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. *(z. B. Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger [manuell oder elektronisch] sowie bei der nachträglichen Überprüfung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren, elektronische Signatur)*	**Tech. Maßnahmen** • Verschlüsselung des Zugangs zum E-Mail-System • Bereitstellung über verschlüsselte Verbindungen wie sftp, https im Webshare-Bereich und bei Umfragesoftware **Org. Maßnahmen:** • Schreibschutz durch Konvertierung in PDF-Dokumente, Transportsicherung mobiler Datenträger durch Passwortschutz und ggf. Verschlüsselung. Nutzung kryptographischer Verfahren bei WLAN, E-Mail-Kommunikation (Datentransport zwischen Rechner und Mailserver), Blackberry etc. • Datentransport nur in verschlüsselter Form. Dabei separate Übermittlung der Passworte über einen anderen Kommunikationsweg.
5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. *(z. B. Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung gewährleisten, etwa durch Protokollierungs- und Auswertungssysteme)*	**Org. Maßnahmen:** • Keine Arbeiten am Originaldatensatz. Veränderte Datensätze werden mit Änderungsdatum und Nutzerkennung kenntlich gemacht.

6.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der AG verarbeitet werden können. *(Abgrenzen der Kompetenz zwischen der AG und der/des AN [Beispiel: eindeutige Vertragsgestaltung, Kriterien zur Auswahl der/des AN, Kontrolle der Vertragsausführung])*	Org. Maßnahmen: • Mit Auftragsverarbeitern schließt das ifeu-Institut Auftragsverarbeitungsverträge, die den Anforderungen von Art. 28 DSGVO genügen. • Der Einsatz von Unterauftragnehmern wird unter der Voraussetzung gestattet, dass mit diesen, den Anforderungen von Art. 28 DSGVO genügende, Auftragsverarbeitungsverträge geschlossen werden.
7.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. *(z. B. Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen, Maßnahmen zur Datensicherung [Beispiel: Backup- Verfahren, Spiegeln von Festplatten, unter- brechungsfreie Stromversorgung, Firewall, Notfallplan]*	**Tech. Maßnahmen** • Serverraumüberwachung Temperatur • Übersicht über alle Betriebsmittel und deren Verbindungen zueinander • Überwachung von Wartung / Kapazitäten / Zuständigkeiten etc. je Betriebsmittel • Notstromversorgung mittels USV für alle Server **Org. Maßnahmen:** • Backup & Recovery-Konzept (ausformuliert) • Regelmäßiges Backup aller Server und Datenbanken, auch Offsite-Backup.
8.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	**Tech. Maßnahmen** • Es werden Microsoft Office Produkte eingesetzt und das Trennungsgebot durch die Dokumentenstruktur gewährleistet. **Org. Maßnahmen:** • Das Trennungsgebot wird durch die Dokumentenstruktur gewährleistet

Anlage 3: genehmigte Subunternehmer

Folgende Subunternehmer gelten mit Abschluss dieses Vertrages als genehmigt:

Firma	Ort der Datenverarbeitung	Auftrag/Art der Datenverarbeitung
Microsoft Ireland Operations Limited	EU	E-Mail Provider /E-Mail-Transport-Server-Software

Anlage 4: Weisungsgeber/ -empfänger

Für den Auftraggeber: [Vorname Name, Funktion, E-Mail, Telefon]

Für den Auftragnehmer:

Dominik Jessing
Datenschutzbeauftrager ifeu-Institut
E-Mail: datenschutz@ifeu.de
Telefon: +49 (0)6221 4767 0