Auftragsverarbeitungsvertrag

zwischen

XU Group GmbH,

Mehringdamm 33, 10961 Berlin,
eingetragen im Handelsregister des Amtsgerichts Charlottenburg unter HRB 172976 B,
vertreten durch die Geschäftsführer:in Nicole Gaiziunas-Jahns und Dr. Christopher Jahns,

- nachstehend „Auftragsverarbeiter, Auftragnehmer, Anbieter oder XU" genannt -

und

Auftraggeber

- nachstehend „Verantwortlicher, Kunde" genannt -

- Auftragsverarbeiter und Auftraggeber nachstehend auch „Parteien“ genannt -

Standardvertragsklauseln

ABSCHNITT I

Klausel 1

Zweck und Geltungsbereich

a) Der Zweck dieser Standardvertragsklauseln („Klauseln“) besteht darin, die Einhaltung von Artikel 28 Absatz 3 und (4) der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung des Artikels 95/46/EG (Datenschutz-Grundverordnung).
b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 sicherzustellen.
c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind integraler Bestandteil der Klauseln.
e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.
f) Diese Klauseln gewährleisten für sich allein nicht, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt sind.

Klausel 2

Unveränderlichkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, außer um die in den Anhängen angegebenen Informationen zu ergänzen oder zu aktualisieren.
b) Dies hindert die Parteien nicht daran, die in diesen Klauseln enthaltenen Standardvertragsklauseln in einen umfassenderen Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese nicht direkt oder indirekt im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen einschränken.

Klausel 3

Auslegung

a) Wenn in diesen Klauseln Begriffe verwendet werden, die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definiert sind, haben diese Begriffe dieselbe Bedeutung wie in der jeweiligen Verordnung.
b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.
c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen einschränkt.

Klausel 4

Vorrang

a) Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen bestehender oder später abgeschlossener Vereinbarungen zwischen den Parteien haben diese Klauseln Vorrang.

Klausel 5 – Optional

Kopplungsklausel

a) Eine Einrichtung, die nicht Vertragspartei dieser Klauseln ist, kann mit Zustimmung aller Vertragsparteien jederzeit als Verantwortlicher oder Auftragsverarbeiter diesen Klauseln beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.
b) Nach Ausfüllen und Unterzeichnung der in Buchstabe a genannten Anhänge wird die beitretende Stelle als Vertragspartei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder Auftragsverarbeiters gemäß Anhang I.
c) Rechte und Pflichten aus diesen Klauseln gelten für die beitretende Stelle nicht für den Zeitraum vor ihrem Beitritt als Vertragspartei.

ABSCHNITT II

VERPFLICHTUNGEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

a) Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1. Anweisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Anweisungen des Verantwortlichen, es sei denn, er ist aufgrund von Unionsrecht oder dem Recht eines Mitgliedstaats, dem er unterliegt, dazu verpflichtet. In diesem Fall teilt der Auftragsverarbeiter dem Verantwortlichen vor der Verarbeitung diese rechtlichen Anforderungen mit, es sei denn, dies ist aus Gründen des öffentlichen Interesses nach dem betreffenden Recht nicht zulässig. Der Verantwortliche kann während der gesamten Dauer

der Verarbeitung personenbezogener Daten weitere Anweisungen erteilen. Diese Anweisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Ansicht ist, dass die Anweisungen des Verantwortlichen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzvorschriften der Union oder eines Mitgliedstaats verstoßen.

7.2 Zweckbindung

a) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für die in Anhang II genannten spezifischen Zwecke, es sei denn, er erhält weitere Anweisungen vom Verantwortlichen.

7.3. Dauer der Verarbeitung personenbezogener Daten

a) Die Daten werden vom Auftragsverarbeiter nur für den in Anhang II angegebenen Zeitraum verarbeitet.

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter trifft mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Sicherheitsverletzung, die versehentlich oder unrechtmäßig zur Zerstörung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung oder zum unbefugten Zugriff auf die Daten führt (im Folgenden als „Verletzung des Schutzes personenbezogener Daten“ bezeichnet). Bei der Bewertung des angemessenen Schutzniveaus berücksichtigen die Parteien den Stand der Technik, die Implementierungskosten, die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die Risiken für die betroffenen Personen.

b) Der Auftragsverarbeiter gewährt seinen Mitarbeitern Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, nur in dem Umfang, der für die Ausführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter stellt sicher, dass die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Vertraulichkeitspflicht unterliegen.

7.5. Sensible Daten

a) Betrifft die Verarbeitung personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder Daten, die genetische Daten oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person enthalten, Daten über Gesundheit, Sexualleben oder sexuelle Orientierung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten (im Folgenden „sensible Daten“),

wendet der Auftragsverarbeiter besondere Einschränkungen und/oder zusätzliche Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
b) Der Auftragsverarbeiter reagiert unverzüglich und angemessen auf Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln.
c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in diesen Klauseln festgelegten und sich unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 ergebenden Verpflichtungen nachzuweisen. Auf Verlangen des Verantwortlichen ermöglicht der Auftragsverarbeiter auch die Überprüfung der von diesen Klauseln erfassten Verarbeitungsvorgänge in angemessenen Abständen oder bei Anzeichen einer Nichteinhaltung und trägt dazu bei. Bei der Entscheidung über eine Überprüfung oder ein Audit kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.
d) Der Verantwortliche kann das Audit selbst durchführen oder einen unabhängigen Auditor beauftragen. Die Audits können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und sind gegebenenfalls nach angemessener Vorankündigung durchzuführen.
e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) auf Anfrage die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse der Audits, zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter ist vom Verantwortlichen allgemein ermächtigt, in einer vereinbarten Liste aufgeführte Unterauftragsverarbeiter zu beauftragen. Der Auftragsverarbeiter wird den Verantwortlichen mindestens zwei Wochen im Voraus schriftlich über beabsichtigte Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern informieren, damit der Verantwortliche vor Beauftragung des/der betreffenden Unterauftragsverarbeiters/Unterauftragsverarbeiter ausreichend Zeit hat, solchen Änderungen zu widersprechen. Der Auftragsverarbeiter wird dem Verantwortlichen die erforderlichen Informationen zur Verfügung stellen, damit dieser sein Widerspruchsrecht ausüben kann.
b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungsvorgänge (im Auftrag des Verantwortlichen), muss dieser Auftrag durch einen Vertrag erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen die gleichen Datenschutzverpflichtungen auferlegt, wie sie für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Verpflichtungen erfüllt, denen der Auftragsverarbeiter gemäß

diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie dieser Unterauftragsvereinbarung und aller späteren Änderungen zur Verfügung. Soweit dies zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, erforderlich ist, kann der Auftragsverarbeiter den Text der Vereinbarung vor der Offenlegung einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang für die Einhaltung der Verpflichtungen des Unterauftragsverarbeiters aus dem mit dem Auftragsverarbeiter geschlossenen Vertrag. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seinen vertraglichen Verpflichtungen nicht nachkommt.

e) Der Auftragsverarbeiter schließt mit dem Unterauftragsverarbeiter eine Drittbegünstigungsklausel ab, wonach der Verantwortliche im Falle des tatsächlichen oder rechtlichen Erlöschens des Auftragsverarbeiters oder seiner Zahlungsunfähigkeit das Recht hat, den Unterauftragsvertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Anweisungen des Verantwortlichen oder zur Einhaltung einer besonderen Bestimmung des Unionsrechts oder des Rechts eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und entspricht Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter gemäß Ziffer 7.7 einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungsvorgänge (im Auftrag des Verantwortlichen) beauftragt und diese Verarbeitungsvorgänge eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, stellen der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 durch die Verwendung von Standardvertragsklauseln sicher, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 angenommen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über alle Anfragen der betroffenen Person. Er antwortet nicht selbst auf die Anfrage, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung seiner Verpflichtung, auf Anfragen von betroffenen Personen zur Ausübung ihrer Rechte zu reagieren. Bei der Erfüllung seiner Verpflichtungen gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Zusätzlich zu seiner Verpflichtung gemäß Ziffer 8 Buchstabe b unterstützt der Auftragsverarbeiter den Verantwortlichen unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen bei der Erfüllung der folgenden Verpflichtungen:

   1. die Verpflichtung zur Durchführung einer Folgenabschätzung für den Datenschutz bei den geplanten Verarbeitungsvorgängen (im Folgenden „Datenschutz-Folgenabschätzung"), wenn eine Form der Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt;
   2. die Verpflichtung, vor der Verarbeitung die zuständige(n) Aufsichtsbehörde(n) zu konsultieren, wenn eine Datenschutz-Folgenabschätzung ergibt, dass die Verarbeitung ein hohes Risiko mit sich bringen würde, sofern der Verantwortliche keine Maßnahmen zur Risikominderung ergreift;
   3. die Verpflichtung, die Richtigkeit der personenbezogenen Daten zu gewährleisten, indem der Verantwortliche unverzüglich informiert wird, wenn festgestellt wird, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
   4. Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen fest, mit denen der Auftragsverarbeiter den Verantwortlichen bei der Anwendung dieser Klausel unterstützt, sowie den Umfang und das Ausmaß der erforderlichen Unterstützung.

Klausel 9

Mitteilung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten wird der Auftragsverarbeiter mit dem Verantwortlichen entsprechend zusammenarbeiten und ihn unterstützen, damit dieser seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder, falls anwendbar, gemäß den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen nachkommen kann.

9.1. Verletzung des Datenschutzes bei der Verarbeitung durch den Verantwortlichen

Im Falle einer Verletzung des Schutzes personenbezogener Daten, die sich auf die vom Verantwortlichen verarbeiteten Daten bezieht, unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) unverzügliche Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem der Verantwortliche von der Verletzung Kenntnis erlangt hat, sofern dies relevant ist (es sei denn, die Verletzung des Schutzes personenbezogener Daten dürfte keine Gefahr für die Persönlichkeitsrechte und Freiheiten natürlicher Personen begründen);
b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in dem Bericht des Verantwortlichen anzugeben sind und mindestens Folgendes umfassen:
    1) die Art der personenbezogenen Daten, soweit möglich unter Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen sowie der Kategorien und der ungefähren Anzahl der betroffenen Datensätze;
    2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
    3) die vom Verantwortlichen getroffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Milderung ihrer möglichen nachteiligen Auswirkungen.

Soweit nicht alle diese Informationen gleichzeitig bereitgestellt werden können, enthält die ursprüngliche Meldung die zu diesem Zeitpunkt verfügbaren Informationen und weitere Informationen werden unverzüglich nachträglich bereitgestellt, sobald sie verfügbar sind;

a) in Übereinstimmung mit der in Artikel 34 der Verordnung (EU) 2016/679 festgelegten Verpflichtung, die betroffene Person unverzüglich über die Verletzung des Schutzes personenbezogener Daten zu informieren, wenn diese Verletzung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellt.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten, die sich auf die vom Auftragsverarbeiter verarbeiteten Daten bezieht, benachrichtigt der Auftragsverarbeiter den Verantwortlichen unverzüglich nach Bekanntwerden der Verletzung. Diese Mitteilung muss mindestens folgende Angaben enthalten:

a) eine Beschreibung der Art der Verletzung (unter Angabe, soweit möglich, der Kategorien und der ungefähren Anzahl der betroffenen betroffenen Personen und der ungefähren Anzahl der betroffenen Datensätze);

b) die Kontaktdaten einer Kontaktstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten erhältlich sind;
c) die voraussichtlichen Folgen und die bereits getroffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Milderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen gleichzeitig bereitgestellt werden können, enthält die ursprüngliche Meldung die zu diesem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden unverzüglich nachträglich bereitgestellt, sobald sie verfügbar sind.

Die Parteien legen in Anhang III alle weiteren Informationen fest, die der Auftragsverarbeiter bereitstellen muss, um den Verantwortlichen bei der Erfüllung seiner Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III

SCHLUSSBESTIMMUNGEN

Klausel 10

Verstoß gegen die Klauseln und Beendigung der Vereinbarung

a) Unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 kann der Verantwortliche für den Fall, dass der Auftragsverarbeiter seinen Verpflichtungen aus diesen Klauseln nicht nachkommt, den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diesen Klauseln nachkommt oder der Vertrag gekündigt wird. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er aus irgendeinem Grund nicht in der Lage ist, diese Klauseln einzuhalten.
b) Der Verantwortliche hat das Recht, den Vertrag insoweit zu kündigen, als er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
    1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall jedoch innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
    2) der Auftragsverarbeiter diese Klauseln erheblich oder wiederholt verletzt oder seinen Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht nachkommt;

3) der Auftragsverarbeiter einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde(n) in Bezug auf seine Verpflichtungen aus diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag insoweit zu kündigen, als er sich auf die Verarbeitung personenbezogener Daten gemäß diesen Klauseln bezieht, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber informiert wurde, dass seine Anweisungen gegen geltende gesetzliche Bestimmungen gemäß Klausel 7.1(b) verstoßen.

d) Bei Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bestätigt dem Verantwortlichen, dass dies geschehen ist, oder gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht vorhandene Kopien, es sei denn, dass eine Aufbewahrungspflicht nach dem Recht der Union oder eines Mitgliedstaats besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I

Auftragsverarbeiter:

Name:	*XU Group GmbH*
Adresse:	*Mehringdamm 33, 10961 Berlin*
Name, Funktion und Kontaktdaten:	*Michael Seidl, Head of Business Technology & Information Security*
Name:	*Projekt 29 GmbH & Co. KG*
Adresse:	*Ostengasse 14, 93047 Regensburg*
Name, Funktion und Kontaktdaten:	*Christian Volkmer, Datenschutzbeauftragter*

ANHANG II

Beschreibung der Verarbeitung

Kategorien von betroffenen Personen, deren personenbezogene Daten verarbeitet werden

Nutzer, die sich auf der XU-Plattform registrieren. Diese Nutzer sind Kunden des Auftraggebers.

Kategorien der verarbeiteten personenbezogenen Daten

Um sich für die XU-Plattform anzumelden, benötigt XU in der Regel die folgenden personenbezogenen Daten:

- E-Mail-Adresse
- Vollständiger Name

Um sich für die XU-Plattform anzumelden, nutzt XU drei Verfahren:

Direkte Einladungen: Wir senden potenziellen Nutzern personalisierte E-Mail-Einladungen mit einem Registrierungslink. Im Rahmen dieses Prozesses werden der Vor- und Nachname erfasst, um die Einladung zu personalisieren. Die Empfänger müssen den Registrierungsprozess abschließen, um Zugang zur Plattform zu erhalten. Die Einhaltung der Datenschutzgesetze wird durch die Einholung der erforderlichen Einwilligungen vor der Erfassung und Verwendung personenbezogener Daten gewährleistet.

Selbstregistrierung: Bei dieser Methode können sich Personen ohne vorherige Einladung direkt auf der Plattform anmelden, sofern sie über eine E-Mail-Adresse aus einer zugelassenen Domain verfügen. Dadurch wird sichergestellt, dass die Registrierung auf bestimmte Organisationen oder Gruppen beschränkt ist. Es gibt keine zusätzlichen Alters- oder Identitätsprüfungen, was den Onboarding-Prozess vereinfacht.

Token-Zugang: Tokens werden an berechtigte Personen verteilt und gewähren ihnen das Recht, sich auf der Plattform zu registrieren. Diese Methode stellt sicher, dass nur autorisierte Benutzer auf den Registrierungsprozess zugreifen können. Tokens können so gestaltet werden, dass sie ablaufen und den Zugriff auf bestimmte Funktionen oder Inhalte einschränken, wodurch die Sicherheit und Exklusivität erhöht wird.

Verarbeitete sensible Daten (falls zutreffend) und geltende Einschränkungen oder Schutzmaßnahmen, die der Art der Daten und den damit verbundenen Risiken in vollem Umfang Rechnung tragen, wie z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugriff auf die Daten, Beschränkungen der Weitergabe oder zusätzliche Sicherheitsmaßnahmen

Um die XU-Plattform nutzen zu können, ist eine namentliche Registrierung auf der Plattform im Registrierungsbereich erforderlich. Nur Personen, denen eine Lizenz zur Nutzung der XU-Plattform erteilt wurde, dürfen sich registrieren. Bei der Registrierung sind wahrheitsgemäße Angaben zu machen und die Verwendung des richtigen Namens ist obligatorisch.

Art der Verarbeitung

XU: Die Daten werden automatisiert und anonymisiert verarbeitet. Wir speichern die Daten sicher und übertragen sie nur über verschlüsselte Verbindungen.

Zweck(e), zu dem/denen die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

Kunden und Nutzer erklären sich damit einverstanden, dass XU sie im Auftrag des Verantwortlichen über die bei der Registrierung angegebenen Daten (z. B. Name, E-Mail-Adresse) kontaktiert. Gründe für die Kontaktaufnahme können sein: Erinnerung an auf der Plattform gebuchte Webinare, Nachbereitung der Webinare, Auswertung der Lerngewohnheiten, Erinnerung an nicht abgeschlossene Lernmodule, Überwachung des Lernprozesses, Neuigkeiten zur XU-Plattform und Einholung von Feedback.

Zwecke der Verwendung personenbezogener Daten im Auftrag des Verantwortlichen können auch sein: Informationen über E-Mail-Adressen zum Abgleich mit dem Kundenstamm. Bereitstellung und Nutzung der XU-Plattform für Kunden. Durchführung spezifischer Lernmodule mit dem Ziel der Weiterbildung im Bereich des Verantwortlichen.

Zu den personenunabhängigen Daten gehören das Lernverhalten der Nutzer insgesamt auf der XU-Plattform, d. h. welche Inhalte wie oft gelernt wurden, Anmelderaten für Webinare usw.

Dauer der Verarbeitung

2 Monate, Dauer des Pilotprojekts. Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch der Zweck, die Art und die Dauer der Verarbeitung anzugeben.

ANHANG III

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Datensicherheit

ERLÄUTERUNG:

Die technischen und organisatorischen Maßnahmen müssen konkret beschrieben werden; eine allgemeine Beschreibung reicht nicht aus.

Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen, die der/die Verantwortliche(n) getroffen hat/haben (einschließlich aller relevanten Zertifizierungen), um unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen ein angemessenes Schutzniveau zu gewährleisten Beispiele für mögliche Maßnahmen:

Siehe Anhang „TOM“

ANHANG IV

Liste der Unterauftragsverarbeiter

ERLÄUTERUNG:

Dieser Anhang muss von Unterauftragsverarbeitern im Falle einer gesonderten Genehmigung (Klausel 7.7(a), Option 1) ausgefüllt werden.

Der Verantwortliche hat die Verwendung der folgenden Unterauftragsverarbeiter genehmigt:

Unterauftragsverarbeiter	Erbrachte Dienstleistung	Art der verarbeiteten personenbezogenen Daten	Zweck der Datenverarbeitung
Sachbearbeiter	Authentifizierungsdienste	- Benutzerkennungen (z. B. Benutzernamen, E-Mail-Adressen) - Authentifizierungstoken - IP-Adressen	Zur Authentifizierung von Benutzern, die auf die LXP zugreifen, und zur sicheren Verwaltung von Benutzersitzungen.
Posthog	Tracking und Analyse	- Daten zu Benutzerinteraktionen (z. B. Seitenaufrufe, Klicks) - Browser- und Geräteinformationen - IP-Adressen	Zur Analyse des Benutzerverhaltens innerhalb der LXP, zur Optimierung der Benutzererfahrung und zur Verbesserung der Plattformfunktionalität.
Sentry	Fehlerüberwachung und -meldung	- Benutzerkennungen (bei angemeldeten Benutzern während eines Fehlers) - Technische Daten zu Fehlern (z. B. Stacktraces, Browserinformationen) - IP-Adressen	Zur Überwachung, Identifizierung und Behebung von Fehlern innerhalb der LXP, um einen reibungslosen und zuverlässigen Betrieb der Plattform zu gewährleisten.
Heroku	Cloud-Hosting-Dienste	- Alle personenbezogenen Daten, die von der LXP verarbeitet werden, da Heroku die gesamte Plattform hostet - Protokolle, die IP-Adressen und Daten zur Benutzeraktivität enthalten können	Bereitstellung einer sicheren und skalierbaren Infrastruktur für das Hosting Ihrer LXP, um Verfügbarkeit und Leistung zu gewährleisten.
Typeform	Umfragen und Formularerstellung	- In Formularen angegebene Benutzerkennungen und Kontaktinformationen - Antworten auf Umfrage-/Formularfragen, die personenbezogene Daten enthalten können	Um interaktive Umfragen und Formulare für Benutzerfeedback, Registrierung und andere Datenerfassungsaktivitäten innerhalb der LXP zu erstellen und zu verwalten.
Azure	Cloud-Computing-Dienste	- Alle personenbezogenen Daten, die von der LXP verarbeitet werden, wenn Azure-Dienste für Hosting, Datenbanken oder andere	Bereitstellung einer Reihe von Cloud-Diensten, einschließlich Hosting, Datenbanken und Analysen, zur

		Cloud-Dienste verwendet werden - Protokolle und Diagnosedaten	Unterstützung der Infrastruktur und Funktionen der LXP.
HubSpot	Marketing- und CRM-Dienste	- Benutzerkennungen wie E-Mail-Adressen - Daten zum Marketingengagement (z. B. E-Mail-Öffnungen, Klicks) - CRM-Daten zu Benutzerinteraktionen und -präferenzen	Zur Verwaltung von Marketingkampagnen, E-Mail-Kommunikation und Kundenbeziehungsaktivitäten sowie zur Analyse der Nutzerinteraktion und -präferenzen.
New Relic	Leistungsüberwachung	- Technische Daten zur Anwendungsleistung - Anonymisierte Benutzersitzungsdaten für die Leistungsanalyse - IP-Adressen in Protokollen	Zur Überwachung der Leistung der LXP, zur Identifizierung von Engpässen oder Problemen, die die Benutzererfahrung beeinträchtigen, und zur Verbesserung der Gesamteffizienz der Plattform.

Anhang „TOM“

Technische und organisatorische Maßnahmen (TOM)

gem. Artikel 32 EU-DSGVO, § 64 BDSG-neu

(Sicherheit der Datenverarbeitung)

Pseudonymisierung und Verschlüsselung

(Art. 32 Abs. 1 lit. a DSGVO, Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehen zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlich gesondert aufbewahrt werden und entsprechende technische und organisatorische Maßnahmen unterliegen.

Wir nutzen die Cloud-Services im Bereich der Infrastrukturdienste von Microsoft. Hierzu werden Umsetzungsverfahren zur Pseudonymisierung und Verschlüsselung direkt auf der Plattform eingesetzt. Zudem werden kryptographische Verfahren wie z.B. TLS und SSL zur Verschlüsselung verwandt. In Datenbanken, Festplatten und Datensicherungen werden zusätzlich Verschlüsselungen mittels RSA realisiert. Ein Konzept für eine generelle Pseudonymisierung wird derzeit erarbeitet. Hier können personenbezogene Daten sinnvoll minimiert und dessen Verarbeitung datensparsam eingeschränkt werden.

Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen

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

Vertraulichkeit

Maßnahmen zur Gewährleistung der Vertraulichkeit der Systeme und Dienste, die einen unautorisierten Zugriff auf personenbezogene Daten verhindern sollen.

Zutrittskontrolle

Unbefugten ist der Zutritt zu den Räumen, in denen personenbezogene (pb) Daten verarbeitet werden, zu verwehren.

Dies wird durch nachfolgende Maßnahmen realisiert: Sicherheitsschlösser, ein Schließsystem mit Codesperre, ein manuelles Schließsystem, Alarmanlagen, Videoüberwachung, Gefahrenmeldeanlagen mit Verbindung mit einer Zentrale. Außerdem werden Besuche von Fremden Dritten protokolliert.

Eine Videoüberwachung ist sehr heikel, stellt sie doch einen erheblichen Eingriff in das Persönlichkeitsrecht dar. Daher bedarf eine Videoüberwachung immer einer legitimierenden Rechtsform. Die Wahrnehmung des Hausrechts und die Wahrnehmung berechtigter Interessen (möglicher Einbruch) sind Gründe, Kameras einzusetzen. Wichtig ist uns, dass der Zweck (für jede eingesetzte Videokamera) dokumentiert ist, damit die Aufsichtsbehörde bei einer Kontrolle den Einsatz nachvollziehen kann.

Es wird auf die Videoüberwachungsanlage deutlich hingewiesen werden (z.B. mit Schildern). Tonaufnahmen sind unzulässig. Bei einer Video-Überwachung dokumentieren wir folgende Punkte: Ort der Kameras, Standorte der Monitore, Hinweis auf Videoüberwachung gegeben, Aufzeichnungsart, Aufbewahrungsdauer, Aufbewahrungsort.

Schlüsselregelung/Schlüsselbuch

Die Schlüsselvergabe wird zentral verwaltet und dokumentiert. Dabei wird die Herausgabe der Schlüssel, wer zu welchen Räumen Zutritt hat und wer den Generalschlüssel hat namensscharf dokumentiert. Zudem besteht eine Pflicht Mitarbeiter- und Gästeausweise sichtbar bei sich zu tragen. Zutritt für Fremdpersonal ist ausschließlich in Begleitung von Internen gestattet. Zusätzlich müssen sich das Fremdpersonal in eine Liste eintragen. Außerdem besteht eine Regelung, die den Mitarbeiter, der am aktuellen Arbeitstag als letztes die Räumlichkeiten des Unternehmens verlässt, dazu verpflichtet die Räumlichkeiten abzuschließen. Bei Verlust des Schlüssels wird dies umgehend angezeigt und aufgrund der elektronischen Form kann der Schlüssel umgehend gesperrt werden. Um die Historie der Zutrittsberechtigungen in einer Übersicht zu vorliegen zu haben, wird ein Schlüsselbuch geführt.

Zugangskontrolle

Unbefugtes Nutzen der Datenverarbeitungssysteme muss verhindert werden.

Dazu erfolgt eine Authentifikation ausschließlich passwortgeschützt und unter Nutzung einer Zwei-Faktor-Authentifizierung mit Sperr-Routine bei zu häufiger Falscheingabe. Des Weiteren werden aktuelle Anti-Virenschutzprogramme und Firewalls mit regelmäßigen Aktualisierungen sowohl der Programme und Signaturen eingesetzt.

Durch die Benennung von klaren Verantwortlichen für die Updates und das Patchmanagement entspricht die jeweilige Installationsversion der aktuellen Empfehlungen des Herstellers.

Bildschirmschoner werden mit Passwort zur Reaktivierung versehen, um auch hier den Zugang auch während der Geschäftszeiten bei kurzer oder längerer Abwesenheit sicher zu gestalten.

Benutzerprofile werden mit unterschiedlichen Berechtigungen erstellt und mit Passwörtern versehen. Die Benutzer-Accounts werden im Rahmen der dafür festgelegten Richtlinien überwacht. Die Nutzung der Passwörter ist so angelegt, dass sie verpflichtend ist. Für die Erstellung von Passwörtern wurden Richtlinien festgelegt. Für die Anmeldung besteht eine begrenzte Anzahl an Fehlversuchen.

Die Rechnergehäusen sind verriegelt. Für den Einsatz von außen wird eine VPN-Technologie verwendet, um auf interne Systeme zugreifen zu können. Externe Schnittstellen wie USB-Sticks oder CD-ROMs sind per Einstellung gesperrt. Inhalte davon können nicht auf das interne System übertragen werden. Ein Intrusion-Detection-Systemen findet hierfür Einsatz. Für die Verwendung von Externen Datenträgern gibt es klare Richtlinien. Darüber hinaus sind die Mitarbeiter angewiesen eine Clean Desk Policy zu pflegen.

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Hierzu werden viele Maßnahmen eingesetzt. Beginnend mit einem Nutzer-Berechtigungskonzept mit einer zeitnahen Sperrung/Löschung der Berechtigungen für ausgeschiedener Mitarbeiter. Die Verwaltung der Nutzerrechte erfolgt durch den Systemadministrator und dem jeweiligen Projektmanager mittels Vier-Augen-Prinzip. Die Anzahl der Administratoren wird dabei auf das Notwendigste reduziert. Um dem Prinzip der Funktionstrennung zu folgen, werden die Admin-Nutzerrechte getrennt nach Lernplattform, CRM und andere Applikationen eingerichtet.

Selbstverständlich finden unsere Passwort Richtlinien auch hier Anwendung. Die Zugriffe auf Anwendungen werden protokolliert und vor Wiederverwendung der Daten findet eine physische Löschung der Datenträger statt.

Falls Datenträger vernichtet werden müssen, so findet dieser Vorgang auch ordnungsgemäß statt. In unserem Unternehmen kommen zudem auch Aktenvernichter zum Einsatz. Ergänzend werden aber auch Dienstleister zur Aktenvernichtung in Anspruch genommen. Die Datenträger und Aktenordner werden bis zur Vernichtung in abschließbaren Schränken aufbewahrt.

Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Hierfür werden Daten physikalisch getrennt auf gesonderten Systemen oder Datenträgern gespeichert. Datensätze von unterschiedlichen Personen werden logisch getrennt und mit Zweckattributen/Datenfeldern versehen. Zuordnungsdaten werden wiederum auch von den eigentlichen Daten getrennt und pseudonymisiert.

Die Vorgaben im Berechtigungskonzept legen die Datenbankrechte fest. Es besteht eine Trennung von Produktiv- und Testsystem.

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

Maßnahmen zur Gewährleistung der Integrität der Systeme und Dienste, die gewährleisten, dass personenbezogene Daten nicht (unbemerkt) geändert werden können.

Weitergabekontrolle

Maßnahmen, die 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.

Um die Weitergabekontrolle ausreichend gewährleisten zu können, greifen wir auf die Nutzung von Standleitungen bzw. VPN-Tunneln zurück. Die Weitergabe von Daten erfolgt in anonymisierter oder pseudonymisierter Form. Außerdem werden Passwörter separat auf alternativen Kommunikationskanälen übermittelt.

Die E-Mail-Übertragung (SSL/TLS) wie die E-Mail-Inhalte (GPG/PGP bzw. S/MIME) werden verschlüsselt. Die Datenweitergabe erfolgt anhand vertraglich vereinbarten Rechten und Pflichten. Die Datenträger werden eindeutig dokumentiert und Löschfristen festgelegt.

Wenn notwendig, werden Datenträger für den Transport sicher verpackt und die Auswahl von Transportpersonal bzw. -dienstleistern erfolgt sorgfältig. Es bestehen Regelungen zum sicheren Transport von Datenträgern und Dokumentation des Datentransportes (Empfänger von Daten, Zeitspanne der geplanten Überlassung und Löschfristen etc.). Wenn mobilen Datenträger zum Einsatz kommen, so beinhalten diese eine Verschlüsselungsfunktion.

Innerhalb des Unternehmens ist auch das WLAN verschlüsselt (mind. WPA 2). Falls sensible Daten weitergegeben werden sollen, so geschieht auch dies in verschlüsselter Form mit SFTP/PGP und dem Einsatz von Checksummen/Hash-Verfahren beim Packen/Entpacken von Dateien. Für die kryptographischen Schlüssel wurde eine Verwaltung eingerichtet.

Um einen Überblick zu behalten, wurde eine Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen erstellt.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Um dies zu gewährleisten, protokollieren wir die der Eingabe, Änderung und Löschung von Daten in unserem System. Die Protokollkontrolle findet manuell oder automatisiert statt. Jeder Nutzer erhält einen Individuellen Benutzernamen.

Auch auf die sichere Aufbewahrung von Papierunterlagen, von denen Daten ins EDV-System übernommen wurden, wird wert gelegt.

Insbesondere setzen wir hier auch auf die Maßnahmen die Nachvollziehbarkeit durch Berechtigungskonzept sukzessive zu gewährleisten.

Technisch

Des Weiteren kommen diverse technische Maßnahmen zum Einsatz, um eine angemessene Eingabekontrolle sicherzustellen. Office 365 und Azure Logs (Admin Audit Log) sind die führenden Systeme, wenn es um die Protokollierung geht. Als Dokumentenmanagementsystem ist SharePoint zum Einsatz. Logfiles werden für die Nachvollziehbarkeit der Löschung, Änderung, Anlegen von personenbezogenen Daten angelegt. Diese werden versioniert und alte Logfiles im Papierkorb abgelegt. Mit der Lernplattform SSO soll das (unbeabsichtigte) Überschreiben der Daten verhindert werden.

Organisatorisch

Auch organisatorische Maßnahmen sind implementiert, um eine angemessene Eingabekontrolle sicherzustellen. Die einzigen Programme, in denen Daten eingegeben, geändert, oder gelöscht werden können, sind die Lernplattform, im Browser, in Office 365 und in den Apps. Zur Nachvollziehbarkeit der Aktionen erhält jeder Benutzer seinen individuellen Benutzernamen. Auch die Vergabe Rechten zur Eingabe, Änderung oder Löschung erfolgt individuell. Über die Rechtvergabe entscheiden der Admin, die XU, das Learn-Management-System und der Kunde. Die Vergabe der Zugriffsrechte auf die Logfiles erfolgt ausschließlich über den Admin.

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

Es muss sichergestellt werden, dass personenbezogene Daten gegen (zufällige) Zerstörung oder Verlust geschützt werden. Und andererseits muss die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sein.

Verfügbarkeit

Gewährleistung, dass personenbezogene Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn sie gebraucht werden. Die Fähigkeit, die Verfügbarkeit der

personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit. c DSGVO). Gewährleistung, dass eingesetzte Systeme und Dienste im Störungsfall schnell wiederhergestellt werden können.

Belastbarkeit

Gewährleistung, dass die Systeme und Dienste so ausgelegt sind, dass auch punktuell hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen leistbar bleiben.

Technisch

Für die Router und die Firewall besteht ein Überspannungsschutz. Der Anbieter setzt eine Monitoring-Software zur ständigen Überwachung einer reibungslosen Datensicherung ein. Dies ist vertraglich sichergestellt. Der installierte Virenschutz und die Firewall sind von Windows. Genügend Speicher- und Leistungskapazitäten sind vorhanden. Diese werden regelmäßig mit einem Last- und Performancetest geprüft. Backups, Spiegelungen von Festplatten werden in der Cloud erstellt, wo auch die redundante Datenspeicherung stattfindet. Recoverytests werden auch lokal durchgeführt. Um Angriffe, die gegen ein Computersystem oder Rechnernetz gerichtet sind, zu erkennen, wird ein Intrusion-Detection-Systems (IDS) eingesetzt.

Organisatorisch

Es wird nach einem Datenschutzkonzept gehandelt, was allerdings beim Anbieter liegt. Genauso wie die räumlich getrennte Archivierung der Datensicherungen an einem sicheren Ort. Die Schulung der Mitarbeiter hinsichtlich der Nutzung der IT-Systeme übernimmt der Hauseigene Datenschutzbeauftragte. Die Sensibilisierung der Mitarbeiter hinsichtlich des betrieblichen Datenschutzes ist in Planung. Die Admins sind für die Überwachung der technischen Maßnahmen verantwortlich.

Auftragskontrolle

Die Auftragskontrolle ist nur anwendbar im Falle der Auftragsdatenverarbeitung im Sinn des § 62 BDSG neu, bzw. Art. 28 DSGVO. Es muss sichergestellt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen lt. Vertrag verarbeitet werden

Technisch

Im Fall der Rolle des Auftragnehmers bei der Auftragsdatenverarbeitung erfüllen wir die technischen Anforderungen.

Organisatorisch

Auftragnehmer werden sorgfältig im Hinblick auf den Datenschutz ausgewählt (betrifft auch Subunternehmen). Die Vertragsgestaltung wird eindeutig nach §62 BDSG neu bzw. Art. 28 DSGVO festgelegt. Der Datenschutzbeauftragte des Auftragnehmers wird konkret benannt und dessen Kontaktdaten mitgeteilt. Die TOMs des Dienstleisters werden nach der Angemessenheit in Art. 32 Abs. 1 DSGVO kontrolliert. Löschfristen sind festgelegt. Ein Löschkonzept ist aktuell in Planung. Auch die Sicherstellung der weisungsgemäßen Durchführung der Auftragsdatenverarbeitung als Auftragnehmer befindet sich in Planung. Die Kontrollrechte des Auftraggebers der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen (auch bei Subunternehmen) sind schriftlich festgelegt. Der Auftraggeber hat das Recht auf Kontrolle zur Vertragsausführung. Eine Übersicht über die Dienstleister und deren Dienstleistungen ist vorhanden.

Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
(Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 DSGVO)

Zur regelmäßigen Überprüfung und Bewertung der Maßnahmen wurden auch hier technische und organisatorische Maßnahmen ergriffen.

Technisch

Neben einer technischen Überprüfung wird die technische Umsetzung nach Zertifikat-Anforderungen kontrolliert. Außerdem wird Wert darauf gelegt die Technik aktuell zu halten.

Organisatorisch

Eine Datenschutzrichtline wurde erstellt. Die Verantwortlichen für die regelmäßigen Prüfungen sind benannt. Die Maßnahmen werden auf Wirksamkeit überwacht und bewertet. Falls Handlungsbedarf besteht, kann dieser somit festgestellt werden. Zertifizierungen liegen vor.