

# Allgemeine LXT-Vertragsbedingungen für die Transfer Toolbox

(Stand: 11. Mai 2021)

## § 1 Vertragsgegenstand und Begriffsbestimmungen

- (1) Vertragsgegenstand ist der Lizenzkauf der von uns in Kooperation mit dem Institut für Transferwirksamkeit (ITW) entwickelten Plattform Transfer Toolbox. Diese Corporate E-Learning-Software im Rahmen eines Software as a Service (SaaS) wie von Ihnen als **gewerblicher Kunde** (nachfolgend „Kunde“) gemäß unserem Angebot (nachfolgend „**BI-Angebot**“) bestellt.
- (2) Als „**Transfer Toolbox**“ ist die von Ihnen zur Nutzung bestellte und von uns zur Verfügung gestellte Zugriff auf die E-Learning Plattform bezeichnet. BI bietet zahlreiche weitere Lerninhalte, Tools und Systeme zur Entwicklung von „Learning Professionals“. BI erteilt somit nutzerbasierte Lizenzrechte für Lerner, die der Kunde zur Nutzung bestimmt und berechtigt.
- (3) Die nachstehenden Begriffe, die in diesen Allgemeinen Vertragsbedingungen verwendet werden, haben folgende Bedeutung:
  - „**Kunde**“ sind Sie als Vertragspartner von BI, dem die Nutzung der Transfer Toolbox einschließlich der Nutzerlizenzen zu den nachfolgenden Bedingungen überlassen wird. „Kunde“ kann eine natürliche oder eine juristische Person oder sonstige Institution sein, die die von BI hiermit zur Verfügung gestellte Plattform von natürlichen Personen nutzen lässt. Eventuelle nach § 15 AktG mit dem Kunden verbundene Unternehmen sind hingegen nicht als „Kunde“, also als Vertragspartner, beteiligt. Dies auch nicht, wenn die vom Kunden berechnete Nutzer einem mit dem Kunden verbundenen Unternehmen angehören.
  - „**Nutzer**“ sind alle natürlichen Personen, die zur Nutzung der hiermit von BI zur Verfügung gestellten Transfer Toolbox berechtigt sind. Soweit nichts anderes geregelt ist, sind dies nur Nutzer, die entweder Gesellschafter des Kunden sind oder solche, die in einem Dienst-, Arbeits- oder Ausbildungsverhältnis oder auf sonstige Weise, den Weisungen des Kunden bei der Nutzung der Transfer Toolbox unterliegen.
  - Als „**Nutzungsvertrag**“ sind die hier gegenständliche **Allgemeinen Vertragsbedingungen**, zur Nutzung der Transfer Toolbox, **einschließlich Anlagen** in Verbindung mit dem **BI-Angebot** bezeichnet.
  - „**Nutzungsbedingungen**“ sind die Bedingungen zur Nutzung der Transfer Toolbox in ihrer Anwendung gemäß Anlage, die von allen Nutzern der Transfer Toolbox vor der Anwendung zu lesen und zu beachten sind.

## § 2 Vertragsschluss, Geltungsbereich der Allgemeinen LXT-Vertragsbedingungen für die Transfer Toolbox

- (1) Bei einer Bestellung der Transfer Toolbox gemäß BI-Angebot, schließen Sie den Nutzungsvertrag mit:

**Bildungsinnovator** (eLearning Manufaktur GmbH), Erkrather Straße 401, 40231 Düsseldorf

E-Mail:	sales@bildungsinnovator.com
Telefon:	0211 176074 80
Telefax:	0211 545559 89
Handelsregister	Amtsgericht Düsseldorf HRB 73424
Vertretungsberechtigte/r Geschäftsführer:	Adolf Rudolf Riegler

- (2) Etwaige Präsentationen der Transfer Toolbox durch Vertreter von BI oder auf den Websites von BI oder durch andere Medien sind keine bindenden Angebote von BI. Vielmehr wird Ihnen nach Kontaktaufnahme mit BI die Möglichkeit gegeben, ein verbindliches Angebot zum Abschluss des Nutzungsvertrages mit BI gemeinsam zu erarbeiten. **Erst wenn Ihnen das nach Abstimmung erstellte BI-Angebot mit den Allgemeinen LXT-Vertragsbedingungen für die Transfer Toolbox zugeht und das BI-Angebot von Ihnen angenommen wird, kommt der Nutzungsvertrag unter Geltung der Allgemeinen LXT-Vertragsbedingungen für die Transfer Toolbox zustande.**
- (3) Den Zugang zu der Transfer Toolbox erhalten Sie von uns in der von uns bereitgestellten Lernplattform LXT zur Verfügung gestellt.
- (4) Änderungen oder Ergänzungen des Nutzungsvertrages durch individuelle Vertragsabreden im Sinne des § 305b BGB bedürfen keiner Form. Im Übrigen bedürfen Änderungen oder Ergänzungen der **Textform**. Eine mündliche Aufhebung des Textformerfordernisses ist nicht möglich.
- (5) Sind im BI-Angebot und in diesen Allgemeinen Vertragsbedingungen widersprüchliche Regelungen zum gleichen Gegenstand enthalten, gilt das im BI-Angebot Vereinbarte als spezielle individuelle Regelung zum Vertragsgegenstand vor.
- (6) Eventuelle **Einkaufsbedingungen/AGB des Kunden** haben nur Gültigkeit, wenn sie ausdrücklich von BI akzeptiert werden, wobei bei widersprüchlichen Leistungsbedingungen die Bedingungen nach diesem Vertrag stets vorrangig gelten.

## § 3 Vertragslaufzeit und Kündigung

- (1) Das Vertragsverhältnis beginnt am Tag der Bereitstellung des betriebsfähigen Transfer Toolbox.
- (2) Der Nutzungsvertrag läuft auf unbestimmte Zeit (Lifetime Lizenz).

- (3) Das Recht der Vertragsparteien zur **Kündigung aus wichtigem Grund** ohne Einhaltung einer Kündigungsfrist bleibt unberührt. Ein wichtiger Grund liegt vor, wenn die ausdrücklich geregelten Pflichten aus dem Nutzungsvertrag von einer Vertragspartei grob verletzt, sowie insbesondere dann, wenn über das Vermögen der anderen Vertragspartei das Insolvenzverfahren eröffnet wird oder die andere Vertragspartei insolvent oder zahlungsunfähig wird. Ein wichtiger Grund liegt ferner dann vor, wenn der Kunde mit der Entrichtung des Entgelts oder eines nicht unerheblichen Teils des Entgelts in Verzug ist.

#### § 4 Vergütung, Vergütung bei Veränderung der Nutzeranzahl

- (1) BI erhält eine **im Voraus** fällige einmalige Nutzungsgebühr, die sich der Höhe nach aus dem in § 1 Abs. 1 benannte und vom Kunden angenommene **BI-Angebot** ergibt.
- (2) Eine **individuelle Anpassung oder Weiterentwicklung von LXT für den Kunden** ist nicht Bestandteil dieses Vertrages.

#### § 5 Zahlungsbedingungen

- (1) Die im Voraus an BI zu entrichtende Vergütung gemäß § 4 wird erstmalig vor Bereitstellung der Transfer Toolbox in Rechnung gestellt. Spätestens 10 Tage nach Zugang der Rechnung ist die Vergütung fällig.
- (2) **BI-Rechnungen** werden **ausschließlich elektronisch versendet**. Die Versendung der Rechnung per Normalpost wird entsprechend den gesetzlichen Bestimmungen nur auf gesonderten Wunsch vorgenommen

#### § 6 Transfer Toolbox-Bereitstellung, sonstige Leistungen von BI und Mitwirkungspflichten des Kunden

- (1) Die für die Nutzung der Transfer Toolbox wird von BI bereitgestellt und gegen Zugriffe Dritter geschützt. Der zur Nutzung der Transfer Toolbox erforderliche Zugang zum Internet wird vom Kunden sichergestellt.
- (2) Jeder Nutzer erhält zu seiner Registrierung als Transfer Toolbox-Nutzer entweder unmittelbar per E-Mail von BI oder vom Kunden selbst seine persönlichen Zugangsdaten zugeschickt. Der Kunde ist verpflichtet, die zur Registrierung erforderlichen E-Mail-Adressen der Nutzer mitzuteilen und die Nutzer vorher darüber zu unterrichten.
- (3) Der Kunde erhält Lizenzrechte von BI. Der Kunde stellt deshalb sicher, dass die Transfer Toolbox ihrem Zweck (Lernen) entsprechend und nur in dem von ihm bestimmten Nutzerkreis genutzt wird. Veränderungen des Nutzerkreises (z. B. Änderung der E-Mail-Adressen der Nutzer) teilt der Kunde unverzüglich mit. Diese Pflicht besteht neben der persönlichen Pflicht der Nutzer gegenüber BI, die als **Anlage 1** beigefügten **LXT-Nutzungsbedingungen** einzuhalten. Die LXT-Nutzungsbedingungen sind zudem jederzeit auf der bereitgestellten LXT-Plattform einsehbar.
- (4) BI strebt eine Verfügbarkeitsquote der Plattform in Höhe von 99,5 % im Jahresmittel an.

## § 7 Nutzungsrechte

- (1) BI räumt dem Kunden, vorbehaltlich vollständiger Vergütung das einfache, nicht übertragbare, zeitlich unbegrenzte Recht zur Nutzung der Transfer Toolbox ein. Dies gilt auch in Bezug auf künftige Nutzungsformen der Transfer Toolbox.
- (2) Sollte BI die Transfer Toolbox nicht mehr über die LXT-Plattform bereitstellen, wird dem Kunden auf Wunsch ein SCORM-Paket zur Verfügung gestellt. In diesem Fall dürfen Sie das Ihnen zur Verfügung gestellte SCORM-Paket nicht an Dritte, ihrem Nutzerkreis nicht angehörigen, weitergeben.
- (3) Die von Ihnen erworbenen Nutzungslizenz berechtigt Sie und die Personen, die von Ihnen als Nutzer beim Erwerb der Nutzungslizenz bestimmt und uns gegenüber benannt werden (z.B. die Angehörigen Ihres Unternehmens oder einer bestimmten organisatorischen Einheit, die Ihren Weisungen bzw. Ihrer Aufsicht unterliegen) zur persönlichen und nicht übertragbaren Nutzung der Transfer Toolbox.
- (4) Im Übrigen gelten für die Transfer Toolbox für jeden Nutzer, die bei der Registrierung als Nutzer einsehbaren, hier als **Anlage 1** beigefügten **LXT-Nutzungsbedingungen**.
- (5) Nutzungsrechte, die aufgrund gesetzlicher Lizenzen, insbesondere nach Maßgabe der §§ 60a ff. UrhG wahrgenommen werden dürfen, sind nicht Gegenstand dieses Nutzungsvertrages und werden durch die überlassene Nutzung von LXT nicht berührt.

## § 8 Schutzrechtsverletzungen, Freistellungspflichten der Parteien

- (1) Die von BI in Kooperation mit dem Institut für Transferwirksamkeit hergestellte Transfer Toolbox und die überlassene Nutzung der LXT-Plattform, einschließlich dazu gehöriger Handbücher und Dokumentation, unterfällt dem Schutz des § 2 UrhG. Rechte Dritter an den geschützten Werken bleiben davon unberührt. BI ist deshalb nach vorheriger Ankündigung, unbeschadet etwaiger Schadensersatzansprüche des Kunden, jederzeit berechtigt auf eigene Kosten Änderungen an der Transfer Toolbox vorzunehmen, die gewährleisten, dass etwaige Verletzungen Schutzrechte Dritter durch die Transfer Toolbox oder die Nutzung der LXT-Plattform ausgeschlossen bleiben.
- (2) Dem Kunden obliegt es, die über die bei der Nutzung der Transfer Toolbox zu beachtenden Rechte Dritter aufzuklären.
- (3) Der Kunde stellt BI auf erstes Anfordern und auf eigene Kosten von allen Ansprüchen Dritter frei, sofern die Inanspruchnahme von BI durch Dritte auf die behauptete vertrags- oder gesetzeswidrige Nutzung der Transfer Toolbox durch den Kunden oder den Nutzer beruht. Umgekehrt stellt BI den Kunden von Ansprüche Dritter frei, die auf einer behaupteten Schutzrechtsverletzung von BI als Anbieterin der Transfer Toolbox beruhen. Die Parteien sind einander zur unverzüglichen Unterrichtung über etwaige geltend gemachte Ansprüche Dritter, die die gegenseitige Freistellungspflicht begründen, verpflichtet.

## § 9 Gewährleistung, Wartung und Service-Leistungen

- (1) BI überlässt die Transfer Toolbox in einem zum vertragsgemäßen Gebrauch geeigneten Zustand und erhält diesen Zustand. Die Pflicht zur Erhaltung beinhaltet nicht die Anpassung der Transfer Toolbox an veränderte Einsatzbedingungen, technische und funktionale Entwicklungen wie die Veränderung der IT-Umgebung des Kunden, insbesondere Änderung der Hardware oder des Betriebssystems, Anpassung an den Funktionsumfang konkurrierender Produkte oder Herstellung der Kompatibilität mit neuen Datenformaten.
- (2) Leistungen von BI, die zum Ziel haben, die Transfer Toolbox auf dem aktuellen technischen Stand zu halten (Wartungsleistungen) oder Störungen zu beheben, werden zu den Bedingungen des § 6 Nr. 4 behoben.

## § 10 Haftung

- (1) BI haftet unbeschränkt für **Schäden aus Verletzung des Lebens, des Körpers oder der Gesundheit sowie für Schäden, die auf Vorsatz und grobe Fahrlässigkeit** von BI oder eines seiner Erfüllungsgehilfen beruhen. Für Schäden, die auf eine **leicht fahrlässige Verletzung vertragswesentlicher Pflichten** beruhen, haftet BI für den vertragstypisch vorhersehbaren Schaden, mit dessen Entstehung typischerweise gerechnet werden muss. Für **sonstige Fälle leicht fahrlässigen Verhaltens** ist die Haftung von BI auf EUR 25.000,00 je Schadensfall begrenzt.
- (2) Im **Fall des Datenverlustes** haftet BI nur für den typischen Wiederherstellungsaufwand, der bei regelmäßiger und gefahrensprechender Anfertigung von Sicherungskopien eingetreten wäre
- (3) Die verschuldensunabhängige Haftung von BI für Mängel der Transfer Toolbox, die bereits bei Vertragsschluss vorhanden waren (§ 536a Abs. 1 Halbsatz 1 BGB) ist ausgeschlossen.
- (4) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

## § 11 Datenschutz, Datenschutz Tätigkeiten für den Kunden

- (1) Bei der Nutzung der Transfer Toolbox werden personenbezogene Daten verarbeitet. Einzelheiten dazu sind den **Informationen zur Datenverarbeitung (IDV)** gemäß **Anlage 3** zu entnehmen. Die IDV sind zudem auf der LXT-Plattform jederzeit in ihrer aktuellen Version einsehbar.
- (2) Der Kunde ist „Verantwortlicher“ und BI „Auftragsverarbeiter“ i.S.d. Art. 28 DSGVO, sofern mindestens eine der folgenden Personengruppen bei der Datenverarbeitung betroffen ist:
  - Nutzer der Transfer Toolbox wie in § 1 Abs. 3 definiert;
  - Nutzer, die sich über die von BI im Rahmen dieses Vertrages zur Verfügung gestellten Registrierungsdaten persönlich anmelden.

Die Parteien schließen zur Konkretisierung ihrer datenschutzrechtlichen Verpflichtungen den als **Anlage 4** mit seinen Anhängen (**TOM-Liste, Liste der Unterauftragsverarbeiter, Liste der beim RZ-Betreiber IPB ergriffenen technischen und organisatorischen Maßnahmen**) beigefügten **„Vertrag über Auftragsverarbeitung“ i.S.d. Art. 28 Abs. 3 DSGVO**.

- (3) **Individuelle vergütungspflichtige Datenschutz Tätigkeiten** für den Kunden, die im Rahmen der Auftragsverarbeitung anfallen, sind gemäß § 4 Abs. 3 des Auftragsverarbeitungsvertrag (Anlage 4) geregelt und gesondert vom Kunden zu beauftragen.

**§ 12 Übertragbarkeit der Rechte aus diesem Vertrag, Abtretungsverbot, Rechtswahl und Gerichtsstandsvereinbarung, salvatorische Klausel**

- (1) Weder diese Vereinbarung noch jeglicher Anspruch hieraus ist ohne vorherige schriftliche Zustimmung der anderen Partei auf einen Dritten übertragbar bzw. abtretbar.
- (2) Es gilt deutsches Recht.
- (3) Gerichtsstand für alle Streitigkeiten, die im Zusammenhang mit diesem Vertrag entstehen, ist Düsseldorf. Es bleibt BI jedoch unbenommen, den Kunden auch an dessen Sitz zu verklagen.
- (4) Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder nichtig sein oder werden, berührt dies nicht die Wirksamkeit des Vertrages im Übrigen. Die Parteien verpflichten sich, die unwirksame oder nichtige Bestimmung durch eine wirksame Bestimmung zu ersetzen, die dem rechtlich und wirtschaftlich Gewollten am nächsten kommt.

**Anlagen:**

- Anlage 1: LXT-Nutzungsbedingungen  
Anlage 3: Informationen zur Datenverarbeitung (IDV)  
Anlage 4: Auftragsverarbeitungsvertrag (einschl. Anhänge: TOM-Liste, Unterauftragsverarbeiter)

# LXT-Nutzungsbedingungen

Stand: 05. Januar 2021

Die LXT-Plattform ist eine auf einem Cloud-Server von uns, **Bildungsinnovator, eLearning Manufaktur GmbH, Erkrather Straße 401, 40231 Düsseldorf** laufende Software. LXT ermöglicht es Ihnen als Nutzer Lerninhalte zu produzieren und mit anderen („Lerner“ und „Autoren“), die wie Sie von unserem Kunden (nachfolgend „**Ihr Unternehmen**“) zur Nutzung von LXT berechtigt sind, zu teilen. Die Einrichtung Ihres Nutzerkontos im Auftrag Ihres Unternehmens setzt voraus, dass Sie gemäß dem zwischen uns und Ihrem Unternehmen bestehenden Nutzungsvertrag über die LXT-Plattform (nachfolgend „Nutzungsvertrag“ genannt), den folgenden Nutzungsbedingungen zustimmen.

## **§ 1 Voraussetzungen Ihrer Nutzung der LXT-Plattform**

Zur Nutzung der LXT-Plattform erhalten Sie von Ihrem Unternehmen oder unmittelbar von uns Ihre Zugangsdaten (Registrierungsdaten), die Sie ausschließlich zur persönlichen und nicht übertragbaren Nutzung für die Dauer unseres Nutzungsvertrages mit Ihrem Unternehmen berechtigen.

Sie sind als Nutzer zum Zeitpunkt der Registrierung verpflichtet, wahre Angaben über Ihre Person, insbesondere über Ihre Angehörigkeit zum Kreis der LXT- Nutzungsberechtigten Ihres Unternehmens, zu machen.

Ihre Zugangsdaten dürfen Sie nicht an Dritte weitergeben und müssen diese sicher verwahren. Ihre Zugangsdaten erhalten Sie bei Verlust ausschließlich über die uns von Ihrem Unternehmen zuvor mitgeteilte E-Mail-Adresse.

## **§ 2 Nutzungsdauer, Beendigung des Nutzungsrechts, Nutzungssperre**

Die Dauer Ihrer Nutzungsberechtigung richtet sich nach der vereinbarten Dauer des Nutzungsvertrages und setzt Ihre Zugehörigkeit zum Kreis der von Ihrem Unternehmen berechtigten Nutzer voraus. Ihre Nutzungsberechtigung endet deshalb nicht nur spätestens mit der Beendigung des LXT-Nutzungsvertrages, sondern auch wenn Ihnen die Nutzung unmittelbar durch Ihr Unternehmen nicht mehr gestattet wird. Das kann zum Beispiel der Fall sein, wenn Sie als Mitarbeiter des Unternehmens ausscheiden.

Für den Fall, dass wir feststellen sollten, dass Sie nicht mehr von Ihrem Unternehmen zur Nutzung von LXT berechtigt sind, sind wir berechtigt Ihr Nutzerkonto unverzüglich und ohne vorherige Ankündigung zu sperren.

Zur Sperre Ihres Nutzerkontos sind wir ebenfalls berechtigt, wenn Anhaltspunkte dafür bestehen, dass Ihr Konto durch einen nicht berechtigten Dritten genutzt wird, oder wenn die Anwendbarkeit oder die Sicherheit der von uns zur Verfügung gestellten LXT-Plattform durch Ihr Verhalten oder durch die Nutzung von Ihrem Nutzerkonto aus beeinträchtigt wird.

Wenden Sie sich deshalb im Fall einer Sperre, die Sie für nicht berechtigt halten, zunächst an Ihrem für uns zuständige Ansprechpartner in Ihrem Unternehmen, der sich mit uns in diesem Fall in Verbindung setzen wird.

### **§ 3 Umfang des Nutzungsrechts, Einschränkungen der Nutzung der LXT-Plattform**

Mit der Registrierung und Zustimmung zu diesen Nutzungsbedingungen erhalten Sie ein einfaches, nicht übertragbares Recht zur Nutzung der LXT-Plattform mit dem Zweck innerhalb des Kreises der von Ihrem Unternehmen berechtigten Nutzer Lerninhalte zu Erstellen oder mit anderen Nutzern zu teilen.

Die Systemvoraussetzungen der Nutzung der LXT-Plattform, etwaige Erweiterungen des Nutzungszweckes oder des Nutzerkreises vereinbaren wir ausschließlich mit Ihrem Unternehmen in dessen Auftrag wir Ihnen die Nutzung dieser Plattform ermöglichen.

Als Betreiberin der LXT-Plattform behalten wir uns das Recht vor, den Betrieb der Plattform vorübergehend einzustellen, sofern dies zur Weiterentwicklung oder zur Abwendung einer Fehl- oder Sicherheitsfunktion erforderlich ist. Damit verbundene Nutzungseinschränkungen werden Ihrem Unternehmen, zu dessen Nutzerkreis Sie angehören angekündigt bzw. angezeigt.

Über zeitliche, räumliche oder zweckgebundene Voraussetzungen Ihrer persönlichen Nutzungsberechtigung ist allein Ihr Unternehmen Ihnen gegenüber zur Aufklärung berechtigt und verpflichtet.

Wenden Sie sich deshalb im Fall einer Nutzungsbeeinträchtigung zunächst an Ihrem für uns zuständige Ansprechpartner in Ihrem Unternehmen, der sich mit uns in diesem Fall in Verbindung setzen wird

### **§ 4 Technische Voraussetzungen, Kosten der LXT-Nutzung**

Die technischen Voraussetzungen der Nutzung der LXT-Plattform und etwaige mit der Nutzung verbundenen Dienstleistungen und Kosten werden ausschließlich mit Ihrem Unternehmen, in dessen Auftrag wir Ihnen die persönliche Nutzung der LXT-Plattform ermöglichen, vereinbart. Für Sie persönlich fallen keine Kosten für die Nutzung der LXT-Plattform an.

### **§ 5 Gewährleistung, Supportleistungen**

Wir entwickeln unsere LXT-Plattform ständig weiter, weshalb sich ihre Funktionen – oder jeweils Teile davon – vorübergehend oder permanent ändern können. Sollten Sie eine zuvor bestehende Funktion vermissen, lassen Sie uns auch da am besten von einem für uns zuständigen Ansprechpartner aus Ihrem Unternehmen kontaktieren. Möglicherweise befindet sich die Funktion infolge einer Entwicklung woanders.



Unsere vertraglichen Leistungs- und Gewährleistungspflichten sind Gegenstand des Nutzungsvertrages mit Ihrem Unternehmen. Ihr Unternehmen hat gemäß dem zwischen uns bestehenden Nutzungsvertrages die Verpflichtung, etwaige auch bei Ihrer Nutzung der LXT-Plattform auftretenden Störungen oder Mängel unverzüglich uns gegenüber anzuzeigen. Bitte wenden Sie sich deshalb bei allen Störungen unverzüglich an den für uns in Ihrem Unternehmen zuständigen Ansprechpartner.

### **§ 6 Haftung**

Wir haften Ihnen gegenüber als unmittelbaren Nutzer der LXT-Plattform nur, soweit wir gesetzlich dazu verpflichtet sind. Soweit wir Ihnen gegenüber gesetzlich haften, haften wir uneingeschränkt für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit sowie für Schäden, die auf unser vorsätzliches oder grob fahrlässiges Handeln beruhen.

Bei leichter Fahrlässigkeit ist unsere Haftung nur auf typische und vorhersehbare Schäden, begrenzt.

Unsere Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

Im Fall des Datenverlustes haften wir nur für den typischen Wiederherstellungsaufwand, der bei regelmäßiger und gefahrenstprechender Anfertigung von Sicherungskopien eingetreten wäre.

### **§ 7 Datenschutz, Verarbeitung Ihrer personenbezogenen Daten im Auftrag**

Im Rahmen Ihrer Nutzung von LXT verarbeiten wir personenbezogenen Daten der Nutzer. Alle Details zu den Datenverarbeitungen und Ihren Rechten als Betroffene finden Sie in die auf unserer LXT-Plattform abrufbaren **Informationen zur Datenverarbeitung (IDV)**.

### **§ 8 Änderung der Nutzungsbedingungen**

Wir weisen darauf hin, dass sich die vorliegenden Bedingungen nachträglich u.a. im Zusammenhang mit Änderungen des mit Ihrem Unternehmen (unser Kunde) abgeschlossenen Nutzungsvertrages ändern können. In diesen Fällen erhalten Sie darüber eine Mitteilung. Die jeweils aktuellen Nutzungsbedingungen finden Sie dann ebenfalls abrufbar auf unserer LXT-Plattform.

## LXT

# Informationen zur Datenverarbeitung

Stand: 05.01.2021

### Information über die Erhebung personenbezogener Daten

Hier informieren wir über die Verarbeitung personenbezogener Daten bei der Nutzung unserer E-Learning-Plattform „LXT“ („die Plattform“). Verantwortlicher gem. Art. 4 Abs. 7 EU-Datenschutz-Grundverordnung (DSGVO) sind wir, „Bildungsinnovator“ (eLearning Manufaktur GmbH, alle Kontaktdaten sind im [Impressum](#) unserer [Website](#)).

### Teil 1: Daten bei jeder Nutzung der Plattform

#### 1. Browser-Daten

(1) Bei jeder Nutzung der Plattform, also unabhängig davon, ob Sie sie als Lernender, Autor, Administrator oder in einer sonstigen Funktion nutzen, erheben wir die personenbezogenen Daten, die Ihr Browser während der Nutzung der Plattform an unseren Server übermittelt. In diesen Fällen erheben wir die folgenden Daten, die für uns technisch erforderlich sind, um die Plattform verwendbar zu machen und die Stabilität und Sicherheit zu gewährleisten (Rechtsgrundlage ist Art. 6 Abs. 1 S. 1 lit. f DSGVO):

- IP-Adresse;
- Datum und Uhrzeit der Anfrage;
- Zeitzonendifferenz zur Greenwich Mean Time (GMT);
- Inhalt der Anforderung (konkrete Seite) ;
- Zugriffsstatus/HTTP-Statuscode;
- jeweils übertragene Datenmenge;
- Webseite, von der die Anforderung kommt (Referrer-URL);
- Browsertyp und -version;
- Sprache und Version der Browsersoftware;
- von Ihrem Endgerät genutztes Betriebssystem und dessen Oberfläche;
- übertragene Datenmenge;
- anfragender Telekommunikationsprovider.
- Dauer der Anfrage

(2) Wir löschen Server-Logs im Regelfall nach sieben Tagen, im Einzelfall auch später, wenn konkrete Anhaltspunkte uns den berechtigten Verdacht geben, dass die Plattform rechtswidrig genutzt wurde oder wird oder ein die Sicherheit oder Stabilität der Plattform gefährdendes Ereignis eingetreten ist. In einem Fall dieses Abs. 2 werden die Daten nach Ablauf von 90 Tagen ab dem Zeitpunkt gelöscht, an dem sie zur Aufklärung des vermutlich eingetretenen Ereignisses nicht mehr benötigt werden.

## 2. Cookies und Window.localStorage

- (1) Zusätzlich zu den zuvor genannten Daten werden bei Ihrer Nutzung der Plattform Cookies und Daten über die JavaScript-Funktion „Window.localStorage“ auf Ihrem genutzten Endgerät gespeichert. Die Plattform nutzt sowohl transiente und persistente Cookies, deren Umfang und Funktionsweise im Folgenden erläutert werden:
- (2) Zu den verwendeten **transienten Cookies** zählen insbesondere die Session-Cookies, die eine Session-ID speichern, mit der sich verschiedene Anfragen Ihres Browsers der gemeinsamen Sitzung zuordnen lassen. Dadurch kann Ihr Rechner wiedererkannt werden, wenn Sie auf die Plattform zurückkehren. Die Session-Cookies werden gelöscht, wenn Sie sich ausloggen oder den Browser schließen.

Es werden folgende transiente Cookies verwendet (zu den Details jedes Dienstes vgl. die Informationen im entsprechenden Kapitel):

### **JSESSIONID**

Inhalt:	Session ID
Zweck(e):	Erkennung und Zuordnung des Nutzers während seiner aktuellen Sitzung in der Plattform
Gesetzt von:	eLearning Manufaktur GmbH
Ablauf/Löschfrist	Session: Dieses Cookie wird beim Schließen des Browsers gelöscht.

### **org.springframework.web.servlet.i18n.CookieLocaleResolver.LOCALE**

Inhalt:	vom Nutzer aktuell ausgewählte Sprache
Zweck(e):	Generierung von PDFs in der vom Nutzer ausgewählten Sprache
Gesetzt von:	eLearning Manufaktur GmbH
Ablauf/Löschfrist	Session: Dieses Cookie wird beim Schließen des Browsers gelöscht.

### **contentLanguage**

Inhalt:	vom Nutzer als präferiert angegebene Sprache
Zweck(e):	Nutzung der Plattform in der vom Nutzer präferierten Sprache
Gesetzt von:	eLearning Manufaktur GmbH
Ablauf/Löschfrist	Session: Dieses Cookie wird beim Schließen des Browsers gelöscht.

### **contentLanguageSetByUserId**

Inhalt:	vom Nutzer gesetzte Sprache
Zweck(e):	Verwendung der Plattform in der vom Nutzer gewählten Sprache
Gesetzt von:	eLearning Manufaktur GmbH
Ablauf/Löschfrist	Session: Dieses Cookie wird beim Schließen des Browsers gelöscht.

- (3) Die **persistenten Cookies** werden automatisiert nach einer vorgegebenen Dauer gelöscht, die sich je nach Cookie unterscheiden kann. Sie können die Cookies in den Sicherheitseinstellungen Ihres Browsers jederzeit löschen. Es werden folgende persistente Cookies verwendet:

**\_pk\_id\***

Inhalt:	Setzt eine ID zur Erkennung des Users
Zweck(e):	Dient der Erkennung eines Users für Auswertungen die im Rahmen von Matomo möglich sind (siehe Punkt 3.)
Gesetzt von:	eLearning Manufaktur GmbH
Ablauf/Löschfrist	13 Monate

**\_pk\_ref\***

Inhalt:	Attributinformationen
Zweck(e):	interne Auswertung im Rahmen von Matomo (siehe Punkt 3)
Gesetzt von:	eLearning Manufaktur GmbH
Ablauf/Löschfrist	6 Monate

**\_pk\_ses\***

Inhalt:	Vorübergehende Daten eines Besuchs
Zweck(e):	Dient der internen Auswertung die im Rahmen von Matomo möglich sind (siehe Punkt 3.)
Gesetzt von:	eLearning Manufaktur GmbH
Ablauf/Löschfrist	30 Minuten

**SPRING\_SECURITY\_REMEMBER\_ME\_COOKIE**

Inhalt:	Status der Einstellung der „Angemeldet bleiben“-Funktion
Zweck(e):	Vermeidung unnötiger Logins, Komfort für den Nutzer
Gesetzt von:	eLearning Manufaktur GmbH
Ablauf/Löschfrist	30 Tage

- (4) Unter Nutzung der JavaScript-Technologie **„Window.localStorage“** werden weitere Datenkategorien gespeichert, um die Inhalte der Plattform der konkreten Nutzersituation anzupassen und die Nutzung komfortabler und/oder einfacher zu machen. Die Funktionen beinhalten insbesondere die folgenden Datenkategorien:
- Aktivierung/Nutzung der Funktion „Angemeldet bleiben“, mit der Neuanmeldung bei jedem Browser-Neustart vermieden werden kann;
  - Speicherung des Logins (genauer: der Authentifikation) des Nutzers, um ein Login bei Nutzung mehrerer Browser-Tabs und -Fenster nicht wiederholen zu müssen;
  - Speicherung der bereits absolvierten Teile der Hilfetour für Trainings, um Neulingen den Einstieg in die Plattformnutzung zu erleichtern, Hilfen aber nicht wiederholt anzuzeigen;

- Aktivierung/Nutzung des Bearbeitungsmodus in Trainings;
  - Verwaltung von in die Zwischenablage gelegten Inhalten, um Inhalte zwischen verschiedenen Browser-Reitern und -Fenstern austauschen und kopieren zu können.
- (5) Sie können Ihren Browser entsprechend Ihren Wünschen konfigurieren und die Annahme von Third-Party-Cookies ablehnen. Die Nutzung der Plattform ist ohne Verwendung jedweder Cookies und ohne die Verwendung von Window.localStorage nicht möglich.

### 3. Tracking des verwendeten Browsers via Matomo

- (1) Um nachvollziehen zu können, mit welchen Browsern die Plattform genutzt wird, protokollieren („tracken“) wir die Aufrufe der Einstiegsseite der Plattform durch alle Nutzer mit dem selbst auf unseren Servern gehosteten open-source-System „Matomo“ (<https://matomo.org/>, ehemals „Piwik“). Hierbei erheben wir IP-Adressen, die um die letzten drei Stellen gekürzt wurden. Matomo setzt für das genannte Tracking zu dem genannten Zweck sowohl transiente wie persistente Cookies. Rechtsgrundlage für diese Nutzung ist unser Interesse an einer möglichst fehlerfrei nutzbaren Plattform (Art. 6 Abs. 1 S. 1 lit. f DSGVO).
- (2) Sie können die Erhebung der aufgeführten Daten widersprechen, indem Sie die unten stehenden Link aufrufen. In diesem Fall wird in Ihrem Browser ein sog. Opt-Out-Cookie abgelegt, was zur Folge hat, dass Matomo keine Sitzungsdaten erhebt. Achtung: Wenn Sie das genannte Cookie oder all Ihre Cookies löschen, muss das genannte Cookie erneut von Ihnen gesetzt werden.

<https://piwik.elearning-manufaktur.com/index.php?module=CoreAdminHome&action=optOut&language=de>

Die über Matomo erhobenen Daten werden nicht routinemäßig gelöscht.

### 4. Kontaktaufnahme

Sollten Sie uns direkt kontaktieren (z. B. über die E-Mail-Adresse [support@bildungsinnovator.com](mailto:support@bildungsinnovator.com)), werden die von Ihnen mitgeteilten Daten (z. B. Ihr Name, Ihre E-Mail-Adresse und weitere Daten wie Ihre Telefonnummer) von uns verarbeitet, um Ihr Anliegen zu behandeln. Rechtsgrundlage dieser Verarbeitung ist die Notwendigkeit zur Erfüllung Ihrer Anfrage gem. Art. 6 Abs. 1 S. 1 lit. b DSGVO. Je nach Anfrage müssen wir Ihre Daten für eine gewisse Zeit speichern, um unserer Rechenschaftspflicht nachkommen zu können; Rechtsgrundlage dieser Speicherung ist Art. 6 Abs. 1 S. 1 lit. c DSGVO.

### 5. Kategorien erhobener personenbezogener Daten unabhängig von Nutzerrechten

Bei der Nutzung der Plattform werden die folgenden Datenkategorien über alle Nutzer unabhängig von der Nutzerrolle bzw. den gewährten Nutzerrechten (also vor allem über lernende Nutzer) verarbeitet:

- Zeitpunkt jedes einzelnen **Logins und Login-Versuches**;
- **Berechtigungen** Ihres Nutzerkontos und deren Veränderungen inkl. Zeitstempel;

- **Lernfortschrittsdaten**
  - i. **Aufrufe von Inhalten** („Karten“): Bezeichnung der Karte, Zeitstempel des Aufrufes und Ihre Nutzer-ID;
  - ii. **all Ihre Antworten auf Quizfragen**: wann Sie welche Frage(n) beantwortet haben und ob die jeweilige Antwort richtig oder falsch war;
  - iii. **Antworten im Rahmen von Quizkolektionen**: von Ihnen gegebene Antworten, im Rahmen der Quizkolektion erreichte Punkte sowie die für die Bewältigung der gesamten Quizkolektion benötigte Zeit;
  - iv. von Ihnen **erlangte Zertifikate**.
- die von Ihnen angelegten **Lesezeichen**;
- **Ihre Bewertungen** von Karten, ggf. inkl. Bewertungstext;
- von Ihnen mit anderen und von anderen mit Ihnen geteilte Karten inkl. Zeitstempel des Teilens;
- **an Sie und von Ihnen delegierte Aufgaben** inkl. Zeitangabe des jeweiligen Delegierens und ggf. Kommentaren zu jeder Aufgabe;
- **von Ihnen an Experten gestellte Fragen**.

## 6. **Kategorien erhobener personenbezogener Daten abhängig von der Nutzerrolle bzw. den Nutzerrechten**

Die folgenden zusätzlichen Kategorien personenbezogener Daten werden in der Plattform abhängig von der jeweiligen Nutzerrolle bzw. den einem Nutzer gewährten Rechten verarbeitet:

<b>Gewährtes Recht</b>	<b>Verarbeitete Datenkategorien</b>	<b>Einsichtsberechtigte Nutzer</b>
„Aufgabenverwaltung benutzen“	welche Aufgaben wann von welchem Nutzer welchem Nutzer delegiert wurden	Nutzer mit dem Recht „Aufgabenverwaltung benutzen“.
„Inhaltsberechtigungen setzen“	welcher Nutzer wann Berechtigungen für welchen Inhalt oder entfernt hat	Bildungsinnovator-Administratoren
„Reporting einsehen“	welcher Nutzer wann Reports mit welchen Parametern erstellt/heruntergeladen hat	Bildungsinnovator-Administratoren
„Papierkorb benutzen“	welche Inhalte wann von welchem Nutzer gelöscht wurden	alle Nutzer einer Installation
„Erstelle, aktualisiere, lösche Benutzer/ Benutzergruppen/ Rollen“	jede Änderung einer Nutzerberechtigung	Bildungsinnovator-Administratoren
„Vorlagen benutzen“	welcher Nutzer wann welche Vorlage angelegt hat	Jeder Nutzer mit „Vorlagen benutzen“.
„Inhaltsberechtigungen setzen“	Jede Änderung von Inhaltsberechtigungen wird protokolliert.	Bildungsinnovator-Administratoren
„Skillsets verwalten“	berechtigungsrelevante Änderungen (Hinzufügen von Kollektionen oder Benutzergruppen zu einem Skillset)	Bildungsinnovator-Administratoren

## **Teil 2: Welche Nutzer welche Daten einsehen können**

In diesem Abschnitt erklären wir Ihnen, welche anderen Nutzer in der Plattform auf welche Ihrer Daten zugreifen können. Da die technischen Administratoren der Installation auf alle personenbezogenen Daten zugreifen können (und das zur Sicherstellung der fehlerfreien Funktion der Plattform auch müssen), wird hierauf nicht weiter eingegangen.

### **1. Ihre Antworten auf Quizfragen**

Nutzer mit Zugriff auf die Benutzerverwaltung können sehen, ob Sie eine bestimmte Frage wahr oder falsch beantwortet haben, außerdem den Zeitstempel Ihrer ersten und Ihrer letzten Antwort auf diese Frage.

### **2. Ihre erlangten Zertifikate**

Nutzer mit der Berechtigung „Reporting einsehen“ können einsehen, welche Zertifikate Sie wann erlangt haben.

### **3. Wer Sie wann innerhalb der Plattform finden kann**

- Beliebige andere Lernende können Ihren Namen und Ihre E-Mail-Adresse finden, wenn sie eine jemand anderem eine Lernkarte teilen wollen, indem sie die ersten drei Anfangsbuchstaben Ihres Vor- oder Nachnamens eintippen.
- Nutzer mit der Berechtigung „Aufgabenverwaltung benutzen“ können die in lit. a genannte Suchfunktion außerdem nutzen, wenn sie anderen Nutzern Aufgaben zuweisen (delegieren).

### **4. Sie als Experte/Expertin**

Wenn Ihnen als Experte/Expertin eine Frage gestellt wird, ist Ihr Name im Zusammenhang mit der/den an Sie gestellte(n) Frage(n) von allen Nutzern sichtbar, sobald Sie auf die jeweilige Frage antworten. Im Gegensatz zu Lernenden, die Ihnen anonym Fragen stellen können, können Sie als Experte/Expertin nicht anonym antworten.



### **Teil 3: Speicherfristen und Ihre Rechte**

- 1.** Wenn und soweit nicht anders beschrieben, werden die in diesem Dokument genannten Datenkategorien grundsätzlich bis zur Löschung der Plattform gespeichert. Sie haben jedoch selbstverständlich das Recht auf Löschung nach Maßgabe der folgenden Hinweise.
- 2.** Unabhängig davon, wie Sie die Plattform verwenden, haben Sie als betroffene Person gegenüber uns folgende Rechte hinsichtlich der Sie betreffenden personenbezogenen Daten:
  - Recht auf Auskunft;
  - Recht auf Berichtigung oder Löschung;
  - Recht auf Einschränkung der Verarbeitung;
  - Recht auf Widerspruch gegen die Verarbeitung;
  - Recht auf Datenübertragbarkeit.
- 3.** Sie haben zudem das Recht, sich bei einer Datenschutz-Aufsichtsbehörde über die Verarbeitung Ihrer personenbezogenen Daten durch uns zu beschweren. Bevor Sie das tun, empfehlen wir jedoch, Kontakt mit uns aufzunehmen.
- 4.** Unsere Datenschutzbeauftragte erreichen Sie unter den folgenden Kontaktdaten:

Innara UG (haftungsbeschränkt) & Co. KG  
Frank Stiegler  
Martin-May-Straße 10  
60594 Frankfurt

Telefon: +49 69 6642699-00

Fax: +49 69 6642699-09

E-Mail: [datenschutz@bildungsinnovator.de](mailto:datenschutz@bildungsinnovator.de) ([Public PGP Key](#), [S/MIME-Zertifikat](#))

## Anlage 4: Vertrag über Auftragsverarbeitung iSd. Art. 28 Abs. 3 DSGVO

(Stand: 23.04.2021)

### Präambel

Diese Anlage inklusive ihrer Anhänge konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den vertragsgemäßen Leistungen der Auftragnehmerin (BI – eLearning Manufaktur GmbH) für den Auftraggeber (Kunde) im Rahmen der Bereitstellung der Plattform „LXT“ (ehemals „Lernkarten“) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit diesem Zweck im Zusammenhang stehen und bei denen Beschäftigte der Auftragnehmerin oder durch die Auftragnehmerin Beauftragte personenbezogene Daten („Daten“) des Auftraggebers verarbeiten. Die vorliegende Vereinbarung ersetzt eventuelle vorherige Vereinbarungen zum Datenschutz zwischen den Vertragsparteien.

**Wenn bzw. soweit zwischen den Parteien zuvor ein Vertrag über Auftragsdatenverarbeitung nach § 11 BDSG in der bis zum 24.05.2018 gültigen Fassung geschlossen wurde, wird der besagte Vertrag durch den vorliegenden ersetzt.**

Überschriften in diesem Dokument dienen nur der Orientierung.

### § 1 Gegenstand und Dauer der Auftragsverarbeitung

- (1) Aus dem Hauptvertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art und Zweck der Datenverarbeitung	inkludierte Datenkategorien	Kategorien Betroffener
Betrieb der Plattform „LXT“ als Cloud-Plattform	<ul style="list-style-type: none"> <li>• Stammdaten der Nutzer: Name, E-Mail-Adresse</li> <li>• Account-Daten der Nutzer: Rollen, Berechtigungen, Benutzernamen, Hierarchien, Logins (Login-Zeitpunkte und -Dauer)</li> <li>• Lernstandsdaten: absolvierte Inhalte, Testergebnisse/ Abschlussnoten</li> <li>• Kommunikationsdaten: E-Mails, Chats (Metadaten wie Inhalte)</li> </ul>	<ul style="list-style-type: none"> <li>• Mitarbeiter des Auftraggebers</li> <li>• Nutzer der Plattform</li> <li>• Administratoren der Auftragnehmerin</li> </ul>

Support-Leistungen der Auftragnehmerin auf Weisung des Auftraggebers	beliebige nach Vorgabe des Auftraggebers, voraussichtlich regelmäßig Kontakt- und Lernfortschrittsdaten	beliebige nach Vorgabe des Auftraggebers, voraussichtlich regelmäßig Mitarbeiter des Auftraggebers und LXT-Nutzer
--	---	---

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

- (2) Die vertraglich vereinbarten Datenverarbeitungen finden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Wenn bzw. soweit hiervon abgewichen werden soll, müssen die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sein, und dem Auftraggeber ist die jeweilige Änderung mindestens 30 (dreißig) Tage vorher anzukündigen.

## § 2 Verantwortlichkeit des Auftraggebers

- (1) Die Auftragnehmerin verarbeitet personenbezogene Daten im Auftrag des Auftraggebers gem. Art. 28 DSGVO. Der Auftraggeber ist alleiniger Verantwortlicher iSd. Art. 4 Nr. 7 DSGVO.
- (2) Die im Rahmen der Auftragsverarbeitung für die Tätigkeit der Auftragnehmerin erforderlichen Weisungen werden vom Auftraggeber anfänglich durch den Vertrag festgelegt und können von ihm danach in Textform an die von der Auftragnehmerin bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden („Einzelweisung“). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

## § 3 Pflichten der Auftragnehmerin

- (1) **Weisungsgetreue Verarbeitung**  
Die Auftragnehmerin darf Daten betroffener Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, es sei denn, es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 lit. a) DSGVO vor. Die Auftragnehmerin informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder geändert wurde.
- (2) **Ergreifung technischer und organisatorischer Maßnahmen (“TOM“)**  
Die Auftragnehmerin wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie wird TOM zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Art. 24, 32, 5 DSGVO genügen. Die Auftragnehmerin darf die TOM laufend fortentwickeln, auch um dem technischen Fortschritt Rechnung tragen zu können. Sie darf insoweit alternative adäquate Maßnahmen ergreifen, solange das Schutzniveau der in Anhang 1 zu dieser Anlage festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

- (3) **Unterstützung des Auftraggebers bei der Umsetzung von Betroffenenrechten**  
Die Auftragnehmerin unterstützt den Auftraggeber im angemessenen Umfang bei der Erfüllung der Anfragen und Ansprüche Betroffener gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO verpflichtet sich die Auftragnehmerin, den Auftraggeber bei der Abwehr des Anspruches im angemessenen Umfang zu unterstützen.
- (4) **Verpflichtung aller Daten verarbeitender Person**  
Die Auftragnehmerin setzt gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO im Rahmen ihrer Vertragserfüllung nur Personen ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Auftragnehmerin und jede ihr unterstellte Person mit Zugang zu personenbezogenen Daten 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) **Unterrichtung bei Datenschutzverletzungen**  
Die Auftragnehmerin unterrichtet den Auftraggeber unverzüglich, wenn ihr Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Sie trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
- (6) **Hinweis über Maßnahmen der Aufsichtsbehörde**  
Die Auftragnehmerin informiert den Auftraggeber über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf die vertragsgegenständlichen Leistungen beziehen, und stimmt Vorgehen mit ihm ab. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die auftragsverarbeitungsgemäße Verarbeitung personenbezogener Daten bei der Auftragnehmerin ermittelt.
- (7) **Compliance-Prüfungsverfahren**  
Die Auftragnehmerin kontrolliert regelmäßig die internen Prozesse und ihre TOM, um deren Einklang mit den Anforderungen des geltenden Datenschutzrechts zu gewährleisten.
- (8) **Herausgabe/Löschung von Daten nach Auftragsende**  
Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.
- (9) **Einrede des Zurückbehaltungsrechts ausgeschlossen**  
Die Einrede des Zurückbehaltungsrechts iSd. § 273 BGB wird hinsichtlich der im Rahmen dieser Vereinbarung von der Auftragnehmerin verarbeiteten personenbezogenen Daten ausgeschlossen.
- (10) **Datenschutzbeauftragte**  
Die Auftragsverarbeiterin hat die Innara UG & Co. KG, Martin-May-Straße 10, 60594 Frankfurt, dort Herrn Frank Stiegler (Fon: +49 69 664269911, E-Mail: [datenschutz@bildungsinnovator.com](mailto:datenschutz@bildungsinnovator.com)) zur externen Datenschutzbeauftragten bestellt.

#### **§ 4 Pflichten des Auftraggebers**

**(1) Hinweis bei Fehlern**

Der Auftraggeber hat die Auftragnehmerin unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

**(2) Unterstützung der Auftraggeberin bei der Umsetzung von Betroffenenrechten**

Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO gilt § 3 Abs. 3 S. 2 dieses Vertrages entsprechend.

**(3) Vergütung der Datenschutzleistungen der Auftragnehmerin**

Der Auftraggeber hat der Auftragnehmerin die im Rahmen dieser Vereinbarung über Auftragsverarbeitung entstehenden Tätigkeiten nach den vereinbarten, ansonsten nach üblichen Sätzen zu vergüten, soweit sie individuell für den Auftraggeber erbracht und nicht wegen eines schuldhaften Verstoßes der Auftragnehmerin gegen ihre Pflichten aus dieser Vereinbarung erforderlich werden. Zu den Tätigkeiten nach diesem S. 1 zählen insbesondere die Durchführung von bzw. Mitwirkung bei folgenden Aktivitäten:

- a) Audits seitens des Auftraggebers bei der Auftragnehmerin, wenn bzw. soweit dabei keine erheblichen Datenschutzverstöße festgestellt werden;
- b) Anfragen Betroffener sowohl bei der Auftragnehmerin direkt wie auch beim Auftraggeber, wenn und soweit die Auftragnehmerin hierbei mitwirkt;
- c) vom Auftraggeber gewünschte Einschränkung, Löschung usw. von Daten, soweit es ihm mit der von der Auftragnehmerin zur Verfügung gestellten Lösung technisch unmöglich ist, die gewünschte Datenverarbeitung selbst vorzunehmen;
- d) vom Auftraggeber gewünschte Mitwirkung bei Datenschutzfolgenabschätzungen;
- e) Hinweise an den Auftraggeber, die durch rechtswidrige datenschutzrechtliche Weisungen des Auftraggebers ausgelöst werden;
- f) Mitwirkungen der Auftragnehmerin (inkl. Betriebsablaufstörungen bei ihm), die durch Durchsuchungen öffentlicher Stellen bei ihr bzgl. Daten des Auftraggebers nötig werden;
- g) Mitwirkung bei Meldungen des Auftraggebers nach Art. 33 DSGVO und bei Benachrichtigungen Betroffener nach Art. 34 DSGVO, wenn bzw. soweit die Auftragnehmerin den Grund der Melde- bzw. Benachrichtigungspflicht nicht schuldhaft verursacht hat.

#### **§ 5 Qualitätssicherung**

**(1) Die Auftragnehmerin weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten durch folgende Unterlagen nach:**

- a) schriftliche Bestellung des/der Datenschutzbeauftragten, die/der ihre/seine Tätigkeiten nach Art. 38, 39 DSGVO nachweist;
- b) Vorlage der Vertraulichkeitsvereinbarung gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO;

- c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- d) geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach TISAX).

(2) **Datenschutzaudits**

Wenn und soweit die Auftragnehmerin die Einhaltung der nach dieser Vereinbarung zu ergreifenden Maßnahmen nicht nach diesem Abs. 1 nachweisen kann, hat der Auftraggeber das Recht, sich im Benehmen mit der Auftragnehmerin durch Kontrollen von der Ergreifung der nach dieser Vereinbarung von der Auftragnehmerin zu ergreifenden TOM in deren Geschäftsbetrieb zu überzeugen. Die Auftragnehmerin darf die hierfür erforderlichen Prüfungen in der Regel von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden abhängig machen. Wenn bzw. soweit diese Kontrollen dem Auftraggeber keine personenbezogenen Daten und keine von der Auftragnehmerin aus einem anderen Grund vertraulich zu behandelnden Daten anderer Geschäftspartner der Auftragnehmerin zur Kenntnis gelangen lassen können, darf der Auftraggeber die jeweilige Kontrollmaßnahme selbst durchführen. Soweit die Kontrolle Daten verarbeitet, die nicht zum Bereich der Auftragsdaten des Auftraggebers gehören, hat er sie von einem standesrechtlich zur Verschwiegenheit verpflichteten Dritten, z. B. einem Rechtsanwalt oder Wirtschaftsprüfer durchführen zu lassen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zur Auftragnehmerin oder zu einem oder mehreren ihrer Kunden stehen oder kein diesem Vertrag entsprechendes Datenschutz- und IT-Sicherheitsniveau nachweisen können, darf die Auftragnehmerin diesen Prüfer ablehnen, und der Auftraggeber hat einen anderen Prüfer zu wählen, bei dem die genannten Voraussetzungen nicht vorliegen.

**§ 6 Unterauftragsverhältnisse**

- (1) Die Auftragnehmerin setzt Unternehmern zur Erbringung auch von (Teil-)Leistungen („Subunternehmer“) ein. Subunternehmer gelten als „Unterauftragsverarbeiter“, wenn/soweit sie personenbezogene Daten im Auftrag der Auftragnehmerin verarbeiten, nicht jedoch, wenn sie anlässlich ihrer gegenüber der Auftragnehmerin erbrachten Leistungen
- a) personenbezogene Daten lediglich als Nebenleistung bei der Sicherstellung von Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von **Datenverarbeitungsanlagen** verarbeiten (z. B. bei Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartungs- oder Benutzer-Support-Leistungen) oder
  - b) lediglich Möglichkeit des Zugriffs auf personenbezogene Daten des Auftraggebers haben, sich aber **vertraglich verpflichtet haben, keinen solchen Zugriff zu nehmen** (z. B. Provider von Rechenzentrumsfläche und Begleitleistungen wie Schutz vor Elementarschäden und dauerhafte Stromversorgung).

Subunternehmer, die nach dieser Regelung keine Unterauftragsverarbeiter sind, werden in diesem Dokument als „Zulieferer“ bezeichnet.

- (2) Die Auftragnehmerin darf Zulieferer nach eigenem freiem Ermessen beauftragen, ersetzen und Verträge mit ihnen kündigen, solange die Pflichten der Auftragnehmerin nach diesem Vertrag erfüllt sind. Sie hat dem Auftraggeber eine Liste eingesetzter Zulieferer auf dessen Wunsch vorzulegen.
- (3) **Die Auftragnehmerin darf Unterauftragsverarbeiter nur nach vorheriger ausdrücklicher dokumentierter Zustimmung des Auftraggebers beauftragen.** Die Zustimmung zur Beauftragung der in Anhang 2 zu dieser Anlage aufgeführten Unterauftragsverarbeiter erteilt der Auftraggeber im Rahmen des Abschlusses dieses Vertrages. Jeder Wechsel eines Unterauftragsverarbeiters unterliegt der vorherigen dokumentierten Zustimmung des Auftraggebers, die er jedoch nicht ohne erheblichen datenschutzrechtlichen Grund verweigern darf.
- (4) Unabhängig davon, ob ein Subunternehmer Unterauftragsverarbeiter ist, hat die Auftragnehmerin den angemessenen Schutz und die angemessene Sicherheit der verarbeiteten Daten des Auftraggebers durch vertragliche Vereinbarungen und wirksame Kontrollmaßnahmen sicherzustellen.

## § 7 Informationspflichten, Schriftformklausel, Rechtswahl

- (1) Sollten die Daten des Auftraggebers bei der Auftragnehmerin durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, hat die Auftragnehmerin den Auftraggeber unverzüglich darüber zu informieren. Die Auftragnehmerin wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten ausschließlich beim Auftraggeber als verantwortlicher Stelle iSd. DSGVO liegen.
- (2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen der Auftragnehmerin – bedürfen der Textform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (3) Bei etwaigen Widersprüchen gehen Regelungen zum Datenschutz in dieser Anlage den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

### Anhänge zu diesem Dokument:

- Anhang 1: Liste ergriffener technischer und organisatorischer Maßnahmen  
Anhang 2: Liste eingesetzter Unterauftragsverarbeiter  
Anhang 3: Liste beim RZ-Betreiber IPB Internet Provider in Berlin GmbH ergriffener technischer und organisatorischer Maßnahmen

## Anhang 1

### Technische und organisatorische Maßnahmen

gem. Art. 24, 32 DSGVO (Stand: 23.04.2021)

Die in diesem Dokument aufgeführten Maßnahmen werden von der Auftragnehmerin bei der Erbringung ihrer vertraglichen Tätigkeiten für den Auftraggeber zum Schutz von Daten („Daten“ meint auch in diesem Anhang personenbezogene Daten gem. Art. 4 Nr. 1 DSGVO) ergriffen.

Die Auftragnehmerin ist unabhängig von den hier beschriebenen Maßnahmen nach dem TISAX-Standard (einem Standard zum Nachweis von IT-Sicherheitsmaßnahmen) zertifiziert, ergreift also weitere Informationssicherheitsmaßnahmen, die auf Wunsch des Auftraggebers zur Verfügung gestellt werden.

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

### Überblick zu Maßnahmen der Zutritts-, Zugangs- und Zugriffskontrolle

Es existieren drei verschiedene Arten von Datenverarbeitungsanlagen:

- (ein oder mehrere) Server in einem oder mehreren Rechenzentren („RZ“) („der Server“);
- „mobile Endgeräte“ der Auftragnehmerin, also Endgeräte mit einem mobilen Betriebssystem (z. B. iOS und Android);
- „stationäre Endgeräte“ der Auftragnehmerin, also alle Endgeräte, die keine mobilen Endgeräte sind.

### Standortsituation Server Heinlein Support GmbH („Heinlein“)

Ein oder mehrere Server, auf denen LXT-Installationen betrieben werden, werden von der Subunternehmerin Heinlein Support GmbH („Heinlein“), ihrerseits unter Nutzung der Subunternehmerinnen IPB Internet Provider Berlin GmbH („IPB“) bereitgestellt. Die beiden zuletzt genannten RZ-Betreiber sind ISO 27001-zertifiziert.

Heinlein verarbeitet hierbei Daten nicht primär im Auftrag, sondern stellt vorrangig Hardware und RZ-Kapazitäten (gegen Elementarschäden geschützter Standort mit unterbrechungsfreier Stromversorgung und solider Internetverbindung) und begleitende Dienstleistungen bereit, tauscht z. B. defekte Festplatten, sorgt für erforderliche Server-Neustarts u. Ä..

Die von Heinlein hierbei genutzten RZ befinden sich in Berlin.

### Standortsituation Server Amazon Web Services, Inc. („AWS“)

Prinzipiell ähnlich wie Heinlein/IPB stellt AWS Serverkapazitäten zur Verfügung, auf denen LXT-Installationen betrieben werden, die ebenfalls ISO 27001-zertifiziert sind.



## Standortsituation Niederlassung Düsseldorf

Die Büroräume in Düsseldorf befindet sich im 2. Stock des „Factory Campus“ an der Erkrather Straße 401 in Düsseldorf, einem umzäunten und mit Bewegungsmelder-gesteuerter Beleuchtung versehenen Gebäudekomplex, in dem sich Büros verschiedener Unternehmen befinden, u. a. der Auftragnehmerin. Die meisten Fenster und Nebentüren des Gebäudes im Erdgeschoss sind mit Rollläden versehen, die außerhalb der Bürozeiten manuell heruntergelassen werden. Das Gebäude ist außerhalb der üblichen Bürozeiten verschlossen und während der üblichen Bürozeiten über einen Hauseingangsschlüssel betretbar, der Mitarbeitern aller Unternehmen im Factory Campus ausgehändigt wird, der über die Hauseingänge hinaus keine Türen öffnet. Das Gebäude wird an verschiedenen Stellen (Flure, Eingangshalle, Gesellschaftsräume) videoüberwacht. Die Büroräume der Auftragnehmerin sind nur über Transponder betretbar, die nur Mitarbeitern der Auftragnehmerin ausgehändigt werden. Nicht begleitete Besucher müssen sich am zentralen Empfang des Factory Campus anmelden, an den sie gelangen können, wenn sie am Eingang klingeln und der Empfang ihnen Zutritt gewährt. Besucher müssen, um Zutritt zu Büroräumen der Auftragnehmerin zu erhalten, von Mitarbeitern der Auftragnehmerin am Empfang abgeholt werden.

## Standortsituation Niederlassung Kleve

Die Büroräume der Klever Niederlassung befindet sich in einem Gebäude an der Schloßtorstraße 39 in Kleve, in dem sich nur die Büroräume der Auftragnehmerin befinden. Das Grundstück ist umzäunt, und das Gebäude ist außerhalb üblicher Arbeitszeiten verschlossen und mit einer Alarmanlage gesichert, die an verschiedene Bewegungsmelder im Gebäude gekoppelt ist und Alarm an ein externes Sicherheitsunternehmen meldet. Bewegungsmelder an der Außenseite des Gebäudes steuern außerhalb üblicher Arbeitszeiten Licht am Gebäude. Die meisten Fenster und Nebentüren des Gebäudes im Erdgeschoss sind mit Rollläden versehen, die außerhalb der Bürozeiten manuell heruntergelassen werden. Während üblicher Arbeitszeiten ist das Gebäude mit einem elektrischen Türöffner betretbar, der nur den am Standort Kleve tätigen Mitarbeitern der Auftragnehmerin sowie der Geschäftsführung und, soweit vorhanden, Prokuristen ausgehändigt wird.

### 1.1. Zutrittskontrolle

**Ziel:** Verarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sind gegen Zutritt durch Unbefugte zu sichern.

**Ergriffene Maßnahmen im RZ:**

<b>Situation bei IPB</b>
Dieser RZ-Betreiber ist ISO 27001-zertifiziert; das Zertifikat ist unter <a href="https://www.ipb.de/company/certifications.html">https://www.ipb.de/company/certifications.html</a> ) abrufbar. Der RZ-Betreiber ergreift TOM nach Maßgabe des als Anhang 3 beigefügten Dokumentes.
<b>Situation bei AWS</b>
Es werden Maßnahmen nach Maßgabe der ISO 27001-Zertifizierung (abrufbar unter <a href="https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf">https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf</a> ) ergriffen.

**Ergriffene Maßnahmen in der Niederlassung Düsseldorf:**

Bereich	Situation
Grundstück	<ul style="list-style-type: none"> <li>• umzäuntes Gelände</li> <li>• Bewegungsmelder-gesteuerte Beleuchtung auf dem Grundstück</li> </ul>
Gebäude	<ul style="list-style-type: none"> <li>• Fenster und Nebentüren des Gebäudes sind außerhalb der Bürozeiten rollladengesichert.</li> <li>• Gebäudetüren sind außerhalb der Bürozeiten verschlossen. Die entsprechenden Schlüssel, die über die Hauseingänge hinaus keine Türen öffnen, werden Mitarbeitern aller Unternehmen im Factory Campus ausgehändigt.</li> </ul>
Für Mitarbeiter aller Unternehmen im Gebäude zugängliche Flächen	<ul style="list-style-type: none"> <li>• Das Gebäude wird an verschiedenen Stellen (Flure, Eingangshalle, Gesellschaftsräume) videoüberwacht.</li> <li>• Ein zentraler Empfang ist als erster Kontaktpunkt für alle Besucher eingerichtet.</li> </ul>
Büroräume der Auftragnehmerin	<ul style="list-style-type: none"> <li>• Büroräume sind nur über Transponder betretbar, die nur Mitarbeitern der Auftragnehmerin ausgehändigt werden.</li> <li>• Besucher müssen, um Zutritt zu Büroräumen der Auftragnehmerin zu erhalten, von Mitarbeitern der Auftragnehmerin am Empfang abgeholt werden.</li> </ul>

## 1.2. Zugangskontrolle

**Ziel:** Oben genannte Verarbeitungsanlagen sind gegen die unbefugte Nutzung zu sichern.

### Ergriffene Maßnahmen im RZ:

<b>Situation bei IPB (Subunternehmer von Heinlein)</b>
Alle Admin-Zugriffe werden durch personenscharfe SSH-Schlüssel gesichert und sind nur von bestimmten IP-Adressen aus möglich.
<b>Situation bei AWS</b>
Alle Admin-Zugriffe werden durch personenscharfe SSH-Schlüssel gesichert und sind nur von bestimmten IP-Adressen aus möglich.

### Ergriffene Maßnahmen in den Niederlassungen:

Bereich	Situation
stationäre Endgeräte	<ul style="list-style-type: none"> <li>• Festplattenverschlüsselung</li> <li>• Alle Mitarbeiter und Erfüllungsgehilfen der Auftragnehmerin müssen sich über eine personenscharfe Authentifizierung (SSH mit asymmetrischer Verschlüsselung) an jedem Server anmelden, bevor sie auf jedwede Daten zugreifen können.</li> <li>• Authentifizierungsdaten müssen dem aktuellen Stand der Technik entsprechend komplex sein.</li> <li>• Die Betriebssysteme der eingesetzten Endgeräte werden auf dem aktuellen Sicherheitsupdate-Stand gehalten.</li> <li>• Firewall-Einsatz</li> <li>• Sperre virtueller Arbeitsplätze nach Abwesenheit des jeweiligen Nutzers von mindestens 5 Minuten</li> </ul>
mobile Endgeräte	<ul style="list-style-type: none"> <li>• Auf mobilen Endgeräten werden mit Ausnahme von eventuell vom Auftraggeber via E-Mail zugesendeten Daten keine Daten gespeichert.</li> <li>• Mobile Endgeräte werden nicht für Logins auf Servern verwendet.</li> <li>• Die Betriebssysteme der eingesetzten Endgeräte werden auf dem aktuellen Sicherheitsupdate-Stand gehalten.</li> </ul>
externe Datenträger	<ul style="list-style-type: none"> <li>• Externe Datenträger dürfen nicht zur Speicherung von Daten verwendet werden.</li> </ul>
Papierunterlagen	<ul style="list-style-type: none"> <li>• Daten enthaltende Papierunterlagen werden in einem verschlossenen Metallbehälter aufbewahrt und vor bzw. bei ihrer Entsorgung DIN 66399-Klasse-3-konform gelöscht und/oder vernichtet.</li> </ul>

Datenträger	<ul style="list-style-type: none"> <li>• Datenträger werden vor oder bei ihrer Entsorgung DIN 66399-Klasse-3-konform gelöscht und/oder vernichtet.</li> <li>• Vor der Wiederverwendung eines Datenträgers für einen anderen Zweck werden die darauf befindlichen Daten via Secure Erase gelöscht und überschrieben.</li> </ul>
Netzwerke (LAN, WLAN)	<ul style="list-style-type: none"> <li>• In der Niederlassung in Düsseldorf werden ein selbst verwaltetes LAN und ein selbst verwaltetes passwortgeschütztes WLAN genutzt.</li> <li>• In der Niederlassung Kleve werden ein LAN-Netzwerk und zwei getrennte, passwortgeschützte, verschlüsselte WLANs genutzt, eins für Unternehmenszwecke und eins für Besucher und Gäste. Alle hier genannten Netzwerke sind nur der Auftragnehmerin zugänglich.</li> </ul>
Sonstiges	<ul style="list-style-type: none"> <li>• Daten in der Plattform werden grundsätzlich und primär auf dem Server verarbeitet. Auf stationären oder mobilen Endgeräten werden sie grundsätzlich nur temporär verarbeitet, solange es für konkrete Auftragstätigkeiten erforderlich ist.</li> <li>• Ausnahmen zu dem zuvor genannten Grundsatz bilden zwei Fälle: <ol style="list-style-type: none"> <li>1. Der Auftraggeber sendet Daten an die Auftragnehmerin via E-Mail.</li> <li>2. Fehlerbehebungs- oder Support-Zwecke erfordern Änderungen der Kundendatenbank, in der sämtliche Nutzerdaten des Auftraggebers gespeichert werden. Dann kopiert der jeweilige Mitarbeiter der Auftragnehmerin die besagte Datenbank auf seinen verwendeten Rechner und lässt sie dort bis auf weitere Weisung des Auftraggebers gespeichert, um Anschlussfragen beantworten zu können. Der Auftraggeber kann jederzeit zur Löschung auffordern.</li> </ol> </li> <li>• Es existiert eine unternehmensweite Clean Desk-Policy, nach der Datenträger und alle Daten enthaltenden Dokumente vor unberechtigtem Zugang geschützt werden, sowohl in analoger (z. B. über verschließbare Schränke) wie digitaler (z. B. über Desktop-Sperranweisung und -funktion bei Nichtnutzung) Form.</li> </ul>

### 1.3. Zugriffskontrolle

**Ziel:** 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, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

**Situation:**

Je nach Erforderlichkeit für die jeweilige Tätigkeit haben Mitarbeiter der Auftragnehmerin (z. B. Administratoren, Autoren und Trainer) Zugriff auf Daten. Seitens der Auftragnehmerin werden die folgend beschriebenen Maßnahmen ergriffen. Die seitens des Auftraggebers ergriffenen bzw. zu ergreifenden Maßnahmen liegen in seiner Verantwortlichkeit.

**Ergriffene Maßnahmen:**

Bereich	Situation
Zugriffsrechtevergabe (Rechte-/Rollenkonzept)	<ul style="list-style-type: none"> <li>Nutzer können und dürfen auf Daten nur über personenscharfe Konten zugreifen.</li> <li>Berechtigungen werden abhängig von der Erforderlichkeit des jeweiligen Zugriffes vergeben. Zugriffsberechtigungen aller zur Auftragserfüllung tätigen Personen der Auftragnehmerin orientieren sich am <i>principle of least privilege</i> und werden turnusmäßig kontrolliert und sich verändernden Situationen (Vergabe von Rechten an neue Mitarbeiter, Löschung/Sperrung von Rechten ausscheidender Mitarbeiter und Anpassung von Rechten von Mitarbeitern mit veränderten Aufgabenprofilen) unverzüglich angepasst.</li> </ul>
Protokollierung der Zugriffe	<ul style="list-style-type: none"> <li>Alle Lese- und Schreibzugriffe auf Daten werden nutzerscharf protokolliert.</li> </ul>

### 1.4. Trennungskontrolle

**Ziel:** Es ist sicher zu stellen, dass zu unterschiedlichen Zwecken erhobene Daten (logisch oder physisch) getrennt verarbeitet werden können.

**Ergriffene Maßnahmen:**

Bereich	Situation
Trennung von Daten anderer Auftraggeber	Datenbank und Dateien werden entsprechend der Weisung des Auftraggebers in getrennten Verzeichnissen oder Servern mit separaten Berechtigungen gespeichert.

Trennung von Live- und Testdaten	Physikalische Trennung von Daten in der Live-Applikation und in Test-Applikationen (soweit vom Auftraggeber gewünscht).
----------------------------------	---

### 1.5. Pseudonymisierung

**Ziel:** Mit den hier aufgeführten Maßnahmen wird gewährleistet, dass personenbezogene Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer betroffenen Person zugeordnet werden können.

**Situation:**

Es werden keine Pseudo- oder Anonymisierungsmaßnahmen eingesetzt. Die Nutzung der Plattform ist freiwillig, und die Auftragnehmerin hat keine Entscheidungsbefugnis darüber, welcher Nutzer welche Daten einbringt. Nutzer können ihr Konto jederzeit vollständig löschen.

**Ergriffene Maßnahmen:**

Bereich	Situation
Daten für Entwicklungs-/Support-Zwecke	Für den Support und die Entwicklung neuer Features werden von den Entwicklern, soweit möglich, anonymisierte oder pseudonymisierte Daten verwendet.

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

### 2.1. Weitergabekontrolle

**Ziel:** Gewährleistung, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern 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.

**Situation:**

Daten auf der Plattform werden von der Auftragnehmerin nur nach Weisung des Auftraggebers weitergegeben oder übertragen, soweit die Weitergabe bzw. Übertragung nicht zur Erfüllung ihrer Vertragspflichten dem Auftraggeber gegenüber erforderlich ist. Weitergabe und Übertragung von Daten seitens des Auftraggebers liegen in seiner Sphäre. Im Folgenden werden Maßnahmen beschrieben, die die Zugriffe beliebiger Clients auf den Server absichern und protokollieren.

**Ergriffene Maßnahmen:**

Bereich	Situation
Datentransfer vom/zum Server	Jeglicher Datenaustausch wird unter Einsatz von Verschlüsselung und VPN- bzw. SSH-Technologien nach aktuellem Stand der Technik geschützt. Die Auftragnehmerin versendet weder personenbezogene Daten noch Zugangsdaten wie Passwörter über unverschlüsselte Verbindungen.
Sicherung elektronischer Weitergabe	Bei der elektronischen Weitergabe von Dateien nach Weisung des Kunden werden folgende Maßnahmen je nach Inhalt ergriffen: <ul style="list-style-type: none"> <li>• passwortgeschütztes Zip-Archiv</li> <li>• einmal-Downloadlinks mit nicht erratbarer URL</li> <li>• zeitlich begrenzte Downloadmöglichkeit</li> </ul>

**2.2. Eingabekontrolle**

**Ziel:** Gewährleistung, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

**Ergriffene Maßnahmen:**

Bereich	Situation
Sicherheitsrelevante Änderungen	Datenänderungen, die als sicherheitsrelevant eingestuft werden (z. B. Veränderungen von Zugriffsberechtigungen, Veränderungen von Nutzerstammdaten wie Name oder E-Mail-Adresse und dem genutzt Passwort) werden zentral (nicht revisionssicher) protokolliert. Auf diese Protokolldaten haben standardmäßig nur Administratoren der Auftragnehmerin Zugriff.
Sonstige Änderungen	Die Plattform protokolliert beliebige Datenänderungen zur Erbringung der vertraglichen Leistungen und insbesondere zur Möglichkeit der Analyse im Fehlerfall. Die Wahl, ob das geschehen soll, obliegt dem Auftraggeber.
Sämtliche Lese-/Schreibzugriffe auf Daten	Alle Datenlese- und Schreibzugriffe werden vorbehaltlich anderer Weisung des Auftraggebers nutzerscharf protokolliert.

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

#### 3.1. Verfügbarkeitskontrolle

**Ziel:** Gewährleistung, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

**Ergriffene Maßnahmen:**

Bereich	Situation
Daten-Backups	Es werden nach einem System mit einer Mischung aus vollen und inkrementellen Backups und einem Turnus von maximal einem Jahr alle personenbezogenen Daten des Auftraggebers gesichert, die den jeweils zum Zeitpunkt der Herstellung des Backups aktuellen Stand der Daten abbilden. Auf besagte Backups haben nur Systemadministratoren der Auftragnehmerin Zugriff.

#### 3.2. Zuverlässigkeit

**Ziel:** Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden

**Ergriffene Maßnahmen:**

Bereich	Situation
Server-Monitoring	<ul style="list-style-type: none"> <li>• automatische Überwachungssysteme (Monitoring) kritischer Systeme (Fehler der Datenspeicher, des Dateisystems, Verfügbarkeit der Systeme)</li> <li>• Auftretende Fehler und Warnungen werden protokolliert.</li> </ul>
Server-Ausfallsicherheitsmaßnahmen	<ul style="list-style-type: none"> <li>• Unterbrechungsfreie Stromversorgung (USV)</li> <li>• Notstrom-Dieselaggregat</li> <li>• Feuer- und Rauchmeldeanlage</li> <li>• Klimaanlage in Serverräumen</li> </ul>



### 3.3. Datenintegrität

**Ziel:** Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

**Ergriffene Maßnahmen:**

Bereich	Situation
Server: RAID 1	Auf dem Server wird RAID-1-Technologie eingesetzt, um fehlerhafte Festplattenfunktionen auszugleichen.

### 3.4. Wiederherstellbarkeit (Systeme)

**Ziel:** Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können

**Situation:**

Der robuste Betrieb der Plattform wird über Monitoring gesichert. Vorfälle werden zunächst der Auftragnehmerin und daraufhin unverzüglich dem Auftraggeber gemeldet. Das Support-Team der Auftragnehmerin sichtet den Plattformbetrieb kompromittierende Vorfälle mit hoher Priorität, und die hierbei eingesetzten Prozessen sind Teil der oben genannten TISAX-Zertifizierung.

**Ergriffene Maßnahmen:**

Bereich	Situation
Backup und Recovery	Datenbank- und Applikationsdateien werden täglich auf einem dedizierten Server mit vollen und mit inkrementellen Backups gesichert, die einander nach einer komplexen Logik überschreiben, um größtmögliche Verfügbarkeit auch älterer Daten zu haben, ohne unnötig Speicherplatz für Backups zu verbrauchen. Daten werden mindestens 7 Tage aufbewahrt. Es wird monatlich geprüft, ob die Backups ordnungsgemäß hergestellt wurden.
Incident Management	Kontaktaufnahme mit Hosting-Provider zum Zwecke des Austauschs defekter Hardware und anschließendes Aufspielen des letzten Backups.

## 4. Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

### 4.1. Datenschutz-Management (DSM)

**Ziel:** Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

#### Ergriffene Maßnahmen:

Bereich	Situation
TISAX-Zertifizierung	Die Auftragnehmerin ist TISAX-zertifiziert (Trusted Information Security Assessment Exchange, ein von der Automobilindustrie etablierter Standard für Informationssicherheit, der von ISO 27001 abgeleitet wurde) und prüft regelmäßig die Einhaltung der hierfür erforderlichen Voraussetzungen.
Verpflichtung auf das Datengeheimnis	Alle für Kunden der Auftragnehmerin tätigen Personen – inkl. Erfüllungsgehilfen – werden von der Auftragnehmerin zur Einhaltung geltender Datenschutzpflichten nach Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO verpflichtet.
Sensibilisierung	Alle für Kunden der Auftragnehmerin tätigen Personen werden regelmäßig, in aller Regel jährlich von der externen Datenschutzbeauftragten geschult und sensibilisiert.
Periodische Prüfung der Einhaltung dieser TOM	Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zu ergreifenden technischen und organisatorischen Maßnahmen durch eine unabhängige Stelle, z. B. die externe Datenschutzbeauftragte.

### 4.2. Incident-Response-Management

**Ziel:** Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

#### Situation:

Die Auftragnehmerin hat im Rahmen ihrer TISAX-Maßnahmen (s. einleitender Kommentar zu diesem Dokument) ein Konzept zur Behandlung von Sicherheitsvorfällen („Sicherheitskonzept Sicherheitsvorfallbehandlung“) etabliert, das auf Wunsch zugesendet werden kann. Das Konzept beinhaltet im Kern folgendes Vorgehen:

Jede Meldung an den Support der Auftragnehmerin wird in Bezug auf Informationssicherheit bewertet. Je nach Ergebnis der Bewertung dort beleuchten die verantwortlichen Personen den Vorfall leiten geeignete Maßnahmen ab, sodass der Auftraggeber seine Informationspflichten aus Art. 33 und 34 DSGVO erfüllen kann.

#### **4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO) (*privacy by design, privacy by default*)**

**Ziel:** Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

**Situation:**

Die Nutzung der gesamten Plattform ist freiwillig, die Eingabe jedweder Datenkategorie seitens ihrer Nutzer optional. Abgesehen von einer Verifikation der Nutzungsberechtigung jedes Nutzerkontos steht es Nutzern nach Dafürhalten der Auftragnehmerin frei, beliebige auch falsche und/oder pseudonyme Daten einzugeben, ohne dass den Betroffenen hieraus Nachteile entstehen. Für die Auftragnehmerin als Anbieterin der Plattform besteht damit kein Erfordernis für weitere Maßnahmen.

#### **4.4. Auftragskontrolle**

**Ziel:** Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

**Ergriffene Maßnahmen:**

<b>Bereich</b>	<b>Situation</b>
Archivierung der Weisungen	Dass Daten nur auftragsgemäß von der Auftragnehmerin eingegeben bzw. verändert bzw. gelöscht werden, wird je nach Weisungsart über das von der Auftragnehmerin genutzte Ticket-System oder Archivierung der E-Mail-Korrespondenz mit dem Auftraggeber nachvollziehbar gemacht.
Protokollierung der Zugriffe	Alle Lese- und Schreibzugriffe auf Daten werden nutzerscharf protokolliert.
Archivierung von weisungsbezogenen E-Mails	Weisungsbezogene E-Mails werden gesichert, um Anweisungen nachträglich nachvollziehen und belegen zu können.
Turnusmäßige Prüfung der Unterauftragsverarbeiter	Die von der Auftragnehmerin eingesetzten Unterauftragsverarbeiter werden zweijährlich auf Einhaltung der von ihnen zu ergreifenden technischen und organisatorischen Maßnahmen geprüft.

## Anhang 2

### Eingesetzte Unterauftragsverarbeiter („UAV“)

Die folgenden Unternehmen erbringen (Teil-)Leistungen im Rahmen der vertragsgegenständlichen Leistungen der Auftragnehmerin für den Auftraggeber.

Name, Anschrift	(Teil-)Leistungen	Datenverarbeitungen des UAVs	Verarbeitungsort(e)	Einschlägige Zertifizierungen	Garantien nach Art. 44 ff.
Heinlein Support GmbH Schwedter Straße 8/9B 10119 Berlin Deutschland	Bereitstellung der Räumlichkeiten und technischen Voraussetzungen des LXT-Serverbetriebes	Löschung von Daten im Rahmen der Vernichtung defekter Datenträger.	EU: Berlin, Deutschland	Deren UAV IPB GmbH ist nach ISO 27001 zertifiziert.	[keine erforderlich]
Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, 1855 Luxemburg, Luxemburg	Betrieb der Serverinfrastruktur der eingesetzten LXT-Installation(en)	Sämtliche Datenverarbeitungen im Rahmen der Leistungserbringung der Auftragsverarbeiterin.	EU: Frankfurt, Deutschland	ISO 27001, ISO 27017, ISO 27018	EU-Standardvertragsklauseln