Allgemeine Nutzungsbedingungen („ANB“) der ARDEX Group GmbH (“ARDEX”)

für die Bereitstellung des „ARDEX-Projektplaners“

Stand: Februar 2021

1. Anwendungsbereich

1.1 ARDEX ist Anbieterin der „ARDEX-Projektplaner“-Software („**Projektplaner-Software**“), nutzbar sowohl über den Browser als auch über eine mobile Applikation („**ARDEX-App**“), zur Erstellung und Verwaltung einer Projekt-Übersicht für Baustoff-Informationen bei Bauvorhaben (Projektplaner-Software und ARDEX-App gemeinsam „**Vertragssoftware**“) für Gewerbetreibende, beispielsweise Handwerker („**Nutzer**“).

1.2 Diese ANB regeln die unentgeltliche Bereitstellung von Vertragssoftware durch ARDEX für die Nutzung durch Nutzer.

1.3 Das Angebot von ARDEX richtet sich an Unternehmer gemäß § 14 BGB. Andere Personen sind nicht berechtigt, die Leistungen von ARDEX zu nutzen.

2. Leistungsgegenstand

2.1 ARDEX stellt Nutzer Projektplaner-Software unentgeltlich als so genannten „Cloud-Dienst“ zum Abruf bereit. Die Bereitstellung als „Cloud-Dienst“ basiert auf dem Grundsatz, dass eine Software von einem externen Dienstleister auf einem externen Server betrieben und von einem Nutzer zeitlich befristet genutzt wird. Das bedeutet: Nutzer erhält die Möglichkeit, über ein internetfähiges Endgerät sowie eine Internetanbindung auf von ARDEX bereitgestellte Server zuzugreifen, auf welchen von ARDEX Projektplaner-Software betreiben wird, und so die Funktionalitäten von Projektplaner-Software zu nutzen.

2.2 Nutzer kann sich für die Nutzung von Vertragssoftware mittels individueller Login-Daten für ein myARDEX-Nutzerkonto registrieren, mit denen Nutzer Vertragssoftware nutzen kann. Mit Registrierung kommt ein Vertrag zwischen ARDEX und Nutzer über Nutzung von Vertragssoftware zustande. Nutzer trifft die notwendigen Vorkehrungen, die Nutzung von Vertragssoftware durch Unbefugte zu verhindern.

2.3 Die Funktionalität von Vertragssoftware gestaltet sich wie folgt:

(a) Vertragssoftware ermöglicht Nutzer die Anlage und Bearbeitung von Bau- und Renovierungsprojekten mit der Ermittlung des projektspezifischen Bedarfs an ARDEX Produkten. Ist ein Projekt zur Zufriedenheit des Nutzers mit Inhalten gefüllt, kann ein Projekt-PDF in beliebigem Detailgrad erstellt werden. Hier kann der Nutzer individuelle Anpassungen vornehmen (zum Beispiel durch das Hinzufügen von Projektdaten, Adressdaten und Kontaktdaten).

(b) Vertragssoftware bündelt folgende von ARDEX bereitgestellte Software-Produkte, die Nutzer zugänglich gemacht werden (nahtlose Anbindung): 1. Projektplaner, 2. Raumplaner, 3. 3D-Mess-Software, 4. Aufbauberater, 5. Verbrauchsrechner und 6. ein PDF-Tool.

Vertragssoftware beinhaltet zum einen die Informationen zum myARDEX-Nutzerkonto sowie eine Maske zum Ändern der persönlichen Daten und zum anderen eine Projektliste, in der alle von Nutzer angelegten Projekte enthalten sind. Wird ein Projekt geöffnet, zeigt sich das Projekt auf der graphischen 2D Oberfläche, auf der alle Räume zueinander angeordnet werden können. Des Weiteren werden die Räume in Listenform dargestellt, in der jedem der Räume ein Raumplan sowie Aufbauten für Boden, Wand und Decke zugeordnet sind.

Wenn Nutzer für einen Raum die Raummaße (Wandlängen und Deckenhöhe) anlegen möchte, nutzt er den Raumplaner. Hier hat er entweder die Möglichkeit, die Raummaße händisch anzulegen oder die 3D-Messsoftware zu nutzen. Zur millimetergenauen Ermittlung der Maße kann ebenfalls zur Eingabe ein Laserdistanzmessgerät genutzt werden.

Mithilfe der 3D-Messsoftware werden mit der Smartphone Kamera die Raummaße ermittelt, die dann an dem Raumplaner übermittelt werden.

Um einer Fläche (Boden, Wand oder Decke) Produkte zuzuordnen, wird der Aufbauberater genutzt. Hier kann in einem jeweiligen Anwendungsszenario (zum Beispiel Boden im Wohnzimmer oder Wand im Badezimmer) mithilfe des vorliegenden Untergrunds und des gewünschten Oberbelags ein empfohlener ARDEX-Standardaufbau ermittelt. Dieser Standardaufbau für optimale Baustellenbedingungen kann noch

individualisiert werden, indem beispielsweise Produkte geändert oder hinzugefügt werden.

Wurde ein Aufbau ausgewählt, rechnet der Verbrauchsrechner automatisch mithilfe der Raummaße die benötigten Mengen und ARDEX-Gebinde aus –gegebenenfalls müssen noch einige Zusatzangaben gemacht werden, wie zum Beispiel Auftragshöhe der Produkte, Mischungsverhältnisse oder Zahnung.

Hat Nutzer einem Projekt alle gewünschten Informationen hinzugefügt, kann ein PDF erstellt werden, dass Nutzer beispielsweise als Materialliste dient oder dessen Kunden als Marketingunterlage zugesandt wird.

3. Nutzungsrechte

Nutzer erhält das nicht ausschließliche, räumlich auf die Bundesrepublik Deutschland beschränkte, nicht übertragbare und nicht unterlizenzierbare Recht, Vertragssoftware während der Laufzeit des auf Basis dieser ANB geschlossenen Vertrags für eigene interne Geschäftszwecke zu nutzen.

4. Mängelhaftung

Aufgrund der kostenlosen Nutzungsmöglichkeit haftet ARDEX gemäß § 600 BGB für aus Sach- oder Rechtsmängeln entstehende Schäden nur, wenn sie diese arglistig verschweigt.

5. Haftung

Aufgrund der kostenlosen Nutzungsmöglichkeit hat ARDEX gemäß § 599 BGB nur Vorsatz und grobe Fahrlässigkeit zu vertreten.

6. Daten

6.1 Im Rahmen der Erbringung der Leistungen verarbeitet ARDEX personenbezogene Daten im Auftrag von Nutzer. Deshalb schließen die Parteien einen Vertrag über eine Auftragsverarbeitung gemäß **Anlage 1 (Auftragsverarbeitungsvereinbarung)** dieser ANB.

6.2 ARDEX erhält an nicht-personenbezogenen Daten über die Nutzung von Vertragssoftware, insbesondere statistische Daten, ein ausschließliches, zeitlich, räumlich und inhaltlich unbeschränktes Nutzungsrecht.

7. Vertragsdauer, Kündigung

Der Vertrag wird auf unbestimmte Zeit geschlossen. Er kann von jeder Partei jederzeit ohne Einhaltung einer Kündigungsfrist gekündigt werden.

8. Abschließende Bestimmungen

8.1 Dieser Vertrag unterliegt deutschem Recht mit Ausnahme des UN-Kaufrechts vom 11. April 1980 (Wiener CISG-Übereinkommen).

8.2 Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist Witten (Deutschland), wenn die Parteien Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliche Sondervermögen sind.

Anlage 1: Auftragsverarbeitungsvereinbarung

Anlage 1 zu den Nutzungsbedingungen für die Projektplaner-Software und ARDEXIA-App

Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO
zwischen

dem registrierten Nutzer (hier bezeichnet als „Auftraggeber“) der **Projektplaner-Software und ARDEXIA-App** (hier bezeichnet als „Vertragssoftware“) als Verantwortlicher

und

ARDEX Group GmbH
Friedrich-Ebert-Str. 45
58453 Witten
als Auftragsverarbeiter

§ 1 Begriffsbestimmungen

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

§ 2 Vertragsgegenstand

(1) Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen im Bereich Hosting von personenbezogenen Daten natürlicher Personen, die der Verantwortliche bei der Nutzung der Vertragssoftware darin eingibt und speichert auf Grundlage der Allgemeinen Nutzungsbedingungen („ANB“) der ARDEX Group GmbH für die Bereitstellung des „ARDEX-Projektplaners“ (im Folgenden „Hauptvertrag“), in der jeweils gültigen Fassung.

Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Verantwortlichen, sofern der Auftragsverarbeiter nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Umfang und Zweck der Datenverarbeitung durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag sowie aus dem **Annex 1** zu diesem Vertrag. Dem Verantwortlichen obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

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

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

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

§ 4 Art der verarbeiteten Daten, Kreis der betroffenen Personen

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

§ 5 Weisungsrecht

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

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

(3) Alle erteilten Weisungen sind sowohl vom Verantwortlichen als auch vom Auftragsverarbeiter zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Verantwortlichen an den Auftragsverarbeiter entstehen, bleiben unberührt.

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

§ 6 Schutzmaßnahmen des Auftragnehmers

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

(2) Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gem. Art. 32 DS-GVO, insbesondere mindestens die in **Annex 2** aufgeführten Maßnahmen getroffen hat. Der Auftragsverarbeiter legt auf Anforderung des Verantwortlichen die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragsverarbeiter ist als betrieblicher Datenschutzbeauftragter bestellt:

DS EXTERN GmbH, Dipl. Kfm. Marc Althaus, Frapanweg 22, 22589 Hamburg, https://www.dsextern.de/anfragen

(4) Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu nutzen oder auf sonstige Weise zu verarbeiten. Der Auftragsverarbeiter wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Beschäftigte genannt), entsprechend verpflichten und über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung

dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragsverarbeiter bestehen bleiben. Dem Verantwortlichen sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Informationspflichten des Auftragnehmers

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

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
c) eine Beschreibung der vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

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

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

(4) Der Auftragsverarbeiter unterstützt den Verantwortlichen erforderlichenfalls bei der Erfüllung der Pflichten des Auftraggebers nach Art. 33 und 34 DS-GVO in angemessener Weise (Art. 28 Abs. 3 S. 2 lit. f DSGVO). Meldungen für den Auftragsverarbeiter nach Art. 33 oder 34 DS-GVO darf der Auftragsverarbeiter nur nach vorheriger Weisung seitens des Verantwortlichen gem. § 5 dieses Vertrags durchführen.

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

(6) Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 6 Abs. 2 dieses Vertrags hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu unterrichten.

(7) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen.

(8) Der Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Verantwortlichen auf Anforderung zur Verfügung zu stellen.

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

§ 8 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters. Hierfür kann er z. B. Auskünfte des Auftragsverarbeiters einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst

persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören.

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

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

(4) Der Auftragsverarbeiter weist dem Verantwortlichen die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

(6) Der Verantwortliche vergütet dem Auftragsverarbeiter den Aufwand, der ihm im Rahmen der Kontrolle entsteht.

§ 9 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Annex 3** genannten Subunternehmer durchgeführt. Der Auftragsverarbeiter ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Er setzt den Verantwortlichen hiervon unverzüglich in Kenntnis. Der Auftragsverarbeiter ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragsverarbeiter hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist. Der Auftragsverarbeiter wird dem Verantwortlichen auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

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

§ 10 Anfragen und Rechte betroffener Personen

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

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

§ 11 Haftung

(1) Verantwortlicher und Auftragsverarbeiter haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung. Der Auftragsverarbeiter stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Verantwortlichen ab.

(2) Der Auftragsverarbeiter stellt den Verantwortlichen von sämtlichen Ansprüchen frei, die betroffene Personen gegen den Verantwortlichen wegen der Verletzung einer dem Auftragsverarbeiter durch die DSGVO auferlegten Pflicht oder der Nichtbeachtung oder Verletzung einer vom Verantwortlichen in dieser AV-Vereinbarung oder einer gesondert erteilten Anweisung geltend machen.

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

(4) Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

§ 12 Außerordentliches Kündigungsrecht

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

§ 13 Beendigung des Hauptvertrags

(1) Der Auftragsverarbeiter wird dem Verantwortlichen nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Verantwortlichen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Der Auftragsverarbeiter hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(2) Der Auftragsverarbeiter ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm vom Verantwortlichen zugeleitet wurden oder die er für diesen erhoben hat.

§ 14 Schlussbestimmungen

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

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

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

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

(5) Diese Vereinbarung tritt mit Wirksamwerden der ANB zwischen den Parteien in Kraft, ohne dass es eines separaten Abschlusses dieser Vereinbarung bedarf.

Anlagen:

Annex 1 – Beschreibung der betroffenen Personen/Betroffenengruppen

Annex 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Annex 3 – Genehmigte Subunternehmer

Annex 1 zur Auftragsverarbeitungsvereinbarung – Beschreibung Datenverarbeitung sowie der betroffenen Personen/Betroffenengruppen sowie der betroffenen /Datenkategorien

- Beschreibung der Datenverarbeitung: Hosting der unten beschriebenen personenbezogenen Daten, die durch den registrierten Nutzer anlässlich der Nutzung des ARDEX-Projektplaners anfallen
- Betroffene Personen: Kunden, Interessenten und Mitarbeiter des registrierten Nutzers
- Betroffene Datenkategorien: Personenstammdaten, Kontaktdaten, Objektdaten, Auftragsdaten

Annex 2 zur Auftragsverarbeitungsvereinbarung – Technische und organisatorische Maßnahmen des Auftragnehmers

Teil 1 – ARDEX Group GmbH

Dokumenteneigenschaften

Verantwortung	IT-Security
Klassifizierung	Intern/Extern
Gültigkeitszeitraum	Unbegrenzt
Überarbeitungsintervall	Jährlich
Nächste Überarbeitung	01.08.2022

Dokumentenstatus und Freigabe

Status	Version	Datum	Name und Abteilung
Erstellt	1.0	01.08.2021	

Dokumentenhistorie

Version	Änderung	Datum	Autor
1.0	Initiale Erstellung	01.08.2021	Patrik Franke

Inhalt

1. Vorwort

Zur Einhaltung der Anforderungen an den Datenschutz und die Datensicherheit gemäß DSGVO und BDSG, insbesondere im Zusammenhang mit Verträgen zur Auftragsverarbeitung, setzt ARDEX Group GmbH die nachfolgend in den einzelnen Aufzählungspunkten beschriebenen Maßnahmen im Unternehmen um.

Die Maßnahmen werden im Rahmen der betrieblichen Abläufe der ARDEX Group GmbH laufend aktualisiert, so dass auf eine Konkretisierung (z. B. in Bezug auf verwendete Hard-/Software) hier verzichtet wird.

2. Maßnahmen gem. Art. 32 DSGVO

2.1. Pseudonymisierung

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.

2.2. Verschlüsselung

Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.

- Verschlüsselung von Speichermedien
- Verschlüsselung der Kommunikation

2.3. Fähigkeit der Vertraulichkeit

Vertraulichkeit bedeutet, dass personenbezogene Daten vor unbefugter Einsichtnahme geschützt sind.

- Individueller Log-In und Kennwortverfahren
- Verwaltung von Berechtigungen
- Dokumentation von Berechtigungen
- Verschlüsselung der Kommunikation
- VPN (Virtual Private Network)
- Gesichertes WLAN
- Gesichertes LAN (802.1x)
- TLS-Verschlüsselung bei Web-Access

2.4. Fähigkeiten der Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten nachweisbar vollständig und unverändert sind.

- Verwendung von Zugriffsrechten
- Funktionelle Verantwortlichkeiten

2.5. Fähigkeit der Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

- Back-Up Verfahren
- Spiegeln von Festplatten / Virtuellen Maschinen
- Virenschutz / Firewall
- Hoch verfügbare Cloud Plattform

2.6. Fähigkeit der Belastbarkeit

Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.

- Penetrationstests für direkt im Internet sichtbare Systeme (fallweise) und anschließende Härtung der Systeme bei Bedarf
- 24h-Monitoring-System in Bezug auf Verfügbarkeit, Performance und Auslastung der für den IT- Betrieb notwendigen Systeme mit Auswertung und Überwachung des Monitoring-Systems durch Mitarbeiter der eigenen IT
- redundante Auslegung der wichtigsten Systeme für den IT-Betrieb

2.7. Wiederherstellbarkeit der Verfügbarkeit und des Zugangs

Die Wiederherstellbarkeit der Verfügbarkeit beschreibt die möglichst zeitnahe Wiederherstellung von Systemen und Zugängen und die damit einhergehende Verfügbarmachung von Daten.

- Back-Up Verfahren
- Hoch verfügbare Cloud Plattform

2.8. Verfahren zur regelmäßigen Überprüfung

Die Gewährleistung der Umsetzung der genannten Datensicherungsmaßnahmen durch regelmäßige Überprüfungen.

- Interne regelmäßige Prüfung durch den Datenschutzbeauftragten
- Erstellung von Prüfberichten

2.9. Unrechtmäßiger Zugang zu personenbezogenen Daten

Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?

- Individueller Log-In und Kennwortverfahren
- Sperrung der Clients bei Erkennung von Unbefugtem Zugriff
- Verwaltung von Berechtigungen
- Dokumentation von Berechtigungen

2.10. Verarbeitung personenbezogener Daten nur nach Anweisung

Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?

- Mitarbeiter sind zu Verhaltensregeln verpflichtet
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Bestimmung von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag

3. Maßnahmen gem. BDSG / Sonstige Maßnahmen

3.1. Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte:

- Schlüssel / Schlüsselvergabe

3.2. Datenträgerkontrolle

Unterbindung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern:

- Automatische Sperrung
- Kennwortverfahren

3.3. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten:

- Automatische Sperrung
- Kennwortverfahren

3.4. Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte:

- Automatische Sperrung
- Kennwortverfahren

3.5. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben:

- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Kenntnisnahme
- Veränderung
- Löschung

3.6. Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:

- Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
- Protokollierung

3.7. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind:

- Protokollierung

3.8. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

- Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
- Protokollierung

3.9. Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können:

- Backup-Verfahren
- Spiegeln von Festplatten

3.10. Zuverlässigkeit

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

- Funktionelle Verantwortlichkeiten
- Monitoring der Verfügbarkeit

3.11. Datenintegrität

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

- Maßnahmen sind ergriffen worden, die die Beschädigung/Veränderung der geschützten Daten während der Verarbeitung oder Übertragung verhindern
- Prüfung der Datenintegrität der Backup-Systeme

3.12. Auftragskontrolle

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

- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung

3.13. Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

- Backup-Verfahren
- Virenschutz / Firewall
- Hoch verfügbare Cloud Plattform

3.14. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können:

- "Interne Mandantenfähigkeit" / Zweckbindung
- Funktionstrennung /Produktion / Test
- Netzwerksegmentierung (Datenflusstrennung)

Teil 2 – engine-produtions GmbH

Technische und organisatorische Maßnahmen

1 Vertraulichkeit

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu den vom Auftragnehmer zwecks Erbringung der ihm übertragenen Leistungen genutzten technischen Einrichtungen zu verwehren.

Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation der Vergabe von Schlüsseln, RFID-Chipkarten oder -Transpondern;
Die Vergabe von Schlüsseln, RFID-Chipkarten oder -Transpondern erfolgt ausschließlich an Mitarbeiter. Die Vergabe wird durch einen weiteren Mitarbeiter begleitet und erfolgt erst nach Unterzeichnung eines Übergabeprotokolls. Im Protokoll werden die beteiligten Personen, das Datum und die Uhrzeit der Vergabe, die Schlüssel-Nummer oder die ID der Chipkarte festgehalten. Das Protokoll wird an zentraler Stelle sicher verwahrt. Alle Inhaber werden zudem darüber informiert, dass Schüssel, RFID-Chipkarten oder -Transponder sicher zu verwahren sind und deren Verlust umgehend zu melden ist.
Gesonderte Zutrittskontrolle für Räume mit kritischer IT-Infrastruktur;
Der Zutritt zu Räumen mit kritischer IT-Infrastruktur (z. B. Serverraum) ist ausschließlich ausgewählten Mitarbeitern gestattet. Die Räume verfügen über keine Fenster. Ein Zutritt ist nur über eine Tür möglich, die stets verschlossen ist. Ein Zutritt zu diesen Räumlichkeiten ist zudem nur mit einem zusätzlichen Schüssel, einer RFID-Chipkarte, einem RFID-Transponder oder mittels eines PINCodes möglich. Externen Personen (z. B. Servicetechnikern) ist der Zutritt nur nach vorheriger Anmeldung und Erfassung der persönlichen Daten gestattet. Ein Zutritt zu Räumen mit kritischer IT-Infrastruktur ist Externen nur in Begleitung von ausgewählten Mitarbeitern gestattet.
Rückgabe von Schlüsseln, RFID-Chipkarten oder -Transpondern nach Austritt von Mitarbeitern;
Vor Beendigung des Anstellungsverhältnisses müssen Mitarbeiter zuvor ausgehändigte Schlüssel, RFID-Chipkarten oder -Transponder zurückgeben. Die Rückgabe wird von einem weiteren Mitarbeiter durchgeführt und überwacht. Die Namen der beteiligten Personen, das Datum und die Uhrzeit der Rückgabe, die Schlüssel-Nummer oder die ID der Chipkarte oder des Transponders werden im Übergabeprotokoll festgehalten. Das Protokoll wird an zentraler Stelle sicher verwahrt.
Verwendung einer Zutrittskontrolle;
Der Zutritt zum Bürogebäude ist ausschließlich mit Hilfe eines entsprechenden Schlüssels, einer RFID-Chipkarte oder eines RFID-Transponders möglich. Diese werden ausschließlich an Mitarbeiter ausgeteilt und müssen vor Austritt aus dem Unternehmen wieder zurückgegeben werden. Eine Vervielfältigung der eingesetzten Schlüssel, RFID-Chipkarten oder -Transponder ist nicht möglich.

1.2 Zugangskontrolle

Es ist zu verhindern, dass die zur Erbringung der in der beschriebenen IT-Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme,
Software) von Unbefugten genutzt werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Automatisches Sperren von PCs / Macs nach fünf Minuten;
Alle im Einsatz befindlichen Arbeitsplatzrechner (PCs, Macs) rufen nach fünfminütiger Inaktivität automatisch die Anmeldemaske des jeweiligen Betriebssystems auf. Ein Zugriff auf die Arbeitsplatzrechner ist dann nur nach vorheriger Eingabe des Nutzerpassworts möglich. So wird verhindert, dass Unbefugte beispielsweise während der Pausenzeiten Zugriff auf kritische Daten erlangen können.
Verwendung einer Firewall;
Im gesamten Unternehmensnetzwerk kommt eine Firewall zum Einsatz, die darin betriebene Arbeitsplatzrechner und Server vor unerwünschten Netzwerkzugriffen schützt. Die Firewall-Firmware wird regelmäßig aktualisiert und die angelegten Firewall-Richtlinien in diesem Zuge überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.
Verwendung personalisierter Logins;
Sowohl für interne als auch externe Systeme werden grundsätzlich personalisierte Logins vergeben. So kann sichergestellt werden, dass durchgeführte Aktionen nachträglich dem jeweiligen Benutzer zugeordnet werden können. Zudem können einzelne Zugänge zielgerichtet gesperrt oder gelöscht werden, ohne dass dies Einfluss auf die Zugänge anderer Mitarbeiter hat.
Verwendung sicherer und individueller Passwörter;
Sowohl für interne als auch externe Zugänge werden ausschließlich sichere Passwörter mit einer Länge von mindestens zehn Zeichen verwendet. Die Passwörter beinhalten zudem mindestens einen Groß- und Kleinbuchstaben, eine Zahl sowie ein Sonderzeichen. Auch wird sichergestellt, dass ein Passwort nicht für mehrere Zugänge verwendet wird. Wird einer der genutzten Zugänge kompromittiert, bleibt die Sicherheit der übrigen Zugänge nachwievor gewahrt.
Verwendung und regelmäßige Aktualisierung eines Virenscanners;
Eingehende E-Mails sowie Arbeitsplatzrechner werden durch einen Virenscanner vor den Auswirkungen von schädlichen Dateien geschützt. Die zur Erkennung von aktuellen Bedrohungen notwendigen Definitionen und Regeln werden regelmäßig aktualisiert. Als gefährlich eingestufte Dateien oder E-Mails werden in einen separaten Quarantäne-Ordner verschoben. Die Wiederherstellung von Dateien aus dem Quarantäne-Ordner ist nur nach vorheriger Freigabe durch ausgewählte Mitarbeiter möglich. Um die korrekte Funktion des eingesetzten Virenscanners sicherzustellen, erfolgt der regelmäßige Scan einer speziellen Testdatei, die von allen aktuellen Virenschutzlösungen erkannt wird.

1.3. Zugriffskontrolle

Es ist sicherzustellen, 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 oder verändert werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation eingerichteter Zugänge für Mitarbeiter;
Alle Zugänge zu internen und externen Systemen werden vor deren Einrichtung dokumentiert. Dabei werden der Name des Mitarbeiters, das jeweilige System sowie der eingerichtete Benutzername protokolliert. Diese Informationen stellen die Basis dafür dar, dass bei einem späteren Austritt zielgerichtet die Zugänge des jeweiligen Mitarbeiters gesperrt bzw. gelöscht werden können.
Minimale Anzahl an Mitarbeitern mit administrativen Rechten;
Um zu gewährleisten, dass lediglich autorisierte Personen Zugriff auf kritische IT-Systeme sowie darauf gespeicherter Daten haben, verfügen nur ausgewählte Mitarbeiter über die notwendigen administrativen Rechte. Diese Mitarbeiter schalten projektbezogen die Zugriffsrechte der anderen Mitarbeiter frei, sofern diese für ihre Arbeit notwendig sind. Nach Abschluss der jeweiligen Arbeiten werden die entsprechenden Rechte wieder entzogen. So wird die Anzahl der Mitarbeiter, die theoretisch Zugriff auf alle im Unternehmen gespeicherten personenbezogenen Daten haben, auf ein absolutes Minimum reduziert.
Nutzung von Benutzer- und Rollenkonzepten für interne und externe Systeme;
Für interne und externe Systeme, die diese Funktionalität unterstützen, werden Benutzer- und Rollenkonzepte beim Anlegen von Zugängen verwendet. Anstatt jeden einzelnen Zugang mit entsprechenden Berechtigungen auszustatten, wird jedem Zugang eine Rolle zugewiesen. Diesen übergeordneten Rollen werden wiederum die notwendigen Berechtigungen zugewiesen. So können Änderungen an den Berechtigungen zentral über die Anpassung der jeweiligen Rolle erfolgen. So kann verhindert werden, dass einzelne Zugänge über Berechtigungen verfügen, die diesen eigentlich nicht gestattet wären.
Sperrung von Zugängen beim Austritt von Mitarbeitern;
Verlässt ein Mitarbeiter das Unternehmen, so erfolgt noch vor dessen Austritt die Sperrung bzw. Löschung aller ihm zugewiesenen Zugänge für interne und externe Systeme. Als Basis für diesen Vorgang wird die Dokumentation der zuvor angelegten Zugänge verwendet. In der Dokumentation wird abschließend ebenfalls die Sperrung bzw. Löschung der Zugänge vermerkt.
Verwendung sicherer und individueller Passwörter;
Sowohl für interne als auch externe Zugänge werden ausschließlich sichere Passwörter mit einer Länge von mindestens zehn Zeichen verwendet. Die Passwörter beinhalten zudem mindestens einen Groß- und Kleinbuchstaben, eine

Zahl sowie ein Sonderzeichen. Auch wird sichergestellt, dass ein Passwort nicht für mehrere Zugänge verwendet wird. Wird einer der genutzten Zugänge kompromittiert, bleibt die Sicherheit der übrigen Zugänge nachwievor gewahrt.
Zentrale Verwaltung von Benutzerzugängen und -rechten;
Zur Dokumentation aller Zugänge für interne und externe Systeme kommt eine Software zum Einsatz, in der alle Informationen zu Mitarbeitern sowie deren Zugängen erfasst werden. Die softwaregestützte Erfassung und Verwaltung alle Benutzerzugänge stellt u. A. sicher, dass beim Austritt von Mitarbeitern alle für ihn angelegten Zugänge vollständig gesperrt bzw. gelöscht werden.

1.4 Weitergabekontrolle

Es muss dafür gesorgt werden, 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 welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Beim Auftragnehmer umgesetzte Maßnahmen:

Beauftragung zuverlässiger Transportunternehmen;
Beim Versand von Daten auf dem Postweg oder beim Transport von Servern wird darauf geachtet, dass nur zuverlässige und vertrauenswürdige Transportunternehmen eingesetzt werden.
Nutzung SSL-verschlüsselter Übertragungswege im Internet;
Für die Übermittlung von Daten mit personenbezogenem Inhalt über das Internet werden ausschließlich SSL/TLS-verschlüsselte Übertragungswege genutzt. Die gesicherte Verbindung zwischen Browser und Zielserver stellt sicher, dass Daten zwischen diesen beiden Systemen nicht von Dritten eingesehen oder manipuliert werden können.
Sorgfältige Auswahl von Transportunternehmen und -fahrzeugen;
Beim physischen Transport von personenbezogenen Daten (z. B. Übermittlung großer Datenmengen auf einer Blu-ray Disc durch einen Kurier) werden nur ausgesuchte und zuverlässige Transportunternehmen mit einwandfreier Reputation beauftragt, die zudem über die notwendige Erfahrung für einen Transport von sensiblen Daten verfügen. Auch die Verfügbarkeit geeigneter Transportfahrzeuge hat Einfluss auf die Auswahl. Nach erfolgreicher Übermittlung wird zudem die Rückmeldung des Empfängers eingeholt, welcher ebenfalls zu seiner Erfahrung mit dem Transportunternehmen befragt wird.
Verwendung von VPN-Systemen zum Login in das Firmennetzwerk;
Ein externer Zugriff auf das Firmennetzwerk ist nur mittels einer VPN-Verbindung möglich. Die hierfür verwendeten Komponenten werden regelmäßig aktualisiert. Zugriffe über VPN werden vollständig protokolliert, um durchgeführte Aktionen

nachträglich nachvollziehen zu können. Zur Nutzung von VPN wird jedem Mitarbeiter, der einen solchen Zugang für seine Arbeit benötigt, ein individueller Zugang erstellt.

1.5 Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Trennung von internem WLAN und Gäste-WLAN;
Gäste, denen ein Zugang zum Internet ermöglicht werden soll, erhalten einen individualisierten Zugang oder die Zugangsdaten zu einem eigenem WLAN. Von diesem separaten WLAN aus ist ein Zugriff auf das firmeninterne Netzwerk und alle dort hinterlegten Daten nicht möglich. So wird verhindert, dass Gäste unberechtigterweise auf personenbezogene Daten im Firmennetzwerk zugreifen können.
Trennung von Live- und Entwicklungssystemen;
Für die Entwicklung und Programmierung stehen den Entwicklern eigene Entwicklungsumgebungen mit anonymisierten oder pseudonymisierten Testdaten zur Verfügung, sodass eine Entwicklung am Produktivsystem mit den darin gespeicherten Echtdaten nicht notwendig ist. So kann verhindert werden, dass versehentlich eine ungewollte Veränderung oder Weitergabe von personenbezogenen Daten erfolgt. Ausschließlich die gemeinsam mit dem Endkunden durchgeführten Live-Tests vor Projektabschluss erfolgen unter Zuhilfenahme der jeweiligen Echtdaten.
Verwendung von Zugriffsberechtigungen für interne Systeme;
Alle internen Systeme sind vor unbefugtem Zugriff gesichert. Es ist nicht möglich, diese ohne eine weitere Anmeldung zu verwenden, wenn man sich im Firmennetzwerk befindet. Die Berechtigungen zur Nutzung der verschiedenen Systeme werden individuell vergeben und können individuell und systembezogen widerrufen werden. Ein genereller Zugriff auf alle im Firmennetzwerk befindlichen Daten wird somit unterbunden.

1.6 Pseudonymisierung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Beim Auftragnehmer umgesetzte Maßnahmen:

Verwendung von pseudonymisierten Daten im Arbeitsalltag: Maßnahmen zur Pseudonymisierung von Daten erfolgen aktuell nicht.

1.7 Verschlüsselung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

Beim Auftragnehmer umgesetzte Maßnahmen:

Verwendung verschlüsselter Übertragungswege für den Datenaustausch;
Werden Daten digital ausgetauscht, die unter Umständen personenbezogene Daten enthalten könnten, findet dies ausschließlich auf sicheren und verschlüsselten Übertragungswegen statt. Es werden insbesondere SSH-Verbindungen genutzt und keine unverschlüsselten Protokolle verwendet, wenn verschlüsselte Alternativen zur Verfügung stehen. So werden E-Mails zum Beispiel via IMAP nur mit SSL/TLS oder HTTPS-Verbindungen.
Verwendung von SSL-Zertifikaten für Hostingumgebungen;
Alle von uns betreuten Webseiten sowie die hierfür genutzten Hostingumgebungen, über die personenbezogene Daten über das Internet übermittelt werden, z. B. durch Kontaktformulare oder Eingabemasken, werden von uns mit SSL-Zertifikaten geschützt. Die Zertifikate werden in regelmäßigen Abständen neu ausgestellt, um einen Diebstahl des Zertifikats und somit das Abgreifen von Daten zu verhindern.

2 Integrität

2.1 Eingabekontrolle

Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

Nutzung von Benutzer- und Rollenkonzepten für interne und externe Systeme;
Für interne und externe Systeme, die diese Funktionalität unterstützen, werden Benutzer- und Rollenkonzepte beim Anlegen von Zugängen verwendet. Anstatt jeden einzelnen Zugang mit entsprechenden Berechtigungen auszustatten, wird jedem Zugang eine Rolle zugewiesen. Diesen übergeordneten Rollen werden wiederum die notwendigen Berechtigungen zugewiesen. So können Änderungen an den Berechtigungen zentral über die Anpassung der jeweiligen Rolle erfolgen. So kann verhindert werden, dass einzelne Zugänge über Berechtigungen verfügen, die diesen eigentlich nicht gestattet wären.
Verwendung personalisierter Logins;
Sowohl für interne als auch externe Systeme werden grundsätzlich personalisierte Logins vergeben. So kann sichergestellt werden, dass

durchgeführte Aktionen nachträglich dem jeweiligen Benutzer zugeordnet werden können. Zudem können einzelne Zugänge zielgerichtet gesperrt oder gelöscht werden, ohne dass dies Einfluss auf die Zugänge anderer Mitarbeiter hat.

2.2 Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle gem. 1.4 dienen auch der Sicherstellung der Integrität.

3 Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

Erstellung von Code-Dokumentationen in der Entwicklung;
Alle entwickelten Systeme und darin verwendete Code-Bestandteile werden durch die Entwickler hinreichend dokumentiert. Dies stellt u. A. eine schnelle Einarbeitung anderer Mitarbeiter in das jeweilige Projekt sicher. Darüber hinaus kann eine Weiterentwicklung der jeweiligen Code-Bestandteile zukünftig auch dann erfolgen, wenn der ursprüngliche Entwickler nicht mehr im Unternehmen tätig ist. Durch eine hinreichende Dokumentation wird zudem sichergestellt, dass Bugs oder Fehler schneller identifiziert und behoben werden können.
Klimatisierung von Räumen mit kritischer IT-Infrastruktur;
Alle Systemkomponenten, die zur Sicherstellung des Betriebs sowie zur Bereitstellung von Kundensystemen notwendig sind (z. B. Server, Netzwerkkomponenten oder Backup-Systeme) sind vor schädlichen Umgebungsbedingungen wie zu hohen Temperaturen oder zu hoher Luftfeuchtigkeit mittels einer Klimatisierung geschützt. Diese wird regelmäßig gewartet und bei einer Erweiterung der Systemkomponenten entsprechend der benötigten Kühlleistung ausgebaut.
Nutzung einer Versionskontrolle in der Entwicklung;
Für die Entwicklung von Anwendungen werden gängige Versionierungssysteme (z. B. Git) eingesetzt. Diese stellen sicher, dass vorherige Softwarestände nicht versehentlich überschrieben werden und die parallele Entwicklung durch mehrere Mitarbeiter an einem System nicht zu Fehlern oder zum Überschreiben von bestehenden Daten führt. Zudem können durch eine Versionskontrolle Änderungen und Fehler nachträglich schneller und besser nachvollzogen und behoben werden. Unabsichtlich durchgeführte Änderungen können außerdem rückgängig gemacht werden.
Regelmäßige Durchführung von Updates;
Alle im Einsatz befindlichen Betriebssysteme sowie darauf installierte

Anwendungen und Bibliotheken werden stets aktuell gehalten. Entsprechende Updates werden regelmäßig eingespielt. Zur Verfügung gestellte Security-Patches werden ebenfalls zeitnah eingespielt, um die entsprechenden Sicherheitslücken schnellstmöglich zu schließen. Werden für Anwendungen oder Bibliotheken keine Security-Updates mehr ausgeliefert oder wird die Anwendung vom Hersteller nicht mehr weiterentwickelt oder betreut, findet ein Upgrade auf eine aktuelle Version statt oder es findet ein Wechsel auf eine noch unterstützte alternative Anwendung statt.
Überprüfung erstellter Datensicherungen;
Erstellte Datensicherungen werden regelmäßig auf ihre Integrität und Wiederherstellbarkeit hin überprüft. Hierfür werden zufällig ausgewählte Daten von einem zufällig ausgewählten Zeitpunkt testweise aus einer Datensicherung wiederhergestellt und mit den Originaldateien verglichen. So können unbrauchbare Datensicherungen oder Fehler im Backup- bzw. Wiederherstellungssystem frühzeitig erkannt und behoben werden.
Verwendung von Brandmeldern;
Zur Vermeidung von Schäden durch Feuer werden Brandmelder verwendet. Diese wurden in jedem Bereich des Bürogebäudes angebracht und untereinander vernetzt. Im unwahrscheinlichen Fall eines Feuers kann so der betroffene Bereich schnell identifiziert und mit Hilfe von öffentlich zugänglichen Feuerlöschern bei Bedarf gelöscht werden. Die Brandmeldeanlage wird regelmäßig durch ein Spezialunternehmen gewartet, um deren ordnungsgemäße Funktion sicherzustellen.
Verwendung einer Firewall;
Im gesamten Unternehmensnetzwerk kommt eine Firewall zum Einsatz, die darin betriebene Arbeitsplatzrechner und Server vor unerwünschten Netzwerkzugriffen schützt. Die Firewall-Firmware wird regelmäßig aktualisiert und die angelegten Firewall-Richtlinien in diesem Zuge überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.
Verwendung eines Überspannungsschutzes für interne Systeme;
Zum Schutz vor Schäden durch Blitzeinschlag oder eine fehlerhafte Netzeinspeisung, werden Einrichtungen verwendet, die eine zu hohe Netzspannung in allen Bereichen des Bürogebäudes verhindern.
Verwendung und regelmäßige Aktualisierung eines Virenscanners;
Eingehende E-Mails sowie Arbeitsplatzrechner werden durch einen Virenscanner vor den Auswirkungen von schädlichen Dateien geschützt. Die zur Erkennung von aktuellen Bedrohungen notwendigen Definitionen und Regeln werden regelmäßig aktualisiert. Als gefährlich eingestufte Dateien oder E-Mails werden in einen separaten Quarantäne-Ordner verschoben. Die Wiederherstellung von Dateien aus dem Quarantäne-Ordner ist nur nach vorheriger Freigabe durch ausgewählte Mitarbeiter möglich. Um die korrekte Funktion des eingesetzten Virenscanners sicherzustellen, erfolgt der regelmäßige Scan einer speziellen Testdatei, die von

allen aktuellen Virenschutzlösungen erkannt wird.
Verwendung von RAID-Systemen;
Zum Schutz vor Hardwareausfällen und Datenverlusten durch defekte Festplatten, werden diese in kritischen IT-Systemen (z. B. lokale Datei- oder Entwicklungsserver) in Form eines RAID-Systems verbaut. In diesem werden Daten auf mindestens zwei Festplatten gespeichert. Auf die in einem RAIDSystem gespeicherten Daten kann somit auch bei einem Ausfall von einer Festplatte weiterhin zugegriffen werden. Defekte Festplatten werden umgehend vom System gemeldet und können entsprechend getauscht werden. Ein Datenverlust kann so vermieden werden.

3.2 Wiederherstellbarkeit

Es müssen Maßnahmen getroffen werden, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall wiederherzustellen.

Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation von datenschutzrelevanten Zwischenfällen;
Datenschutzrelevante Zwischenfälle, bei denen nicht ausgeschlossen werden kann, dass personenbezogene Daten gelöscht oder an unberechtigte Dritte weitergeleitet wurden, werden umfassend dokumentiert. Die Unterlagen dienen zum einen einer lückenlosen Kommunikation an die Datenschutzbehörden sowie die betroffenen Kunden, zum anderen können auf Basis dieser Informationen Verbesserungen umgesetzt werden, die ähnliche Vorfälle zukünftig verhindern.
Nutzung einer Versionskontrolle in der Entwicklung;
Für die Entwicklung von Anwendungen werden gängige Versionierungssysteme (z. B. Git) eingesetzt. Diese stellen sicher, dass vorherige Softwarestände nicht versehentlich überschrieben werden und die parallele Entwicklung durch mehrere Mitarbeiter an einem System nicht zu Fehlern oder zum Überschreiben von bestehenden Daten führt. Zudem können durch eine Versionskontrolle Änderungen und Fehler nachträglich schneller und besser nachvollzogen und behoben werden. Unabsichtlich durchgeführte Änderungen können außerdem rückgängig gemacht werden.
Überprüfung erstellter Datensicherungen;
Erstellte Datensicherungen werden regelmäßig auf ihre Integrität und Wiederherstellbarkeit hin überprüft. Hierfür werden zufällig ausgewählte Daten von einem zufällig ausgewählten Zeitpunkt testweise aus einer Datensicherung wiederhergestellt und mit den Originaldateien verglichen. So können unbrauchbare Datensicherungen oder Fehler im Backup- bzw. Wiederherstellungssystem frühzeitig erkannt und behoben werden.
Verwendung einer Firewall;
Im gesamten Unternehmensnetzwerk kommt eine Firewall zum Einsatz, die darin

betriebene Arbeitsplatzrechner und Server vor unerwünschten Netzwerkzugriffen schützt. Die Firewall-Firmware wird regelmäßig aktualisiert und die angelegten Firewall-Richtlinien in diesem Zuge überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.
Verwendung und regelmäßige Aktualisierung eines Spamfilters;
Um Kunden deren Mitarbeiter, für die wir im Rahmen unserer Dienstleistungen auch das E-Mail-Hosting übernehmen, vor Spam-E-Mails und Phishing-E-Mails zu schützen, kommen spezielle Spamschutzlösungen auf den von uns genutzten Mailservern zum Einsatz. Die zur Erkennung von Spam- und Phishing-E-Mails notwendigen Definitionen und Regeln werden regelmäßig aktualisiert. Um die korrekte Funktion des eingesetzten Spam-Filters sicherzustellen, erfolgt der regelmäßige Scan einer speziellen Testdatei, die von allen aktuellen Spamschutzlösungen erkannt wird.
Verwendung und regelmäßige Aktualisierung eines Virenscanners;
Eingehende E-Mails sowie Arbeitsplatzrechner werden durch einen Virenscanner vor den Auswirkungen von schädlichen Dateien geschützt. Die zur Erkennung von aktuellen Bedrohungen notwendigen Definitionen und Regeln werden regelmäßig aktualisiert. Als gefährlich eingestufte Dateien oder E-Mails werden in einen separaten Quarantäne-Ordner verschoben. Die Wiederherstellung von Dateien aus dem Quarantäne-Ordner ist nur nach vorheriger Freigabe durch ausgewählte Mitarbeiter möglich. Um die korrekte Funktion des eingesetzten Virenscanners sicherzustellen, erfolgt der regelmäßige Scan einer speziellen Testdatei, die von allen aktuellen Virenschutzlösungen erkannt wird.

4 Weitere Maßnahmen

4.1 Datenschutz-Managementsystem

Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert sein.
Beim Auftragnehmer umgesetzte Maßnahmen:
Dokumentation von datenschutzrelevanten Zwischenfällen;
Datenschutzrelevante Zwischenfälle, bei denen nicht ausgeschlossen werden kann, dass personenbezogene Daten gelöscht oder an unberechtigte Dritte weitergeleitet wurden, werden umfassend dokumentiert. Die Unterlagen dienen zum einen einer lückenlosen Kommunikation an die Datenschutzbehörden sowie die betroffenen Kunden, zum anderen können auf Basis dieser Informationen Verbesserungen umgesetzt werden, die ähnliche Vorfälle zukünftig verhindern.
Jährliche Überprüfung der Wirksamkeit der ergriffenen Schutzmaßnahmen;
Unabhängig von zusätzlich durchgeführten externen Security-Audits, erfolgt jährlich eine innerbetriebliche Überprüfung zur Wirksamkeit der ergriffenen

technischen und organisatorischen Schutzmaßnahmen. Hierzu werden die aktuellen Schutzmaßnahmen gemeinsam mit Vertretern aller Verantwortungsbereiche beleuchtet und sofern sinnvoll entsprechende Optimierungen festgelegt.
Sichere Entsorgung von gedruckten Dokumenten;
Gedruckte Dokumente mit sensiblem Inhalt werden nicht über den normalen Papiermüll entsorgt. Stattdessen stehen für deren sichere Entsorgung spezielle Aktenvernichter bzw. abschließbare Papiersammelbehälter zur Verfügung, die von einem Spezialunternehmen (z. B. Reisswolf) nachweislich vernichtet und entsorgt werden.
Sicheres Löschen nicht mehr benötigter Daten;
Nicht mehr benötigte Daten, wie zum Beispiel veraltete Kunden- sowie Projektdaten oder Daten aus Test- bzw. Entwicklungsumgebungen, werden gelöscht, sobald diese nicht mehr für die jeweilige Vertragserfüllung benötigt werden. Die Löschung erfolgt unter Zuhilfenahme spezieller Löschprogramme, welche eine nachträgliche Wiederherstellung der Daten unmöglich machen.

4.2 Auftragskontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
Beim Auftragnehmer umgesetzte Maßnahmen:
Abschluss von AV-Verträgen mit Dienstleistern, Partnern und Kunden;
Mit allen Dienstleistern, Partnern und Kunden, mit denen ein Austausch sowie eine Verarbeitung von personenbezogenen Daten erfolgen, wird ein Vertrag zur Auftragsdatenverarbeitung (AV-Vertrag) gemäß Art. 28 DSGVO geschlossen. In dem AV-Vertrag werden u. a. die folgenden Aspekte zwischen den beiden Vertragspartnern geregelt: “Anwendungsbereich und Verantwortlichkeit”, “Gegenstand und Dauer des Auftrages”, “Beschreibung der Verarbeitung, Daten und betroffener Personen”, “Technische und organisatorische Maßnahmen zum Datenschutz”, “Berichtigung, Einschränkung und Löschung von Daten”, “Pflichten des Auftragnehmers”, “Rechte und Pflichten des Auftraggebers”, “Wahrung von Rechten der betroffenen Person”, “Kontrollbefugnisse”, “Unterauftragsverhältnisse”, “Datengeheimnis und Geheimhaltungspflichten”, “Haftung” und “Informationspflichten, Schriftformklausel, Rechtswahl”. Der AVVertrag wird von beiden Vertragsparteien in schriftlicher oder alternativ in digitaler Form geschlossen. Beide Vertragsparteien verpflichten sich zudem, unverzüglich über relevante Änderungen zu informieren, so dass der AV-Vertrag entsprechend geändert und erneut abgeschlossen werden kann.
Aufklärung von Kunden zum Thema Datenschutz;
Nach Auftragserteilung klären wir Kunden über die von uns ergriffenen

Maßnahmen zum Datenschutz auf und binden diese so gut wie möglich in die entsprechenden Prozesse mit ein. Falls notwendig, empfehlen und installieren wir beim Kunden entsprechende Anwendungen, um einen optimalen Schutz personenbezogener Daten auch Kundenseite zu ermöglichen. So soll ein gleichermaßen hohes Sicherheitsniveau bei beiden Vertragspartnern sichergestellt werden.
Auswahl geeigneter Dienstleister und Partner unter Datenschutzaspekten;
Bei der Beauftragung von Dienstleistern und Partnern erfolgt vorab ein Vergleich möglicher Anbieter unter Datenschutzaspekten. Hierzu holen wir je nach Art und Umfang des Auftrags Informationen zur Verarbeitung von personenbezogenen beim jeweiligen Anbieter ein. Bewertet werden Aspekte wie die Übermittlung von Daten, deren konkrete Verarbeitung sowie die getroffenen technischen und organisatorischen Schutzmaßnahmen. Eine Zusammenarbeit erfolgt ausschließlich mit Dienstleistern und Partnern, die das geforderte Datenschutzniveau glaubhaft sicherstellen können.
Kommunikation von Verhaltensrichtlinien zum Thema Datenschutz an alle Mitarbeiter;
Bei Eintritt in das Unternehmen werden alle wesentlichen Verhaltensrichtlinien zum Thema Datenschutz in schriftlicher wie persönlicher Form an neue Mitarbeiter kommuniziert. Neben unserem grundsätzlichen Verständnis vom Umgang mit personenbezogenen Daten vermitteln wir auch das notwendige Wissen zur korrekten Anwendung aller technischen und organisatorischen Datenschutzmaßnahmen.
Regelmäßige Unterweisung und Fortbildung von Mitarbeitern zum Thema Datenschutz;
Unsere Mitarbeiter werden regelmäßig zu relevanten Datenschutzthemen geschult. Dabei werden sowohl Grundlagen aufgefrischt als auch aktuelle Themen sowie rechtliche Änderungen vermittelt. Neben den entsprechenden datenschutztechnischen Kompetenzen soll so eine hohe Sensibilität für den Schutz personenbezogener Daten bei allen Mitarbeitern gefördert werden.
Schriftliche Anweisungen an Dienstleister;
Sämtliche Anweisungen für die Verarbeitung von personenbezogenen Daten durch Dienstleister werden schriftlich übermittelt und im persönlichen Gespräch erläutert. Die schriftlichen Anweisungen enthalten Informationen zur Art der personenbezogenen Daten sowie zu deren datenschutzkonformer Verarbeitung. Ebenfalls schriftlich vereinbart wird, wie Daten zwischen den beiden Parteien ausgetauscht werden und was bei datenschutzrelevanten Ereignissen zu tun ist.
Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags;
Auftragsbezogene Daten mit personenbezogenen Inhalten, die zur Verarbeitung an uns übermittelt werden, werden bei Beendigung des Auftrags gelöscht, sofern diese nicht aus wichtigem Grund behalten werden müssen. Dies kann zum Beispiel dann notwendig sein, wenn sich aus dem Auftrag weitere

Folgeaufträge ergeben, für deren vertragliche Umsetzung die Daten noch einmal benötigt werden. Eine ordnungsgemäße Löschung erfolgt dann nach Abschluss des letzten Folgeauftrags.
Unterzeichnung einer Verschwiegenheitserklärung durch alle Mitarbeiter;
Alle Mitarbeiter unterzeichnen beim Eintritt in das Unternehmen eine gesonderte Verschwiegenheitserklärung. Darin verpflichten sich die Mitarbeiter, personenbezogene Daten vertraulich zu behandeln und diese ausschließlich auf Weisung ihrer Vorgesetzten zu verarbeiten. Darüber hinaus wird der Mitarbeiter über mögliche Folgen von Verstößen gegen die Vertraulichkeitsverpflichtung aufgeklärt. Alle in der Verschwiegenheitserklärung vereinbarten Punkte gelten auch über den Zeitraum der Anstellung hinaus.

Annex 3 zur Auftragsverarbeitungsvereinbarung – Genehmigte Subunternehmer

Name und ladungsfähige Anschrift des Subunternehmers	**Zweck der Beauftragung des Subunternehmers**
engine-productions GmbH Lindenstraße 20 50674 Köln	Hosting und Data Management ARDEXIA-App und Projektplaner
[…]	