Anlage zur Auftragsverarbeitung nach Art. 28 Abs. 3 EU-Datenschutzgrundverordnung (DS-GVO)

Zwischen Auftraggeber (Verantwortlicher)

(Bitte Firma und Adresse angeben)

Firma:

Name:

Straße, Hausnummer:

Postleitzahl, Ort:

und Auftragnehmer (Auftragsverarbeiter)

xdot GmbH
Feldstiege 78
48161 Münster

Einleitung

Diese Anlage gilt zum Hauptvertrag Cloud-Services und Providing-Dienstleistungen (nachfolgend Vertrag genannt). Als Vertragsbestandteil des Hauptvertrages ergänzt und konkretisiert diese Anlage die neuen Verpflichtungen der Vertragsparteien zum Datenschutz nach EU-Datenschutzgrundverordnung. Die hier genannten Bestimmungen finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

1. Gegenstand und Dauer der Verarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. In Anhang 1 dieser Anlage ist festgelegt, welche Arten von Daten und welche Kategorien betroffener Personen Gegenstand der Verarbeitung im Auftrag sind und welche Maßnahmen der Auftragsverarbeiter zu treffen hat, um die Datenschutzziele während der Auftragsverarbeitung sicherzustellen.

Diese Anlage tritt mit Unterschrift der zuletzt unterzeichnenden Partei in Kraft, frühestens jedoch mit Beginn des 25.05.2018. Ab Inkrafttreten richtet sich die Laufzeit dieser Anlage nach der Laufzeit des Vertrages.

2. Anwendungsbereich und Verantwortlichkeit

1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich ("Verantwortlicher" im Sinne des Art. 4Nr. 7 DS-GVO).

2 Der Auftragsverarbeiter ist für die Einhaltung des Datenschutzes und der Organisation der hierfür notwendigen technischen und organisatorischen Maßnahmen bei der Datenverarbeitung in seinem Verantwortungsbereich allein verantwortlich.

3 Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen. Der Auftraggeber benennt die

weisungsberechtigten Personen schriftlich oder in einem elektronischen Format (Textform). Diese sind in Anhang 1 Nr. 4 aufgeführt.

3. Pflichten des Auftragnehmers

1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 lit. a DS-GVO vor. Der Auftragnehmer 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 abgeändert wurde.

2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen, die im Anhang 2 aufgelistet sind, bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

   Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Artt. 32 bis 36 DS-GVO genannten Pflichten.

4 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben. Die Vertraulichkeitspflicht besteht auch nach Beendigung des Auftrages fort.

5 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer 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 Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen in Anhang 1 Nr. 5. Der Auftragnehmer hat dazu einen Datenschutzbeauftragten benannt, der seine Tätigkeiten gemäß Artt. 38 und 39 DS-GVO ausübt.

7 Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

8 Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

9 Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

10 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

4. Pflichten des Auftraggebers

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

2. Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftraggeber den Auftragnehmer bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

4 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen Anhang 1 Nr. 5.

5. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6. Nachweismöglichkeiten und Kontrollrechte

1 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Der Nachweis kann z.B. erfolgen durch Vorlage einer Einhaltebestätigung seines Datenschutzbeauftragten, unternehmensinterne Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung oder durch Zertifizierungen nach Art. 42 DS-GVO.

2 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt.

3 Der Auftragnehmer darf die Prüfung von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen und sonstiger vertraulicher Informationen des Auftragnehmers abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

7. Unterauftragsverhältnisse (weitere Auftragsverarbeiter)

1 Als Unterauftragsverhältnisse im Sinne dieser Anlage sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

2 Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DS-GVO in Anspruch zu nehmen. Zurzeit sind die in Anhang 3 aufgeführten Subunternehmer für den Auftragnehmer mit der Verarbeitung von personenbezogenen Daten im dort genannten Umfang beschäftigt. Der Auftraggeber erklärt sich mit deren Beauftragung einverstanden.

3 Der Auftragnehmer informiert den Auftraggeber, wenn er eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen binnen einer Frist von 2 (zwei) Wochen nach Zugang der Information über die Änderung aus wichtigem Grund gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch erheben. Der Ein-

spruch ist an die in der Änderungsmitteilung genannte Stelle des Auftragnehmers zu richten. Erfolgt binnen dieser Frist kein Einspruch, so gilt die Zustimmung zur Änderung als erteilt und Anhang 3 als entsprechend geändert. Im Falle des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung nicht zumutbar ist und eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist - die von der Änderung betroffene Leistung gegenüber dem Auftraggeber aus wichtigem Grund kündigen.

4 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus dieser Anlage dem Subunternehmer zu übertragen.

8. Informationspflichten, Schriftformklausel

1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlicher im Sinne der Datenschutz-Grundverordnung liegen.

2 Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, 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 dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Dem Vertrag und dieser Anlage gehen die Datenschutzgrundverordnung und das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU vor.

9. Haftung

Wenn eine spezifische Haftungsregelung im Vertrag vereinbart wurde, gilt diese auch für die Auftragsverarbeitung. Andernfalls haften Auftraggeber und Auftragnehmer gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

10. Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Anlage unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit der Anlage im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen, die die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Anlage als lückenhaft erweist.

11. Unterschriften

Auftraggeber (Verantwortlicher)	xdot GmbH (Auftragsverarbeiter)
Ort, Datum:	Ort, Datum:
Name in Druckbuchstaben	Name in Druckbuchstaben
Unterschrift und Stempel	Unterschrift und Stempel

Anhang 1 – Nähere Beschreibung der Verarbeitung

1. Art und Zweck der Verarbeitung

(Bitte ankreuzen)

- ☐ Der Auftragnehmer erbringt Webhosting- und technische Dienstleistungen für den Auftraggeber.
- ☐ Der Auftragnehmer betreut, verwaltet, administriert und erledigt Wartungsarbeiten für die Serversysteme des Auftraggebers als Full-Managed- oder Managed-Service.

Gegenstand dieser Anlage ist nicht die originäre Nutzung oder die Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Auf Seiten des Auftragnehmers kann der Zugriff auf personenbezogene Daten aber nicht ausgeschlossen werden, da er als Hosting Dienstleister und Administrator von Serversystemen tätig ist.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

2. Art der personenbezogenen Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten:

(Bitte ankreuzen)

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail, IP-Adressen)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ Sonstige Daten: _____

3. Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

(Bitte ankreuzen)

- ☐ Kunden des Auftraggebers
- ☐ Interessenten des Auftraggebers
- ☐ Lieferanten des Auftraggebers
- ☐ sowie jeweils die Beschäftigten i.S.v. § 26 Abs. 8 BDSG der Vorgenannten wie des Auftraggebers
- ☐ Sonstige: _____

4. Berechtige Weisungsgeber und Weisungsempfänger

Zur Erteilung von Weisungen betreffend die Auftragsdatenverarbeitung sind auf Seiten des Auftraggebers ausschließlich folgende Personen berechtigt:
(Bitte angeben)

Name	Funktion	Firma	Telefon	E-Mail

Zum Empfang von Weisungen betreffend die Auftragsdatenverarbeitung sind auf Seiten des Auftragnehmers ausschließlich folgende Personen berechtigt:

Name	Funktion	Firma	Telefon	E-Mail
Mitarbeiter der Abteilung Cloud-Services & IT	Support Team	xdot GmbH	02533 2811808 100	support@xdot.de

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

5. Datenschutzbeauftragte

Beim Auftraggeber ist als Beauftragter für den Datenschutz benannt:
(Bitte angeben, falls Sie einen Datenschutzbeauftragten haben)

Name	Firma	Telefon	E-Mail

Beim Auftragnehmer ist als Beauftragter für den Datenschutz benannt:

Name	Firma	Telefon	E-Mail

Datenschutzbeauftragter	xdot GmbH Rüdiger Niemeier Taubenheimstrasse 24 70372 Stuttgart	0711 / 5065 7305	dsb@xdot.de

Anhang 2 – Technische und organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen hat der Auftragnehmer die folgenden technischen und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Auftragnehmer verfügt über Büros und Rechenzentrum in Münster, sowie über ein Büro in Stuttgart. Unterschiedliche Maßnahmen werden im Folgenden getrennt aufgelistet. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrollmaßnahmen

Bürogebäude

- Abschließbare Räume mit Sicherheitsschlössern
- Videoüberwachung im Eingangsbereich
- Büro befindet sich im 1. Stock
- Keine Büroräume im Erdgeschoss
- Besucheraufenthalte nur mit Begleitpersonen
- Restriktive Schlüsselregelungen

Bürogebäude Münster (zusätzlich)

- Alarmanlage mit Anbindung an Sicherheitsdienst
- Haupteingang mit Schlüssel, Alarmanlage mit persönlichem Dongle, (Zutritt außerhalb der Geschäftszeiten 22:00 Uhr - 7 Uhr nur nach Anmeldung beim Sicherheitsdienst)
- Videoüberwachung innen in den Hauptfluren
- Videoüberwachung außen am Haupteingang (Eine Kamera für Zufahrt, eine für Haupteingang)
- Tor zur Büroeinfahrt (abgeschlossen außerhalb der Betriebszeit)
- Separater, abgeschlossener Serverraum im Büro. Raum ist nicht gekennzeichnet.
- Projektbüros für verschiedene Auftraggeber

Rechenzentrum

- Alarmanlage und Videoüberwachung sind vorhanden.
- Zutritt ist 3-fach gesichert mit Schlüssel, PIN und Chipkarte.
- Betreten nach telefonischer Anmeldung beim NOC
- Überwachung durch Sicherheitsdienst
- Zutritt nur für Administratoren / Mitarbeiter der Hosting Abteilung

- Zutritt für Kunden / Besucher nur in Absprache und nur in Begleitung mit Administratoren / Mitarbeiter der Hosting Abteilung
- Protokollierung des Zutritts
- Tor zur Einfahrt (immer abgeschlossen)

Zugangskontrollmaßnahmen

- Alle Rechner und Server verfügen über personalisierte Logins und Passwortschutz
- Verbot der Weitergabe von persönlichen Passwörtern
- Zugänge sind aufgaben- bzw. projektbezogen nur für die Leistungserbringer vergeben
- zentrale Firewall im Netzwerk

Bürogebäude

- Strenge Passwort Policy für Benutzerpasswörter
- Antivirus- und Schadsoftwarescanner auf jedem Arbeitsplatzrechner
- Personal Firewall auf jedem Arbeitsplatzrechner
- Festplattenverschlüsselung auf Laptops
- Eigener Passwort Safe (Keepass / Truecrypt) für jeden Mitarbeiter
- Verwendung eines Virtual Private Networks (VPN)
- Abgeschottetes Gast WLAN

Rechenzentrum

- Abhängig vom Serverbetriebssystem wird die Windows oder Linux Benutzerverwaltung verwendet
- Remotezugang zur Serverwartung nur per private/public key Verfahren, SSH oder VPN Tunnel
- Sämtliche Server verwenden immer nur eine Minimalkonfiguration und werden regelmäßig gepatched

Zugriffskontrollmaßnahmen

- Einrichtung verschiedener Berechtigungsstufen und Zuteilung derselben auf die Nutzer
- zentrale Firewall inkl. zentralem Logging
- Festlegung von Zugriffsrechten auf Datenträger
- Vernichtung von Ausdrucken durch Aktenvernichter
- Protokollierung der Vernichtung von Datenträgern
- Remote Login nur per SSH / VPN Tunnel

Trennbarkeit

- Einrichtung von Zugriffsrechten zur Mandantenfähigkeit
- Verschiedene Systeme / Datenbanken pro Auftraggeber / Projekt
- Trennung von Produktiv-, Staging-, Test- und Entwicklungssystemen
- Physikalische oder logische Trennung von Systemen

Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)

- Zugriffe auf Webapplikationen und Portale ausschließlich mit SSL / TLS.
- Transport von Daten über unsichere Netze per VPN-Tunnel, SFTP, SSH oder HTTPS Verbindungen
- Software- oder hardwaremäßige Verschlüsselung von mobilen Datenträgern
- Verschlüsselung von Daten als ZIP Dateien auf Basis von AES 256 bit
- Pseudonymisierung soweit für die Art und den Zweck der beauftragten Verarbeitung möglich und von den eingesetzten Applikationen unterstützt

2. Integrität (Art. 32 Abs. 1 lit. B DS-GVO)

Weitergabekontrolle

- Weitergabe an Dritte nur nach Weisung des Auftraggebers
- Weitergabe auf elektronischem Wege ausschließlich über sichere Kommunikationskanäle
- Anhänge von E-Mails als ZIP Dateien auf Basis von AES 256 bit verschlüsselt. Passwort per Telefon.
- Dienstanweisung « E-Mail-Nutzung » belehrt und verpflichtet die Mitarbeiter
- Versand von Datenträgern entweder verschlüsselt oder in speziellen verschlossenen Transportboxen durch einen speziellen Dienstleister.

Eingabekontrolle

- Eingaben durch Mitarbeiter nur über personalisierte Logins inkl. Logging/Protokollierung
- Dokumentation von Zuständigkeiten für die Daten
- Automatische Protokollierung bestimmter Aktionen / Systemprozesse
- Analyse von Logfiles bei Bedarf
- Konfigurationseingabe durch Admins nur über dafür vorgegebene Zugriffe und Werkzeuge

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

- Tägliches Backup mit 14 Tagen Vorhaltezeit.
- Tägliches Prüfen und Einspielen von Sicherheitsupdates, wenn diese verfügbar sind
- Notfallpläne / Meldeprozesse / Bereitschaftsdienst
- Schutzsteckdosenleisten mit Überspannungsschutz
- Brandmeldeanlage

Bürogebäude

- Automatische Updates auf Arbeitsplatzrechnern
- Videoüberwachung zur Diebstahlsicherung
- Externe Aufbewahrung von Sicherheitskopien

Bürogebäude Münster (zusätzlich)

- Eigener Serverraum mit Klimatisierung und USV. Backups maximal für 2 Monate vorhanden.
- Server im 24x7 Monitoring

Rechenzentrum

- Server im 24x7 Monitoring
- Notstromversorgung mit Dieselgenerator
- Vollklimatisierung
- Videoüberwachung zur Diebstahlsicherung
- Sicherheitsdienst
- Alarmanlage und Löschanlage
- Backup / Sicherungssystem in gesondertem Brandschutzbereich

Datenwiederherstellung nach Zwischenfällen (Art. 32 Abs. 1 lit. c DS-GVO)

- Desaster Recovery und Business Continuity Prozess
- Wiederherstellung von ganzen Servern oder einzelnen Daten möglich

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

- Managementprozesse zur regelmäßigen Prüfung der Datenschutzmaßnahmen
- Interne und technische Audits mit dem DSB und den Sicherheitsverantwortlichen
- Einbeziehung des DSB bei Verträgen und Einführung neuer Systeme

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO)

- Interne Richtlinien für Softwareentwickler bei Eigenentwicklungen
- Installationsanleitungen für Administratoren bzgl. Datenschutzvoreinstellungen
- Berücksichtigung des Datenschutzes bei Auswahl und Einsatz von Systemen / Technologien

Auftragskontrolle

- Auftragsverarbeitung nur nach Abschluss eines AV-Vertrages mit Auftraggeber
- Erteilung von Weisungen in schriftlicher oder elektronischer Form
- Schriftliche Bestätigung von mündlichen Weisungen
- Regelung zur Datenlöschung/-vernichtung bei Auftragsbeendigung
- Regelmäßige Kontrolle der Umsetzung
- Vertragliche Vereinbarung von Konventionalstrafen bei Zuwiderhandlungen möglich
- Strenge Auswahl von Dienstleistern, Prüfung und Abschluss eine AV-Vertrages mit Subunternehmern

Anhang 3 – Unterauftragsverhältnisse

Der Auftragnehmer setzt bei der Auftragsverarbeitung personenbezogener Daten für den Auftraggeber die folgenden Unterauftragnehmer mit dem jeweils beschriebenen Auftragsinhalt ein. Der Auftraggeber ist mit diesem Einsatz der Unterauftragnehmer einverstanden.

Unterauftragnehmer	Auftragsinhalt
keine	