VERTRAG ÜBER DIE VERARBEITUNG PERSONENBEZOGENER DATEN IM AUFTRAG (AUFTRAGSVERARBEITUNG)

zwischen der EASY SOFTWARE AG, Jakob-Funke-Platz 1, 45127 Essen (im Folgenden: Auftragnehmer) und dem im Hauptvertrag, der Auftragsbestätigung oder in einem Angebot näher bestimmten Kunden (im Folgenden: Auftraggeber)

Präambel

Dieser „Vertrag über die Verarbeitung personenbezogener Daten im Auftrag“ (nachfolgend Vereinbarung) konkretisiert vor allem die Verpflichtungen der Vertragsparteien zum Datenschutz im Zusammenhang mit dem Umgang des Auftragnehmers mit personenbezogenen Daten des Auftraggebers oder dessen Kunden (nachfolgend Daten). Die datenschutzrechtlichen Regelungen dieser Vereinbarung (§ 1 bis § 8) finden Anwendung auf alle Tätigkeiten bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte, Daten im Auftrage verarbeiten oder mit Daten in Berührung kommen können. Darüber hinaus werden dem Auftragnehmer im Rahmen des Hauptvertrages oder sonstiger Geschäftsbeziehungen zwischen den Parteien, vertrauliche Informationen aus dem Unternehmen des Auftraggebers zur Verfügung gestellt oder es ist nicht ausgeschlossen, dass der Auftragnehmer in den Geschäftsräumen des Auftraggebers in Kontakt mit solchen Informationen kommt.

§ 1 GEGENSTAND, ART, UMFANG, ZWECK UND DAUER DER AUFTRAGSVERARBEITUNG

1.1. Art, Umfang und Zweck der Datenverarbeitung werden in **Anlage 1** konkretisiert. Der Auftragnehmer darf nur die in Anlage 1 genannten Kategorien an Daten, der dort genannten Betroffenen zu den dort oder in einem eventuell vorhandenen Hauptvertrag genannten Zwecken verarbeiten. Das Vorhandensein eines eventuellen Hauptvertrages wird in der Anlage 1 vermerkt.

1.2. Weitere Konkretisierungen bezüglich Zweck und betroffenen Personen bezüglich abweichender Aufträge werden in zusätzlichen Anhängen zur diesem Vertrag geregelt.

1.3. Jede davon abweichende oder darüberhinausgehende Erhebung oder Verwendung von Daten ist dem Auftragnehmer untersagt, insbesondere eine Verwendung der Daten zu eigenen Zwecken.

1.4. Die Dauer dieser Vereinbarung gilt für die Dauer eines bestehenden Vertragsverhältnisses, insbesondere einem bestehenden Wartungsvertrag, oder einem eventuell vorhandenen Hauptvertrag.

§ 2 VERANTWORTLICHKEIT UND WEISUNGSRECHTE DES AUFTRAGGEBERS

2.1. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Datenschutzbestimmungen im Verhältnis zu Betroffenen und Dritten verantwortlich. Die Verantwortlichkeiten des Auftragnehmers gem. Art. 28 Abs. 10, 82, 83 und 84 der Verordnung (EU) 2016/679 (Datenschutzgrundverordnung, nachfolgend **DSGVO**) bleiben unberührt. Der Auftraggeber ist im Verhältnis der Parteien zueinander Eigentümer der Daten und Inhaber aller Rechte an den Daten.

2.2. Der Auftragnehmer verarbeitet Daten ausschließlich im Auftrag und auf dokumentierte Weisung des Auftraggebers gemäß Art. 28, 29 DSGVO, sofern der Auftragnehmer nicht durch geltendes Recht zu einer Datenverarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber dies vor der Verarbeitung mit, sofern das geltende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2.3. Die Weisungen werden anfänglich durch die Anlage 1 und diese Vereinbarung festgelegt und können vom Auftraggeber danach in Textform durch einzelne Weisungen konkretisiert, geändert, ergänzt oder ersetzt werden (Einzelweisung). In dringenden Fällen können Weisungen auch mündlich erteilt werden; eine Bestätigung der Weisung in Textform wird in diesem Fall nachgeholt. Der Auftraggeber besitzt insoweit ein umfassendes Weisungsrecht über Art, Umfang und Zweck der Verarbeitung von Daten.

2.4. Der Auftragnehmer hat Einzelweisungen zumindest in Textform zu bestätigen und zu dokumentieren.

2.5. Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen geltendes Datenschutzrecht verstößt, wird er den Auftraggeber unverzüglich darüber informieren.

§ 3 PFLICHTEN DES AUFTRAGNEHMERS

3.1. Der Auftragnehmer darf Daten ausschließlich im Rahmen des Auftrages und der Weisungen des Auftraggebers und nur im Gebiet der Europäischen Union (EU) und des Europäischen Wirtschaftsraumes (EWR) verarbeiten. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke als für die der Erfüllung des Hauptvertrages. Der Auftragnehmer darf Daten ohne vorherige Zustimmung in Schriftform durch den Auftraggeber auch nicht an Dritte oder andere Empfänger aushändigen. Hiervon ausgenommen sind Datenweitergaben an Subunternehmer nach Maßgabe von § 6 Abs. (2) zweiter Hs. bleibt unberührt.

3.2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird spätestens zu Beginn der Datenverarbeitung technische und organisatorische Maßnahmen (kurz TOM) gemäß Art 28 Abs. 3 lit. c, Art. 32 in Verbindung mit Art. 5 Abs. 1 und 2 DSGVO zum Schutz der Daten des Auftraggebers treffen und diese für die Dauer dieses Vertrages aufrechterhalten. Dabei ist der aktuelle Stand der Technik unter Berücksichtigung des Risikos zu beachten. Diese Maßnahmen werden in **Anlage 3** festgelegt. Eine Änderung der getroffenen Maßnahmen bleibt dem Auftragnehmer nachgelassen, sofern sichergestellt ist, dass das vereinbarte Schutzniveau nicht unterschritten wird. Bei wesentlichen Änderungen wird der Auftraggeber über die Änderungsabsichten des Auftragnehmers rechtzeitig vor deren Umsetzung in Textform informiert. Auf Verlangen weist der Auftragnehmer dem Auftraggeber die Einhaltung dieser Maßnahmen durch Vorlage von Dokumentationsmaterial nach.

3.3. Der Auftragnehmer stellt sicher und kontrolliert regelmäßig, dass die Datenverarbeitung in seinem Verantwortungsbereich, der etwaige Subunternehmer einschließt, im Einklang mit den Bestimmungen dieser Vereinbarung und den Weisungen des Auftraggebers erfolgt und die technisch-organisatorischen Maßnahmen eingehalten werden. Der Auftragnehmer ist verpflichtet, die Kontrollen zu dokumentieren und dem Auftraggeber diese auf Verlangen vorzulegen.

3.4. Der Auftragnehmer hat, sofern nicht bereits geschehen, alle mit der Verarbeitung der Daten beschäftigten Personen schriftlich zur Verschwiegenheit gem. DSGVO zu verpflichten, soweit diese Personen nicht bereits einer vergleichbaren, auch gesetzlichen, Verschwiegenheitspflicht unterliegen. Der Auftragnehmer hat diese Personen dabei in die wesentlichen gesetzlichen Bestimmungen über den Datenschutz einzuweisen und sie zu verpflichten, diese Bestimmungen zu beachten. Auf Verlangen des Auftraggebers wird der Auftragnehmer dies durch Vorlage der Verpflichtungserklärungen nachweisen.

3.5. Der Auftragnehmer gewährleistet, einen Datenschutzbeauftragten zu bestellen und zumindest während der Dauer dieser Vereinbarung zu beschäftigen. Der Name des Datenschutzbeauftragten sowie die Kontaktdaten können der Datenschutzerklärung auf der Homepage des Auftragnehmers (www.easy-software.com) entnommen werden.

3.6. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten des Auftraggebers aus Art. 32 DSGVO (TOM), aus Art. 33 und 34 DSGVO (Meldeverpflichtungen bei Datenpannen) und ggf. aus Art. 35 DSGVO (Datenschutz-Folgenabschätzung) sowie Art. 36 DSGVO (Konsultation der Aufsichtsbehörde).

3.7. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

§ 4 ANFRAGEN BETROFFENER

4.1. Für den Fall, dass ein Betroffener gegenüber dem Auftraggeber berechtigte datenschutzrechtliche Ansprüche geltend macht, wird der Auftragnehmer den Auftraggeber unter Berücksichtigung der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, der Erfüllung dieser Ansprüche nachzukommen.

4.2. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Geltendmachung seiner Rechte wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer wird insbesondere keine Auskunftsverlangen Betroffener beantworten.

§ 5 KONTROLLRECHTE DES AUFTRAGGEBERS

5.1. Der Auftraggeber ist berechtigt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von der Einhaltung der technischen und organisatorischen Maßnahmen durch den Auftragnehmer zu überzeugen. Der Auftraggeber dokumentiert das Ergebnis dieser Kontrollen. Hierfür kann der Auftraggeber z.B. Auskünfte des Auftragnehmers einholen oder zu den üblichen Geschäftszeiten vor Ort in den Geschäftsräumen des Auftragnehmers prüfen oder durch einen Dritten prüfen lassen.

5.2. Der Auftragnehmer gewährt dem Auftraggeber oder einem von ihm beauftragten Dritten die zur Durchführung der Kontrollen erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte und wirkt bei der Kontrolle in angemessenem Umfang aktiv mit.

§ 6 UNTERAUFTRAGSVERHÄLTNISSE („SUBUNTERNEHMER“)

6.1. Der Auftragnehmer darf geeignete Subunternehmer im Gebiet der EU oder des EWR mit der Verarbeitung von Daten im Auftrag und nach Weisung betrauen, wenn der Auftraggeber dem im Einzelfall schriftlich vor Beauftragung des Subunternehmers zugestimmt hat. Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder den Austausch von Subunternehmer informieren. Der Auftraggeber kann der Hinzuziehung oder dem Austausch von Subunternehmern nach Information durch den Auftragnehmer widersprechen. Ein Widerspruch darf nur aus wichtigem Grund erfolgen.

6.2. Dem Subunternehmer müssen die gleichen Datenschutzpflichten auferlegt werden, die in diesem Vertrag festgelegt sind. Insbesondere ist sicherzustellen, dass die geeigneten technischen und organisatorischen Maßnahmen vom Subunternehmer so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des Datenschutzrechts erfolgt. Dem Auftraggeber sind in dem Subunternehmervertrag gegenüber dem Subunternehmer unmittelbar sämtliche Kontrollrechte gem. §5 im Sinne eines echten Vertrages zugunsten Dritter einzuräumen.

6.3. Der Auftraggeber kann den Auftragnehmer dazu auffordern, Auskunft über die datenschutzrelevanten Verpflichtungen des Subunternehmers zu erteilen und Einsicht in die relevanten Vertragsunterlagen zu gewähren.

6.4. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Subunternehmers.

6.5. Die in der **Anlage 2** aufgelisteten Subunternehmer gelten als genehmigt.

6.6. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

§ 7 BESONDERE PFLICHTEN DES AUFTRAGNEHMERS BEI „DATENPANNEN“

7.1. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen datenschutzrechtliche Vorschriften oder diese Vereinbarung, wenn Anhaltspunkte dafür bestehen, dass Daten unrechtmäßig verarbeitet worden sind. § 3 Abs. (6) bleibt unberührt. Der Auftragnehmer trifft außerdem die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen.

7.2. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenzverfahren 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 liegen.

§ 8 RÜCKGABE BZW. LÖSCHUNG VON DATENTRÄGERN BZW. DATEN

8.1. Der Auftragnehmer berichtigt, löscht oder sperrt die Daten unverzüglich, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Löschung von Daten bzw. Vernichtung von Datenträgern übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern dies nicht bereits einem eventuellen Hauptvertrag vereinbart ist. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung zur Löschung nicht erforderlich. Gesetzliche Aufbewahrungsverpflichtungen bleiben unberührt.

8.2. Der Auftragnehmer hat Daten nach Vertragsbeendigung nach Wahl des Auftraggebers zu löschen und/oder zurückzugeben, es sei denn, der Auftragnehmer ist zu einer Speicherung aufgrund anderer Vorschriften verpflichtet. Der Auftragnehmer hat an den Daten kein Zurückbehaltungsrecht, es sei denn, sein Gegenanspruch ist rechtskräftig festgestellt oder unbestritten.

§ 9 SCHRIFTFORMKLAUSEL, VERHÄLTNIS ZUM HAUPTVERTRAG, RECHTSWAHL

9.1. Änderungen und Ergänzungen dieser Vereinbarung bedürfen einer schriftlichen Vereinbarung. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

9.2. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung den Regelungen eines eventuell bestehenden Hauptvertrages vor.

9.3. Es gilt deutsches Recht.

ANLAGE 1

ZWECK, ART UND UMFANG DER DATENVERARBEITUNG, ART DER DATEN UND KREIS DER BETROFFENEN

- Installation von Software beim Auftraggeber
- Wartung und Support der Installation bei Auftraggeber
- Fernwartung der Installation beim Auftraggeber

ART UND UMFANG DER VERARBEITUNG

- Zugriff auf Daten im Wege des Remote-Zugriffs
- Zwischenspeicherungen beim Remote-Zugriff
- Anzeigenlassen von Daten im Wege des Remote-Zugriffs
- Aufnahme der Störungen des Auftraggebers in einem Ticketsystem
- Führung einer Projektakte bezüglich der Installation des Auftraggebers.
- Zugriff des Auftraggebers auf das Extranet zur Information.

ART DER DATEN

- Vor- und Zunamen
- Geburtsdaten
- Anschriften
- E-Mail-Adressen
- Telefonnummern
- IP-Adressen
- Personalakten

KREIS DER BETROFFENEN

- Kunden des Auftraggebers
- Mitarbeiter des Auftraggebers
- Potentielle Kunden des Auftraggebers und Interessenten
- Lieferanten des Auftraggebers

ANLAGE 2

IM VORAUS GENEHMIGTE UNTERAUFTRAGNEHMER

- EASY SOFTWARE Deutschland GmbH, Jakob-Funke-Platz 1, 45127 Essen, Consulting und Vertrieb
- OTRIS Software AG in Dortmund, Königswall 21, 44137 Dortmund, 3rd Level Support für Documents
- CTO Balzuweit GmbH, Lautlinger Weg 3, 70567 Stuttgart, 3rd Level Support für Capture Plus
- I.R.I.S. AG, Heusstraße 23, 52078 Aachen, 3rd Level Support für xTract
- friendWorks GmbH, Theresienplatz 31, 94315 Straubing, Consulting
- Vodafone GmbH, Ferdinand-Braun-Platz 1, 40549 Düsseldorf, Support für Microsoft 365
- SAP Deutschland SE & Co.KG, Rosenthaler Straße 30, 10178 Berlin, ERP System Sap ByD
- KAMP Netzwerkdienste GmbH, Vestische Str. 89−91, 46117 Oberhausen, Colocation und Hosting
- TeamViewer Germany GmbH, Jahnstr. 30, 73037 Göppingen, Fernwartungssoftware

ANLAGE 3

TECHNISCH ORGANISATORISCHE MAßNAHMEN

VERTRAULICHKEIT
(d.h. Daten sind für Unberechtigte nicht zugänglich)

RICHTLINIEN:
- Anhand von Datenschutzrichtlinien ist geregelt, wie mit personenbezogenen Daten im konkreten Fall umzugehen ist.
- Im Rahmen der IT-Sicherheitsrichtlinien ist der sichere Umgang mit Soft- und Hardware definiert sowie die einzuhaltenden Sicherheitsmaßnahmen

SCHULUNG:
- Beschäftigte erhalten regelmäßig Schulungen zum Datenschutz und zur Informationssicherheit.

ZUTRITTSKONTROLLE:
(verhindert, dass Unbefugte räumlich Zutritt zu den Verarbeitungsanlagen/-räumen personenbezogener Daten oder sonstigen personenbezogenen Unterlagen, z. B. Akten oder Datenträgern erhalten)

- Die Zutrittskontrolle zu den Gebäuden oder externen Büros wird entweder über Karten oder aber über Schlüssel gewährt.
- Karten sind mit einem Bild versehen ohne die Nennung des Firmennamens.
- Der Zugang zum internen Rechenzentrum ist mit einer zusätzlichen Sicherung versehen. Nur Mitarbeiter mit dem entsprechenden Recht dürfen diesen Bereich betreten.
- Wir nutzen ein externes Rechenzentrum mit ISO 27001 Zertifizierung. Ein Vertrag zur Auftragsdatenverarbeitung wurde abgeschlossen.Bei externen Rechenzentren achten wir auf eine ISO 27001 Zertifizierung und effektive Maßnahmen zur Zutrittskontrolle
- Besucher der Hauptstelle müssen sich anmelden und bekommen einen Besucherausweis. In den Außenstellen müssen diese sich bei einem Mitarbeiter melden, so dass eine Kontrolle stattfindet. Gemäß IT-Sicherheitsrichtlinie dürfen sich Besucher nicht unbegleitet im Gebäude aufhalten.
- Sensible Datenträger und Papierakten werden in abschließbaren Schränken aufbewahrt.

ZUGANGSKONTROLLE / BENUTZERKONTROLLE:
(verhindert, dass Unbefugte die DV-Systeme in denen personenbezogene Daten verarbeitet werden nutzen können, z. B. User/Passwort-Regelung)

- Der Zugriff auf DV-Anwendungen erfordert eine personalisierte Anmeldung mit dedizierten Benutzerrechten.
- Passwörter müssen eine Länge von 12 Zeichen haben und sollen Groß- und Kleinbuchstaben sowie Zahlen beinhalten.
- Die Speicherung von Passwörtern erfolgt gehasht.
- Die Anzahl der Anmeldeversuche an der Domäne ist begrenzt.
- Nicht mehr genutzte Benutzerkonten werden umgehend deaktiviert.
- Ein Zugriff auf Unternehmensressourcen ohne eine Authentifizierung ist nicht möglich.

ZUGRIFFSKONTROLLE / SPEICHERKONTROLLE / DATENTRÄGERKONTROLLE:
(gewährleistet, dass Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten und Funktionen zugreifen können, z. B. durch Rollen-/Berechtigungskonzepte)

- Als Basis für die Rechtevergabe wird ein Active Directory von Microsoft verwendet. Hier werden über Gruppenzuordnungen die Rechte auf die einzelnen Ressourcen des Netzes vergeben. Wenn möglich werden andere Softwareprodukte an das AD gekoppelt. In der Regel bieten alle eingesetzten Produkte die Möglichkeit der Unterscheidung der Rechte nach Erstellen, Lesen, Schreiben und Löschen.
- Rechte an Ressourcen werden nur nach Notwendigkeit vergeben.
- Rechte müssen über das Ticketsystem des internen IT-Support angefordert werden. Diese werden nur nach Bestätigung durch den entsprechenden Vorgesetzten vergeben.
- Alle Datenträger werden gemäß IT-Sicherheitsrichtlinie verschlüsselt. Durch Löschen der entsprechenden Key werden die Daten auch auf SSD Datenträgern sicher gelöscht. Bei Veräußerung oder Außerbetriebnahme werden Datenträger noch einmal gelöscht.
- Zur Vernichtung von Papierunterlagen stehen Papierschredder zur Verfügung. Bei größeren Mengen wird zu Vernichtung ein Container eines entsprechend zertifizierten Dienstleisters angefordert.

TRENNUNGSGEBOT / TRENNBARKEIT:
(gewährleistet, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können, z. B. durch System- oder Mandantentrennung, etc.)

- Zur Trennung der Daten werden ausschließlich Systeme eingesetzt, die die Trennung entweder durch einen Mandanten, logische Trennbarkeit aufgrund von Datensatzkennzeichen und oder durch Vergabe von Rollen und damit verbundenen Berechtigungen realisieren.

AUFTRAGSKONTROLLE:
(gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können)

- Die Erhebung, Verarbeitung, Berichtigung und Löschung der Daten erfolgt streng gebunden an Auftrag und Einzelweisungen des Auftraggebers gemäß der hier getroffenen vertraglichen Vereinbarungen.
- Unterauftragnehmer werden unter besonderer Berücksichtigung von Art. 28 DSGVO und somit der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt.
- Aufträge und damit verbundene Auftragsverarbeitungsvereinbarungen werden schriftlich erteilt.
- Verträge mit Unterauftragnehmern in Drittstaaten werden unter Anwendung der EU-Standardvertragsklauseln abgeschlossen.
- Beschäftigte sowie eingesetzte Unterauftragnehmer, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, sind schriftlich auf das Datengeheimnis bzw. zur Vertraulichkeit verpflichtet.

VERSCHLÜSSELUNG:
(gewährleistet, dass auf besonders sensible personenbezogene Daten nur mit Kenntnis eines spezifischen Entschlüsselungscodes zugegriffen werden kann.)

- Notebooks, Smartphones, USB Sticks und sonstige mobile Datenträger auf denen sich Daten des Auftraggebers befinden, sind verschlüsselt. Dazu verwenden wir Bitlocker unter Windows oder Filevault unter MacOsX.
- Für die Erstellung von verschlüsselten Containern verwenden wir die OpenSource Applikation Veracrypt. Dies kann von jedem MA bei Bedarf installiert werden.
- Bei der Verwendung von Webapplikationen, sorgen wir für die ausschließliche Ansprechbarkeit über HTTPS.
- Wir stellen den MA ein VPN zur Verfügung, damit diese bei außer Haus Einsätzen eine sichere Netzwerkverbindung nutzen können.

ANONYMISIERUNG / PSEUDONYMISIERUNG:

(gewährleistet, dass die Identifikation einer bestimmten Person vermieden bzw. erschwert wird, sofern eine Identifikation dieser Person für den Zweck der Verarbeitung der personenbezogenen Daten nicht zwingend erforderlich ist – „Datenvermeidung“.)

- Wo immer sinnvoll und möglich (z. B. für Statistiken) werden personenbezogene Daten pseudonymisiert oder anonymisiert.

INTEGRITÄT

(d.h. Daten können nicht verfälscht werden)

TRANSPORTKONTROLLE / ÜBERTRAGUNGSKONTROLLE (WEITERGABEKONTROLLE):

(gewährleistet, dass personenbezogene Daten bei der Weitergabe, also Übertragung oder ihres Transports nicht unbefugt gelesen, kopiert verändert oder entfernt werden können, z. B. durch Transportverschlüsselung)

- Der Zugriff auf Web-basierte DV-Systeme in denen personenbezogene Daten verarbeitet werden ist nur über verschlüsselte Kommunikationsverbindungen (https und TLS) möglich.
- Der Fernzugriff auf das interne IT-Netzwerk von IT-Systemen außerhalb des hausinternen Netzes erfolgt ausschließlich mittels VPN-Technologie.
- Der ein- und ausgehende Datenverkehr wird mittels einer Firewallapliance überwacht. Zeitpunkt, Inhalt, Empfänger sowie der veranlassende Sender von Datenübertragungen werden protokolliert.
- Beim physischen Transport personenbezogener Daten werden sichere Transportbehälter/-verpackungen eingesetzt. Transportpersonal und –fahrzeuge (z. B. bei Kurierdiensten) werden sorgfältig ausgewählt.
- Zum Transport verwendete Datenträger müssen verschlüsselt werden.

EINGABEKONTROLLE:

(gewährleistet, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind, . B. durch Protokollierung)

- Eingaben in und Veränderungen an relevanten Anwendungssystemen werden mittels Protokollen/Logfiles aufgezeichnet und überwacht. Dabei sind die Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten (Inhalt und Zeitpunkt der Änderung) sowie der Ausführende (durch individuelle Benutzernamen, nicht Benutzergruppen) gewährleistet.

VERFÜGBARKEIT, BELASTBARKEIT / WIDERSTANDSFÄHIGKEIT, WIEDERHERSTELLBARKEIT

(d.h. Daten stehen zur Verfügung, wenn sie gebraucht werden)

VERFÜGBARKEITSKONTROLLE:

(gewährleistet, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind, z. B. durch Brandschutzmaßnahmen, etc.)

- Die Server sind über eine USV gegen Stromausfall abgesichert.
- Wir verwenden Virtualisierungslösungen für Server, so dass bei Ausfall einzelner Maschinen ein Weiterbetrieb auf einer anderen Instanz möglich ist.
- Die Serverräume sind klimatisiert.
- Es kommen moderne Brandschutz- und -meldeanlagen zum Einsatz. Automatische Gaslöschanlagen verhindern weitergehende Schäden.

BELASTBARKEIT (IM SINNE VON: WIDERSTANDSFÄHIGKEIT):

(gewährleistet, dass die IT-Systeme widerstandsfähig gegen Angriffe sind)

- Alle DV-Systeme auf denen die vereinbarten Services laufen, sind durch eine Firewall vor Zugriffen von außen geschützt.
- Updates müssen bei Verfügbarkeit zeitnah in alle Systeme eingespielt werden. Automatische Updatemechanismen sind bevorzugt.
- Alle Systeme sind mit Anti-Viren-Software ausgestattet.
- Einsatz von Intrusion-Detection-Systemen in der zentralen Firewall.
- Das Antwortzeitverhalten wesentlicher Systeme wird regelmäßig überwacht, um außergewöhnliche Belastungssituationen (z. B. durch Cyberangriffe) und damit einen möglichen Ausfall der Systeme frühzeitig identifizieren zu können.

WIEDERHERSTELLBARKEIT:

(gewährleistet, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können)

- Die regelmäßig in verschiedenen Generationen automatisch erzeugten Datensicherungen werden redundant in verschiedenen Gebäudeteilen verwahrt.

SICHERSTELLUNG DER DAUERHAFTEN WIRKSAMKEIT DER GETROFFENEN MAßNAHMEN:

(gewährleistet, dass getroffene Maßnahmen regelmäßig überprüft und bei Bedarf angepasst werden)

- Die ordnungsgemäße Einhaltung und Durchführung der hier aufgeführten Maßnahmen wird manuell und/oder DV-technisch protokolliert (Nachweispflicht).
- Alle hier aufgeführten Maßnahmen unterliegen einem regelmäßigen Review und werden kontinuierlich verbessert.

Zusätzliche Anlage 1 zum Standardvertrag über die Verarbeitung personenbezogener Daten im Auftrag (SaaS)

Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kreis der Betroffenen

Zweck der Verarbeitung	▪ Bereitstellung von EASY-Produkten als Software as a Service (SaaS) / Managed Application Hosting ▪ Betrieb und Pflege von EASY-Produkten als SaaS / Managed Application Hosting. ▪ Erstellung von Sonderkonfigurationen für EASY-Produkte im Rahmen der Bereitstellung als SaaS / Managed Application Hosting
Art und Umfang der Verarbeitung	▪ Zugriff auf Daten im Wege des Remote-Zugriffs ▪ Zwischenspeicherungen beim Remote-Zugriff ▪ Anzeigenlassen von Daten im Wege des Remote-Zugriffs ▪ Beseitigung von Störungen und Wartung im Rahmen von SaaS oder Managed Application Hosting ▪ Führung einer Implementierungs-/Customizing-Dokumentation oder Projektakte bezüglich System, Instanz, Tenant, Mandant oder Installation des Kunden (=Auftraggeber).
Art der Daten	▪ Die Systeme werden dem Kunden von EASY ohne personenbezogene Daten zur Verfügung gestellt. Der Kunde ist für die DSGVO-konforme Datenverarbeitung zuständig und darf personenbezogene Daten nur speichern und verarbeiten, wenn ein Erlaubnistatbestand gemäß DSGVO, BDSG oder eines Spezialgesetzes vorliegt.
Kreis der Betroffenen	▪ Kunden des Auftraggebers ▪ Mitarbeiter des Auftraggebers ▪ Potentielle Kunden des Auftraggebers und Interessenten ▪ Lieferanten des Auftraggebers ▪ Sonstige vom Auftraggeber beauftragte Datenverarbeiter

Im Voraus genehmigte Unterauftragnehmer

- virtion GmbH, Südring 11, 33647 Bielefeld -
  Bereitstellung und Betrieb der Server- und Rechenzentrumsinfrastruktur

Technisch-Organisatorische Maßnahmen der virtion GmbH

Definition von Verantwortlichkeiten sowie der regelmäßigen Überprüfung und Dokumentation der zugehörigen Maßnahmen sind in den internen Richtlinien zur Dokumentenverwaltung, zum Wertemanagement und zur Compliance des zertifizierten Informationssicherheits-Managementsystems (ISMS) der virtion GmbH festgelegt.

Anhang Datenschutz- und Sicherheitskonzept / Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO

Dieser Anhang beschreibt die technischen und organisatorischen Maßnahmen des Datenschutz- und Sicherheitskonzepts gemäß Artikel 32 der Datenschutz-Grundverordnung (DS-GVO) als Teil des zertifizierten Informationssicherheits-Managementsystems (ISMS) der virtion GmbH, die in Verbindung mit den vom Auftragnehmer bereitgestellten bzw. durchgeführten Leistungen im Rahmen der Auftragsverarbeitung einzuführen und aufrechtzuerhalten sind.

§ 1 Pseudonymisierung

REGELUNGSGEGENSTAND:
Maßnahmen, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:
Es erfolgt eine automatische Pseudonymisierung bzw. Anonymisierung von IP-Adressen im Rahmen der Erfassung von Zugriffsdaten auf Systemdienste, die zu Zwecken der Aufrechterhaltung der Informationssicherheit, der Systemsicherheit und der Systemstabilität sowie zu Zwecken der Optimierung sowie zur statistischen Erfassung der Nutzung von Diensten ausgewertet und analysiert werden. Eine darüberhinausgehende Verarbeitung personenbezogener Daten, die eine sinnvolle Pseudonymisierung zulassen, erfolgt nicht. Regelungen zur entsprechenden Identifizierung und Klassifizierung von Daten, der resultierenden Vorgehensweise, der Definition von Verantwortlichkeiten sowie der regelmäßigen Überprüfung und Dokumentation der zugehörigen Maßnahmen sind in den internen Richtlinien zur Dokumentenverwaltung, zum Wertemanagement und zur Compliance des zertifizierten Informationssicherheits-Managementsystems (ISMS) der virtion GmbH festgelegt.

§ 2 Verschlüsselung

REGELUNGSGEGENSTAND:
Maßnahmen, um das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbefugte Offenlegung von bzw. unbefugten Zugang zu den im Auftrag verarbeiteten Daten zu reduzieren.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:
Interne Richtlinien zur Kryptographie sowie zur Verschlüsselung im Rahmen der Zugangs- und Zugriffskontrolle, der Informations-übertragung und der Dokumentenverwaltung (zertifiziert nach ISO/IEC 27001 im Rahmen des ISMS der virtion GmbH), darin enthalten sind Regelungen zu technischen und organisatorischen Maßnahmen zur Auswahl kryptographischer Verfahren und Implementierungen, zum Einsatzbereich kryptographischer Systeme (z.B. gemessen am Sicherheitsbedarf) sowie Regelungen zur Schlüsselverwaltung (darunter Regelungen zur Vorgehensweise der Erzeugung, Trennung, Verteilung, Speicherung, Zugriffs- und Vertreterregelung, Gültigkeitsdauer und Vernichtung kryptographischer Schlüssel). Es erfolgt eine regelmäßige, mindestens jährlich durchgeführte Überprüfung und Dokumentation der eingesetzten kryptographischen Verfahren und Systeme, der Art der Speicherung der Schlüssel sowie der jeweiligen Gültigkeitsdauer der Schlüssel im Rahmen des kontinuierlichen Verbesserungsprozesses des ISMS.

Die internen Richtlinien zur Zugangs- und Zugriffskontrolle, zur Informationsübertragung und zur Dokumentenverwaltung bzw. zum Wertemanagement enthalten Regelungen zu technischen und organisatorischen Maßnahmen zur Beschränkung des Zugangs zu internen Systemen über verschlüsselte VPN-Zugänge mit Zwei-Faktor-Authentifizierung (einschließlich der Erzeugung, Trennung des resultierenden Zugangs über VLANs sowie Rollenkonzepte, zeitlich begrenzter Gültigkeitsdauer sowie Deaktivierung des Zugangs), Zugang zu Systemen ausschließlich über kryptografisch verschlüsselte Verbindungen (z.B. ssh), Absicherung des Zugriffs auf vertrauliche Daten auf Arbeitsplatzrechnern sowie mobilen Endgeräten über zwingend erforderliche Vollverschlüsselung aller Datenträger (Festplatten sowie alle anderen Datenträger), ausschließlich verschlüsselte Übertragung vertraulicher Informationen über das Internet sowie ausschließlich verschlüsselte Speicherung vertraulicher Daten auf zu transportierenden physischen Medien.

Die interne Richtlinie zum Incident Management regelt u.a. die Vorgehensweise im Falle einer Entdeckung von Schwachstellen in Verschlüsselungsverfahren oder -systemen und enthält detaillierte Beschreibungen von Maßnahmen, Vorgehensweisen und Verantwortlichkeiten zur Dokumentation und Meldung entsprechender Informationssicherheitsschwachstellen. Die Richtlinie sowie die sich daraus ergebenden Dokumentationspflichten sind Bestandteil regelmäßiger (mindestens jährlicher) interner und externer Audits des ISMS der virtion GmbH.

§ 3 Vertraulichkeit

Maßnahmen, um das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbefugte Offenlegung von bzw. unbefugten Zugang zu den im Auftrag verarbeiteten Daten zu reduzieren.

Physikalische Sicherheit

REGELUNGSGEGENSTAND:
Maßnahmen, um Unbefugten den Zutritt zu den Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten), mit denen Daten im Auftrag verarbeitet werden, zu verwehren.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:
Zu den technischen und organisatorischen Maßnahmen zur physikalischen Sicherheit insbesondere der Datenverarbeitungssysteme und -anlagen im von der virtion GmbH über ihren Dienstleister Filoo GmbH genutzten Rechenzentrum der Telehouse Deutschland GmbH wird auf die bestehenden Sicherheitsvorschriften für Kunden und Fremdfirmen im Auftrag des Kunden verwiesen, die Teil der ISO27001-Zertifizierung des Rechenzentrums der Telehouse Deutschland GmbH sind und die bei der virtion GmbH eingesehen werden können. Darin geregelt sind u.a. Zweck, Geltungsbereich, Verantwortlichkeiten, Koordinierung von Arbeiten, Verhalten von Mitarbeitern, Ansprechpartner, Werkschutzvorschriften, Zugangsregelungen und Kontrollen, Sicherheitsregelungen zur Videoüberwachung, zum Brandschutz, zur Alarmierung und zur Gebäuderäumung.

Zu den konkreten Maßnahmen zur Zutrittskontrolle zum Rechenzentrum gehören:

- Personenkontrolle beim Empfang mit Protokollierung
- elektronisches Zutrittskontrollsystem mit Protokollierung
- Richtlinien zur Begleitung und Kennzeichnung von Besuchern
- personalisierte Schlüsselausgabe an Mitarbeiter mit Protokollierung
- Bestreifung des Geländes durch Sicherheitsdienst mit Protokollierung
- Videoüberwachung des Gebäudes im Innen- und Außenbereich
- Einbruchmeldeanlage mit Bewegungs- und Kontaktmeldern

Die Überprüfung und Dokumentation der technischen und organisatorischen Maßnahmen zur physikalischen Sicherheit des Rechenzentrums ist Gegenstand der internen Richtlinie zu Lieferantenbeziehungen und damit Bestandteil regelmäßiger (mindestens jährlicher) interner und externer Audits des ISMS der virtion GmbH.

Die interne Richtlinie zur Zutrittskontrolle (zertifiziert nach ISO/IEC 27001 im Rahmen des ISMS der virtion GmbH) enthält Regelungen zu technischen und organisatorischen Maßnahmen zur Sicherung des Zutritts zum Bürostandort und zu den Mitarbeiterbüroräumen bzw. den Arbeitsplätzen der virtion GmbH über Schließanlagen sowie über die individuelle und dokumentierte Ausgabe von Sicherheitsschlüsseln und PIN-Codes an die Mitarbeiter der virtion GmbH, die Gebäudesicherung über Türsicherungen und Bewegungsmelder der Alarmanlage sowie Regelungen zum Besuch betriebsfremder Personen am Bürostandort.

Zu den konkreten Maßnahmen zur Zutrittskontrolle zum Bürostandort gehören:

- Personenkontrolle beim Empfang
- elektronisches Zutrittskontrollsystem mit Protokollierung
- Richtlinien zur Begleitung von Besuchern
- personalisierte Schlüsselausgabe an Mitarbeiter mit Protokollierung
- Einbruchmeldeanlage mit Bewegungs- und Kontaktmeldern

Die Überprüfung und Dokumentation der technischen und organisatorischen Maßnahmen zur physikalischen Sicherheit des Bürostandortes ist Bestandteil regelmäßiger (mindestens jährlicher) interner und externer Audits des ISMS der virtion GmbH.

Authentifizierung

REGELUNGSGEGENSTAND:
Maßnahmen, um zu verhindern, dass Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten) von unbefugten Dritten genutzt werden können.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:
Die interne Richtlinie zur Zugangskontrolle (zertifiziert nach ISO/IEC 27001 im Rahmen des ISMS der virtion GmbH) enthält Regelungen zu technischen und organisatorischen Maßnahmen zu Zugangskontroll-systemen, insbesondere verschlüsselte VPN-Zugänge mit Zwei-Faktor-Authentifizierung, Regelung der Kontrolle des Zugangs über Vergabe und Entzug von Benutzer-Accounts zur Authentifizierung des Zugangs zu sicherheitskritischen und vertraulichen Systemen, Zwei-FaktorAuthentifizierung unter Verwendung von Public-Key-Verfahren beim Zugang zu Servern, zum Passwortmanagement und zur Benutzung von Passwörtern, Regelungen des Zugangs zu Arbeitsplatzrechnern durch Absicherung mit Accounts mit sicheren Passwörtern sowie Notwendigkeit einer erneuten Anmeldung durch automatische Sperrung auch bei nur kurzfristiger Abwesenheit. Die Überprüfung und Dokumentation der technischen und organisatorischen Maßnahmen zur Zugangskontrolle ist Bestandteil regelmäßiger (mindestens jährlicher) interner und externer Audits des ISMS der virtion GmbH.

Zu den konkreten Maßnahmen zur Zugangskontrolle gehören:

- zentrale Benutzer-/Passwort-Datenbank zur Zugangskontrolle der Mitarbeiter des Auftraggebers und des Auftragnehmers
- Verwendung von Zwei-Faktor-Authentifizierung für die Zugangskontrolle
- Zugriff besteht nur für Mitarbeiter des Auftraggebers und des Auftragnehmers
- Richtlinien zur Verwendung von Passwörtern (z.B. Mindestlänge, verwendete Zeichen etc.)
- Einsatz von Anti-Malware-Software
- Einsatz von Firewalls

Berechtigungskonzept

REGELUNGSGEGENSTAND:
Maßnahmen zur Sicherstellung, dass zur Benutzung von IT-Systemen Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen dürfen. Im Auftrag verarbeitete Daten dürfen bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:
Die interne Richtlinie zur Zugriffskontrolle (zertifiziert nach ISO/IEC 27001 im Rahmen des ISMS der virtion GmbH) enthält Regelungen zu technischen und organisatorischen Maßnahmen zu Zugriffs-kontrollsystemen, zu Berechtigungskonzepten, Zugriffskontrollen über Rollenkonzepte und Rollendefinitionen, Regelung der Vergabe und des Entzug von Zugriffsrechten, Absicherung des Zugriffs durch kryptografische Maßnahmen, Regelungen zu Benutzer- und Rechtemanagement, automatische zeitliche Zugriffsbegrenzungen sowie regelmäßige Prüfung auf Korrektheit und Dokumentation von Zugängen und vergebenen Berechtigungen. Die Überprüfung und Dokumentation der technischen und organisatorischen Maßnahmen zur Zugriffskontrolle ist Bestandteil regelmäßiger (mindestens jährlicher) interner und externer Audits des ISMS der virtion GmbH.

Zu den konkreten Maßnahmen zur Zugriffskontrolle gehören:

- zentrale Benutzer-Datenbank mit verbindlicher Rollen- und Berechtigungsvergabe für Mitarbeiter des Auftraggebers und des Auftragnehmers
- Vermeidung von unberechtigten Zugriffen durch regelmäßige Sicherheitsupdates
- Protokollierung von Zugriffen auf Anwendungen (insbesondere bei Eingabe, Änderung und Löschung von Daten)
- Sichere Löschung von Datenträgern vor Wiederverwendung
- Sichere Entsorgung bzw. Vernichtung nicht mehr benötigter oder defekter Speichermedien mit Protokollierung
- Einsatz von Aktenvernichtern für physische Dokumente

Weitergabe von Daten

REGELUNGSGEGENSTAND:
Maßnahmen, um sicherzustellen, dass im Auftrag verarbeitete Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:

Die internen Richtlinien zum Wertemanagement, zur Zugriffskontrolle, zur Kryptographie, zur Netzwerksicherheit und zur Informationsübertragung enthalten Regelungen zu technischen und organisatorischen Maßnahmen zur ausschließlich verschlüsselten Übertragung vertraulicher Informationen über das Internet, zum Umgang mit mobilen Speicherlösungen sowie zur zwingend erforderlichen Vollverschlüsselung aller Datenträger (Festplatten sowie aller anderen Datenträger), zum Transport physischer Medien sowie zur ausschließlich verschlüsselten Speicherung vertraulicher Daten auf zu transportierenden physischen Medien.

Zu den konkreten Maßnahmen zur Weitergabekontrolle gehören:

- Die elektronische Übertragung vertraulicher Daten erfolgt generell verschlüsselt
- Die Speicherung vertraulicher Daten auf zu transportierenden physischen Medien erfolgt generell verschlüsselt

Die Regelungen zu resultierenden Vorgehensweisen, der Definition von Verantwortlichkeiten sowie der regelmäßigen Überprüfung und Dokumentation der zugehörigen Maßnahmen sind Bestandteil regelmäßiger (mindestens jährlicher) interner und externer Audits des ISMS der virtion GmbH.

Löschen von Daten

REGELUNGSGEGENSTAND:
Maßnahmen, um personenbezogene Daten nur so lange zu speichern, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:
Die interne Richtlinie zum Wertemanagement enthält Regelungen zu technischen und organisatorischen Maßnahmen zur Klassifizierung, zur Kennzeichnung und zum Umgang mit vertraulichen Informationen sowie zur Speicherung, zur Übertragung und zur Vernichtung von Informationen. Dies schließt die sichere Vernichtung von Daten, Dokumenten und Datenträgern sowie die Definition von Verantwortlichkeiten und Vorgehensweisen für die Löschung von Daten und die Entsorgung physischer Medien sowie die Dokumentation der Löschung und der sicheren Entsorgung ein.

Zu den konkreten Maßnahmen zum Löschen von Daten gehören:

- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung
- Datenschutzgerechte Löschung bzw. Vernichtung von Dokumenten nach Auftragsbeendigung
- Datenschutzgerechte Löschung bzw. Vernichtung von Datenträgern nach Auftragsbeendigung

Die Regelungen zu resultierenden Vorgehensweisen, der Definition von Verantwortlichkeiten sowie der regelmäßigen Überprüfung und Dokumentation der zugehörigen Maßnahmen sind Bestandteil regelmäßiger (mindestens jährlicher) interner und externer Audits des ISMS der virtion GmbH.

Mandantentrennung

REGELUNGSGEGENSTAND:
Maßnahmen, um zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeiten zu können.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:

Die internen Richtlinien zur internen Organisation, zur Betriebssicherheit und zur Netzwerksicherheit enthalten Regelungen zu technischen und organisatorischen Maßnahmen zur Trennung von Kundensystemen, zur Trennung unterschiedlicher Systemumgebungen zur Verringerung des Risikos unautorisierter oder unbeabsichtigter Zugriffe oder Änderungen verschiedener Systemumgebungen für Entwicklung, Integration, Test oder Produktion sowie von internen Systemen und Kundensystemen sowie ggf. von verschiedenen Systemen einzelner Kunden. Dies umfasst die Definition von Maßnahmen für die Trennung von Netzwerken durch geeignete technische und organisatorische Sicherheitsmaßnahmen sowie entsprechende Verantwortlichkeiten und Dokumentationsvorgaben für die Verwaltung und Kontrolle der zugrundeliegenden Netzwerke.

Zu den konkreten Maßnahmen zur Trennungskontrolle gehören:

- Die verarbeiteten Daten werden physikalisch oder logisch getrennt von anderen Daten gespeichert.
- Die Datensicherung erfolgt auf logisch und/oder physikalisch getrennten Systemen

Die Regelungen zu resultierenden Vorgehensweisen, der Definition von Verantwortlichkeiten sowie der regelmäßigen Überprüfung und Dokumentation der zugehörigen Maßnahmen sind Bestandteil regelmäßiger (mindestens jährlicher) interner und externer Audits des ISMS der virtion GmbH.

§ 4 Integrität

Maßnahmen, um das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von im Auftrag verarbeiteten Daten zu reduzieren.

Protokollierung

REGELUNGSGEGENSTAND:
Maßnahmen mittels derer nachträglich überprüft und festgestellt werden kann, ob und von wem im Auftrag verarbeitete Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:
Die internen Richtlinien zur Betriebssicherheit enthalten Regelungen zu technischen und organisatorischen Maßnahmen zur Protokollierung (Logging) und Monitoring von Ereignissen mit Bezug zur Informationssicherheit und zum Datenschutz sowie zur Bereitstellung entsprechender Belege und Protokolle bzw. Beweise, zur Benachrichtigung über unerwünschte Benutzeraktivitäten, Fehler und Ausnahmezustände, zur Protokollierung von Fernzugriffen oder Fernzugriffsversuchen, zur Anfertigung, Speicherung, Datensicherung, Schutz und regelmäßigen Prüfung entsprechender Ereignisprotokolle, zum Schutz von Einrichtungen zum Logging und Monitoring sowie resultierender Aufzeichnungen gegen Manipulationen oder unautorisierten Zugriff sowie zur Protokollierung von Aktivitäten von Systemadministratoren und Systembetreibern, ferner zu Aufbewahrungszeiten, Archivierungsvorgaben und Zugriffsbeschränkungen der gesicherten Protokollierungsdaten.

Zu den konkreten Maßnahmen zur Eingabekontrolle gehören:

- Die Daten werden vom Auftraggeber eingegeben bzw. erfasst; die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber
- Protokollierung von Zugriffen auf Anwendungen und Daten (insbesondere bei Eingabe, Änderung und Löschung der Daten)

Die Regelungen zu den entsprechenden Maßnahmen, die Definition von Verantwortlichkeiten sowie die regelmäßige Überprüfung und Dokumentation der zugehörigen Maßnahmen sind Bestandteil regelmäßiger (mindestens jährlicher) interner und externer Audits des ISMS der virtion GmbH.

§ 5 Verfügbarkeit

Maßnahmen, um das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Nichtverfügbarkeit von im Auftrag verarbeiteten Daten zu reduzieren.

Sicherstellen der Verfügbarkeit

REGELUNGSGEGENSTAND:
Maßnahmen, um im Auftrag verarbeitete Daten gegen zufällige oder mutwillig herbeigeführte Zerstörung oder Verlust zu schützen.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:
Zu den technischen und organisatorischen Maßnahmen zur Verfügbarkeit insbesondere der Datenverarbeitungssysteme und -anlagen im von der virtion GmbH genutzten Rechenzentrum der Telehouse Deutschland GmbH wird auf die bestehenden Maßnahmen verwiesen, die Teil der ISO27001-Zertifizierung des Rechenzentrums der Telehouse Deutschland GmbH sind, darunter Zugangssicherungen durch bauliche Maßnahmen, personelle Maßnahmen wie Personenkontrollen beim Empfang mit Protokollierung, elektronische Zutrittskontrollsysteme mit Protokollierung, sowie Richtlinien zur Begleitung und Kennzeichnung von Besuchern, Maßnahmen zur Ausfallsicherheit wie redundante Klimasysteme, redundante USV-Systeme für unterbrechungsfreie Stromversorgung, Brandschutzkonzept mit Rauchmeldern, automatisierte Löschanlage für Serverräume sowie zentrale Überwachung und Kontrolle aller Betriebsparameter des Rechenzentrums durch den Rechenzentrums-Betreiber bzw. der betriebenen Systeme und Dienste durch die virtion GmbH mit Alarmierung.

Weitere von der virtion GmbH umgesetzte Sicherungsmaßnahmen umfassen interne Richtlinien zur Betriebssicherheit mit Regelungen zu technischen und organisatorischen Maßnahmen und Konzepte zu Backup und Recovery mit mindestens täglicher Sicherung aller relevanten Daten, Einsatz von Schutzsoftware (Virenscanner, Firewalls, Verschlüsselung, Spam-Filter), Einsatz von Festplattenspiegelung und RAID-Systemen zur Erhöhung der Ausfallsicherheit, redundante Auslegung interner Systeme und Ressourcen, regelmäßig überprüfte Notfallpläne, regelmäßig geplante, durchgeführte und dokumentierte Notfalltests zur Überprüfung der Notfallpläne, interne Richtlinien zum Business Continuity Management, regelmäßig durchgeführte und dokumentierte Business Impact Analysen im Rahmen des Risiko-behandlungsplans, regelmäßige Analyse der Bedrohungen und Schwachstellen sowie Risikobewertungen im Rahmen des Risikomanagements als Teil des Informationssicherheits-Managementsystems.

Zu den konkreten Maßnahmen zur Verfügbarkeitskontrolle gehören:

- Backup- und Recovery-Konzept mit mindestens täglicher Sicherung aller relevanten Daten
- Einsatz von Schutzsoftware (Virenscanner, Firewalls, Verschlüsselung, Spam-Filter)
- Einsatz von Festplattenspiegelung / RAID-Systemen
- redundante Klimasysteme
- redundante USV-Systeme für unterbrechungsfreie Stromversorgung
- Brandschutzkonzept mit Rauchmeldern
- Automatisierte Löschanlage für Serverräume
- zentrale Überwachung und Kontrolle aller Betriebsparameter des Rechenzentrums (RZ-Betreiber) bzw. der betriebenen Systeme und Dienste (virtion GmbH) mit Alarmierung

Die Regelungen zu resultierenden Vorgehensweisen, der Definition von Verantwortlichkeiten sowie der regelmäßigen Überprüfung und Dokumentation der zugehörigen Maßnahmen sind Bestandteil regelmäßiger (mindestens jährlicher) interner und externer Audits des ISMS der virtion GmbH.

Zweckbindung

REGELUNGSGEGENSTAND:
Maßnahmen, um sicherzustellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden dürfen. Dies gilt insbesondere auch für die Löschung von Daten.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:
Vertragliche Regelungen zur Auftragsverarbeitung mit Kunden und Lieferanten zur Definition und Festlegung der zu verarbeitenden Daten im Rahmen der Verarbeitungstätigkeiten in Form eines Verzeichnisses, der Anwendungsbereiche und Verantwortlichkeiten, der Pflichten des Auftragnehmers (insbesondere zur Regelung der Weisungsbefugnisse des Auftraggebers, zur Erfüllung der Anforderungen des Datenschutzes durch geeignete technische und organisatorische Maßnahmen sowie zur Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit), zum Umgang mit Anfragen betroffener Personen, zu Nachweismöglichkeiten, Dokumentationspflichten und zur Durchführung von Audits durch den Auftraggeber sowie der Zulässigkeit und der Regelung des Einsatzes von Subunternehmern als weiteren Auftragsverarbeitern.

Zu den konkreten Maßnahmen zur Auftragskontrolle gehören:

- Auftraggeber und Auftragnehmer haben schriftliche Vereinbarungen zur Auftragsverarbeitung abgeschlossen.
- Der Auftragnehmer darf die Daten des Auftraggebers nur entsprechend schriftlicher Vereinbarungen und Weisungen des Auftraggebers verwenden. Insbesondere ist strikte Zweckbindung vereinbart.
- Dem Auftraggeber werden in der Vereinbarung zur Auftragsverarbeitung Vor-Ort-Kontrollrechte eingeräumt.
- Subunternehmen werden sorgfältig ausgewählt und in derselben Weise vertraglich verpflichtet, wie der Auftragnehmer durch den Auftraggeber verpflichtet ist.

§ 6 Belastbarkeit

REGELUNGSGEGENSTAND:
Maßnahmen, um das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder

unbefugter Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu im Auftrag verarbeiteten Daten aufgrund von Systemüberlastungen oder -abstürzen zu reduzieren.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:
Die internen Richtlinien zur Betriebssicherheit, zum Change Management, zum Incident Management, zum Business Continuity Management und zum Risikomanagement enthalten Regelungen zur Betriebsdokumentation und zu Betriebskonzepten, zu Wartungsarbeiten, zur Planung, Durchführung und Dokumentation von Changes, zum Kapazitätsmanagement, zur Trennung von Systemumgebungen, zum Schutz vor Schadsoftware, zur Datensicherung und Datenwiederherstellung, zum Logging und Monitoring, zur Systemkonfiguration und Systemhärtung, zu Zuständigkeiten und Verfahren bei der Meldung von Incidents, zur Bewertung, Einstufung, Behandlung und Dokumentation von Incidents, zur Meldung von Schwachstellen mit Auswirkungen auf die Informationssicherheit, zur Planung, Implementierung und Überprüfung des Notfallmanagements und der zugehörigen Notfallpläne, zur redundanten Auslegung interner Systeme und Ressourcen, zur Planung, Durchführung und Dokumentation von Notfalltests als präventiven Maßnahmen zur regelmäßigen Überprüfung der Korrektheit der Maßnahmen aus den Notfallplänen sowie zur regelmäßigen Analyse der Bedrohungen und Schwachstellen im Rahmen des Risikomanagements.

Die Regelungen zu den entsprechenden Maßnahmen, die Definition von Verantwortlichkeiten sowie die regelmäßige Überprüfung und Dokumentation der zugehörigen Maßnahmen sind Bestandteil regelmäßiger (mindestens jährlicher) interner und externer Audits des ISMS der virtion GmbH.

§ 7 Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

REGELUNGSGEGENSTAND:
Maßnahmen, um das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu diesen durch einen physischen oder technischen Zwischenfall zu reduzieren.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:
Die internen Richtlinien zur Betriebssicherheit, zum Incident Management und zum Business Continuity Management enthalten Regelungen zur Trennung von Systemumgebungen, zur Datensicherung und Datenwiederherstellung, zu Zuständigkeiten und Verfahren bei der Meldung von Informationssicherheitsereignissen, zur Bewertung, Einstufung, Behandlung und Dokumentation von Informationssicherheitsvorfällen, zur Analyse und Nutzung der Erkenntnisse aus Informationssicherheitsvorfällen, zur Meldung von Schwachstellen mit Auswirkungen auf die Informationssicherheit, zur redundanten Auslegung interner Systeme und Ressourcen, zur Planung, Implementierung und Überprüfung des Notfallmanagements und der zugehörigen Notfallpläne im Rahmen eines Notfallhandbuchs, zur Planung, Durchführung und Dokumentation von Notfalltests als präventiven Maßnahmen zur regelmäßigen Überprüfung der Korrektheit der Maßnahmen aus den Notfallplänen sowie zum Training von Notfallsituationen und zum Schutz kritischer Systeme, Informationen und Geschäftsprozesse vor den Auswirkungen größerer Ausfälle von Informationssystemen und Infrastrukturen sowie der Wiederherstellung innerhalb eines angemessenen Zeitraums im Rahmen des Business Continuity Managements der virtion GmbH.

Die Regelungen zu den entsprechenden Maßnahmen, die Definition von Verantwortlichkeiten sowie die regelmäßige Überprüfung und Dokumentation der zugehörigen Maßnahmen sind Bestandteil regelmäßiger (mindestens jährlicher) interner und externer Audits des ISMS der virtion GmbH.

§ 8 Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

REGELUNGSGEGENSTAND:
Darstellung der Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN:
Die internen Richtlinien zum Risikomanagement, zu internen Audits, zu Management Reviews, zur Personalsicherheit und zur Messung der Effektivität des ISMS enthalten Regelungen zur regelmäßigen Analyse der Bedrohungen und Schwachstellen sowie Risikobewertungen im Rahmen des Risikomanagements, zur regelmäßigen Planung, Durchführung und Dokumentation interner Audits des ISMS, zur regelmäßigen Planung, Durchführung und Dokumentation von Management Reviews zur Gewährleistung der Normkonformität des ISMS, zur Erfüllung der Informationssicherheitsziele der virtion GmbH, zum Management Commitment, zur Ressourcensicherung für den Betrieb des ISMS sowie zur kontinuierlichen Verbesserung des ISMS, zum regelmäßigen Training und zur Sicherstellung der Kompetenz und Awareness der Mitarbeiter sowie zur regelmäßigen Überprüfung und Dokumentation der Wirksamkeit der Maßnahmen des ISMS sowie sich evtl. daraus ergebender Maßnahmen im Rahmen der kontinuierlichen Verbesserung des ISMS.

Die Regelungen zu den entsprechenden Maßnahmen, die Definition von Verantwortlichkeiten sowie die regelmäßige Überprüfung und Dokumentation der zugehörigen Maßnahmen sind Bestandteil regelmäßiger (mindestens jährlicher) interner und externer Audits des nach ISO 27001 zertifizierten ISMS der virtion GmbH.

Zusätzliche Technisch-Organisatorische Maßnahmen (EASY Cloud)

Die nachfolgenden Maßnahmen sind zusätzlich zu den Maßnahmen aus dem Standardvertrag zur Auftragsverarbeitung zu sehen und stellen cloudspezifische Ergänzungen dar.

ZUTRITTSKONTROLLE:
- Es gelten zusätzlich die jeweiligen Zutrittsregeln der virtion GmbH.

ZUGANGSKONTROLLE / BENUTZERKONTROLLE:
- Der administrative Zugriff auf die Cloudsysteme ist nur über kryptographisch gesicherte Verbindungen möglich.
- Für jedes Cloudsystem werden personalisierte administrative Zugangsdaten verwendet.
- Passwörter müssen eine Mindestlänge von 12 Zeichen haben und ausreichend komplex sein.
- Der Administrative Zugriff ist zusätzlich durch die Verwendung eines VPN abgesichert.

ZUGRIFFSKONTROLLE / SPEICHERKONTROLLE / DATENTRÄGERKONTROLLE:
- Die virtuellen Maschinen sind netzwerktechnisch voneinander getrennt.
- Eventuell in den Produkten vorhandene Skripting-Möglichkeiten werden für den Kunden deaktiviert. Skripte sind nur durch Personal von EASY implementierbar.
- Kunden erhalten grundsätzlich keine oder nur eingeschränkte Administrationsmöglichkeiten auf Applikationsebene über eine Weboberfläche.

TRENNUNGSGEBOT / TRENNBARKEIT:
- Die Daten werden nach Mandanten/Instanzen getrennt.

VERSCHLÜSSELUNG:
- Der administrative Zugriff auf die Cloudsysteme ist nur über kryptographisch gesicherte Verbindungen möglich.
- Für den Kunden ist der Zugriff nur über HTTPS gesicherte Verbindungen möglich.

TRANSPORTKONTROLLE / ÜBERTRAGUNGSKONTROLLE (WEITERGABEKONTROLLE):
- Nutzung eines Reverse Proxies zur Filterung nicht zugelassener Anfragen.
- Erzwingen von HTTPS bei allen Anfragen.

Verfügbarkeit, Belastbarkeit / Widerstandsfähigkeit, Wiederherstellbarkeit
(d.h. Daten stehen zur Verfügung, wenn sie gebraucht werden)

VERFÜGBARKEITSKONTROLLE:
(gewährleistet, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind, z. B. durch Brandschutzmaßnahmen, etc.)
- Siehe Maßnahmen der Virtion

BELASTBARKEIT (IM SINNE VON: WIDERSTANDSFÄHIGKEIT):
(gewährleistet, dass die IT-Systeme widerstandsfähig gegen Angriffe sind)
- Einsatz einer Firewall.
- Einsatz eines Reverseproxies.

WIEDERHERSTELLBARKEIT:
(gewährleistet, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können)
- Die Daten werden täglich gesichert.