# Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

**Vereinbarung**

zwischen dem/der

................................................................................................

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

**estos GmbH, Petersbrunner Str. 3a, 82319 Starnberg**

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

## 1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

* Der Gegenstand des Auftrags ergibt sich aus dem Dienstleistungsvertrag/Rahmenvertrag vom XX.XX.201X, auf den hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

* Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: ……………………………………………………………………… (Definition der Aufgaben)

(2) Dauer

* Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

* Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

* Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum ...................

oder

* Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von ................... zum ................... gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

## 2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

* Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom ...................

oder

* Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: ........................................

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. Das angemessene Schutzniveau in ……………………….

* ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);
* wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);
* wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);
* wird hergestellt durch genehmigte Verhaltensregeln (Artt 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);
* wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).
* wird hergestellt durch sonstige Maßnahmen: ……………………………. (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO)

(2) Art der Daten

* Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .......................

oder

* Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)
* Personenstammdaten
* Kommunikationsdaten (z.B. Telefon, E-Mail)
* Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
* Kundenhistorie
* Vertragsabrechnungs- und Zahlungsdaten
* Planungs- und Steuerungsdaten
* Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
* ...

(3) Kategorien betroffener Personen

* Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: ..................................

oder

* Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
* Kunden
* Interessenten
* Abonnenten
* Beschäftigte
* Lieferanten
* Handelsvertreter
* Ansprechpartner
* ...

## 3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

## 4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.

* Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
* Als Datenschutzbeauftragte(r) ist beim Auftragnehmer \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
* Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

1. Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.
2. Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].
3. Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
4. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
5. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
6. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
7. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
8. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
9. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

## 6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung 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 Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

1. Eine Unterbeauftragung ist unzulässig.
2. Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

|  |  |  |
| --- | --- | --- |
| Firma Unterauftragnehmer | Anschrift/Land | Leistung |
| ........ | …….. | z. B. Telefonische/r Bestellannahme und Kundenservice |
|  |  |  |

1. Die Auslagerung auf Unterauftragnehmer oder

der Wechsel des bestehenden Unterauftragnehmers

sind zulässig, soweit:

* der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
* der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
* eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

* ist nicht gestattet;
* bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
* bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## 7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) 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.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

* die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
* die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
* aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
* eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

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

## 8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

1. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
2. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
3. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
4. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
5. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

## 9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## 10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

## 11 . Haftung

Auf Art. 82 DS - GVO wird verwiesen.

Im Übrigen wird folgendes vereinbart: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (ggf. ergänzen)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Unterschrift Auftraggeber Unterschrift Auftragnehmer

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum Ort, Datum

# Anlage 1 – Technische und organisatorische Maßnahmen (TOM)

| **Nr.** | **Gebiet** | **Beschreibung** |
| --- | --- | --- |
| **0** | **Organisation** | |
|  | Wie ist die Umsetzung des Datenschutzes organisiert? | Ein externer Datenschutzbeauftragter wird zur Wahrnehmung der Beratungs- und Kontrollfunktionen aus dem DSGVO eingesetzt. |
|  | Nennen Sie uns bitte den Namen und die Kontaktdaten Ihres Datenschutzbeauftragten. | Christian Volkmer Projekt 29 GmbH & Co. KG Ostengasse 14, 93047 Regensburg Tel: +49-941-2986930 E-Mail: c.volkmer@projekt29.de |
|  | In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen? | Regelmäßige Datenschutzschulungen aller Mitarbeiter  Verpflichtung aller Mitarbeiter auf die Datenschutzerklärung |
|  | Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert? | Ja, im Rahmen des internen Verfahrens-verzeichnisses sind die Datenströme dokumentiert und die Zulässigkeit der Verarbeitung und Nutzung nach DSGVO nachgewiesen. |
| **1** | **Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)** | |
| **1.1** | **Zutrittskontrolle** | |
|  | Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert? | Alarmanlage in Gebäudeanteil der Firma. |
|  | Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert? | Sicherungskreise der Alarmanlage. Zutritt nur für Mitarbeiter per dediziertem RFID-Chip.  Benachrichtigung von Sicherheitsdienst und bestimmten Mitarbeitern bei Alarm. |
|  | Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt? | Gesonderter Sicherungskreis der Alarmanlage mit Zugang nur für Administrationspersonal. |
|  | Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft? | Im Rahmen der Kontrollen durch den externen Datenschutzbeauftragten werden auch die Zutrittskontrollmaßnahmen überprüft. |
| **1.2** | **Zugangskontrolle** | |
|  | Wie erfolgt die Vergabe von Benutzerzugängen? | Die Abteilungsleiter bzw. Geschäftsführer melden den Eintritt neuer Mitarbeiter an die Administration.  Mitarbeiter erhalten bei Eintritt Microsoft Active Directory (AD)-Accounts, die Berechtigungen werden über AD-Gruppen geregelt. (Abteilungs-, Team- oder individuell basierte Zugehörigkeiten) |
|  | Wie wird die Gültigkeit von Benutzerzugängen überprüft? | Die Abteilungsleiter bzw. Geschäftsführer sind verpflichtet, relevante Änderungen in Beschäftigungsverhältnissen rechtzeitig der Administration anzuzeigen. |
|  | Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert? | Anforderungen zu Benutzerzugängen können nur von den Abteilungsleitern bzw. Geschäftsführern per E-Mail beantragt bzw. genehmigt werden und werden von der Administration per E-Mail bestätigt. Der Verlauf wird über die Mail-Archivierung festgehalten. |
|  | Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird? | Administrationszugänge erhalten nur der dedizierte Systemadministrator und Vertretungen aufgrund Genehmigung durch die Geschäftsführung.  Alle betreffenden und in Frage kommenden Personen besitzen einen nachweislichen fachlichen IT-Hintergrund mit Erfahrung in der Administration. Sie sind weder temporär noch als externe Mitarbeiter beschäftigt, befinden sich nicht in Probezeit, und wurden auf die Datenschutzerklärung des Unternehmens verpflichtet. |
|  | Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.) und wie ist der Zugang gestaltet? | Der Zugriff ist über eine verschlüsselte VPN-Verbindung (L2TP) für explizit freigegebene Mitarbeiter möglich. Die Authentifizierung erfolgt über die Microsoft Active Directory-Anmeldedaten und einen Preshared Key. |
| **1.3** | **Zugriffskontrolle** | |
|  | Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind? | Es existieren keine gemeinsam genutzten Benutzerzugänge.  Die Benutzer erhalten ein individuelles Initial-Passwort. Eine Änderung des Passwortes wird bei der ersten Anmeldung technisch erzwungen.  Die Mitarbeiter werden bei der Einstellung unterwiesen, sorgsam mit Passwörtern umzugehen und diese nicht anderen Personen zugänglich zu machen. |
|  | Welche Anforderungen werden an die Komplexität von Passwörtern gestellt? | Es werden nur Kennwörter akzeptiert, die keinen Teil des Benutzer-Logons oder –Namens darstellen, 3 aus 4 verschiedenen Zeichenklassen enthalten, und mind. 8 Zeichen lang sind. |
|  | Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann / muss? | Durch Gruppenrichtlinien (Systemeinstellungen Microsoft Active Directory) wird ein Wechsel des Passworts nach 60 Tagen erzwungen oder der Zugriff gesperrt. Das neue Passwort darf nicht einem der drei vorherigen entsprechen. |
|  | Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen? | Zugriffsfreigaben erfolgen User- und Gruppen-basiert für die mit der Verarbeitung betrauten Personen.  Die Systeme sind Passwortgeschützt. Arbeitsplätze werden automatisch bei Inaktivität gesperrt. Die Mitarbeiter sind unterwiesen, bei Verlassen des Arbeitsplatzes ihre Arbeitsplätze zu verlassen und keine sichtbaren bzw. frei zugängliche personenbezogene Daten zu hinterlassen. |
|  | Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden? | Die Geschäftsführung prüft in regelmäßigen Abständen die Rechte und Benutzerstruktur. |
|  | Wie erfolgt die Dokumentation von Zugriffsberechtigungen? | Über die Access Control Lists in den Systemen. |
|  | Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden? | Sporadische Durchsicht der Systemprotokolle durch die Geschäftsführung. |
|  | Wie lange werden Protokolle aufbewahrt?  Wer hat Zugriff auf die Protokolle und wie oft werden sie ausgewertet? | Keine festgelegten Fristen, meist Systemparameter,  ausschließlich die Geschäftsführung. |
| **1.4** | **Trennungskontrolle** | |
|  | Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden? | Zur Trennung der Daten wird ein dezidiertes Rechtesystem eingesetzt. |
| **1.5** | **Pseudonymisierung** | |
|  | Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt? | Regelmäßige Datenschutzschulungen aller Mitarbeiter  Verpflichtung aller Mitarbeiter auf die Datenschutzerklärung |
|  | Wie werden personenbezogene Daten verarbeitet /aufbewahrt, sodass diese nicht den betroffenen Personen zugeordnet werden können? | Die Verarbeitung personenbezogener Daten kann in den meisten Fällen einer betroffenen Person zugeordnet werden. |
| **2** | **Integrität (Art. 32 Abs. 1 lit. b DS-GVO)** | |
| **2.1** | **Weitergabekontrolle** | |
|  | Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten? | Die Weitergabe erfolgt über verschlüsselte Kanäle und/oder die Verschlüsselung der Daten selbst.  Eine Zustellung oder Bekanntgabe von Zugangsdaten erfolgt nur an den vorhergesehen Empfänger. |
|  | Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche? | Ein Versenden per E-Mail oder Bereitstellung per Internet erfolgt über Server mit Transportverschlüsselung (TLS).  Die Verschlüsselung von Daten erfolgt auf Datenträgerbasis über Microsoft Bitlocker und/oder über verschlüsselte ZIP-Archive (AES-256). |
|  | Wie wird die Weitergabe personenbezogener Daten dokumentiert? | n/a |
|  | Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt? | Eine strikte Rechtevergabe sichert die Daten vor unberechtigtem Zugriff. |
|  | Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann? | Dies wird im Rahmen der Kontrollen unter Punkt 1.3 mit geprüft. |
| **2.2.** | **Eingabekontrolle** | |
|  | Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat? | Zugriffs-Logs der Server und Systeme. |
|  | Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden? | Zugriffs-Logs der Applikationen. |
|  | Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß der Weisungen des Auftraggebers erfolgen kann? | Schulung bzw. Sensibilisierung der Mitarbeiter durch regelmäßige Veranstaltungen bzw. Personalgespräche. |
|  | Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers durchführt? | Die Datenverarbeitung von Unterauftragnehmern erfolgt mit eindeutigen Auftragsdefinitionen und einer formalisierten Auftragserteilung. |
|  | Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt? | Festlegung durch Vertragsbindung, bei Wegfall des Zweckes ist ebenfalls eine Löschung der Daten indiziert. |
| **3** | **Verfügbarkeit und Belastbarkeit** | |
| **3.1.** | **Verfügbarkeitskontrolle** | |
|  | Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind? | Die Backup-Datenträger werden in einem entsprechenden Panzerschrank aufbewahrt.  Backup-Sätze werden turnusmäßig extern durch die Geschäftsführung ausgelagert. |
|  | Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet? | Betriebssystem-Sicherheitsupdates und Antiviren-Software und –Definitionen werden zentral automatisiert ausgerollt und aktualisiert.  Antiviren- und Firewall-Lösungen werden auf den Client- und Serversystemen eingesetzt.  Eingehende Mails werden vor Zustellung durch den Mail-Transport-Server auf Schädlinge und gefälschte Absenderdaten geprüft. |
|  | Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden? | Die anfallenden Datenträger werden zentral durch die IT-Abteilung entsorgt.  Funktionsfähige Datenträger werden entsprechend geeigneter Methoden sicher gelöscht. (z.B. mehrfaches Überschreiben)  Nicht funktionsfähige Datenträger werden physikalisch vernichtet. |
| **3.2.** | **Wiederherstellbarkeit** | |
|  | Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten? (rasche Wiederherstellbarkeit nach Art. 32 Abs.1 lit.c DS-GVO) | Die Server- und Stromversorgungssysteme der Verarbeitungsanlage sind redundant ausgelegt, um einem Ausfall vorzubeugen. |
| **4.** | **Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO)** | |
|  | Welche Verfahren gibt es zur regelmäßigen Bewertung/Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)? | Der externe Datenschutzbeauftragte überprüft regelmäßig und teilweise auch unangekündigt, die Einhaltung der technisch-organisatorischen Maßnahmen. |
|  | Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)? | Einsatz eines Ticketsystems (Kayako) zweistufig (1st und 2nd Level); zusätzlich Telefonhotline und automatisierte Überwachung und Alarmierung |
|  | Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)? | Keine Vorbelegung durch Haken; bei Anmeldung im System erfolgen keine Vorbelegungen; Benutzer muss die Anmeldeinformationen jeweils eintragen |
| **4.1** | **Auftragskontrolle** | |
|  | Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenverarbeitung (Datenschutz-Management)? | Das Vertragswerk wurde entsprechend den neuen Richtlinien zur Auftragsdatenverarbeitung gestaltet. Der externe Datenschutzbeauftragte nimmt entsprechende Beratungs- und Kontrollpflichten wahr. |