Vereinbarung zur Auftragsverarbeitung

Regelungen zu Datenschutz und Datensicherheit in Auftragsverhältnissen

Zwischen
Kunde
Adresse

(Nachfolgend „Auftraggeber“ genannt)

und

Enit Energy IT Systems GmbH
Mercystraße 26
79100 Freiburg

(Nachfolgend „Auftragnehmer“ genannt)

(beide gemeinsam nachfolgend „Vertragsparteien“ genannt)

Enit

Präambel

Diese Vereinbarung zur Auftragsverarbeitung spiegelt die Vereinbarung der Parteien in Bezug auf die Bedingungen wider, die die Verarbeitung der personenbezogenen Daten des Kunden (nachfolgend „Auftraggeber" genannt) durch Enit Energy IT Systems GmbH (nachfolgend „Enit" oder „Auftragnehmer" genannt) unter den zwischen den Parteien bestehenden Vertragsverhältnisses regeln. Die Vereinbarung zur Auftragsverarbeitung wird durch Bezugnahme in den jeweiligen Vertragsdokumenten zwischen den Parteien rechtswirksam als Anlage in das zwischen den Parteien bestehende Vertragsverhältnis aufgenommen.

Für Bestandskunden gilt, dass durch das Bereitstellen dieser Vereinbarung vom Auftragnehmer an den Auftraggeber das zwischen den Parteien bestehende Vertragsverhältnis rechtswirksam ergänzt und somit zwischen den Parteien rechtsverbindlich vereinbart wird.

Enit bietet dem Auftraggeber über den Enit hub einen Service zur Erstellung von CO2-Bilanzierung an.

Bei der Erbringung der Leistungen durch Enit oder durch sie beauftragte Unterauftragnehmer (Subunternehmer), wie z.B. Beratungsleistungen im Zusammenhang mit der optimierten Auslegung und Installation von energetischer Infrastruktur, kann ein in Berührung kommen mit personenbezogenen Daten des Auftraggebers nicht ausgeschlossen werden. Soweit dies der Fall ist, verarbeitet der Auftragnehmer personenbezogene Daten nur im Auftrag und nach Weisung des Auftraggebers.

Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung aus Art. 28 EU-Datenschutz-Grundverordnung (DSGVO) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung. In dieser Vereinbarung verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen.

1. Gegenstand des Auftrags, Art und Zweck der Verarbeitung

1) Der Enit hub ist die Softwareplattform von Enit und beinhaltet verschiedene Module welche bspw. zur Erstellung von CO2-Bilanzen, Messkonzepten oder Photovoltaik-Checks genutzt werden können.

(2) Im Übrigen ergibt sich der Gegenstand des Auftrags aus der „Leistungsbeschreibung und dem Service Level Agreement (SLA)" auf welches hier verwiesen wird (im Folgenden „Hauptvertrag").

2. Art der personenbezogenen Daten, Kategorien betroffener Personen

(1) Art der Daten:

- Personenstammdaten (Vorname & Nachname)
- Kommunikationsdaten: E-Mail-Adresse
- Sonstige Informationen, die der Auftraggeber bei Nutzung des Systems verarbeitet

- (insbesondere Daten, die in Kommentarfelder eingetragen werden)
- Log-Daten zur Gewährleistung der IT-Sicherheit

(2) Kreis der betroffenen Personen:

☒ Kunden (Verbraucher)

☒ Kunden (Geschäftskunden)

☒ Interessenten

☐ Mitarbeiter

☐ Lieferanten

☐ Dienstleister

3. Dauer des Auftrages

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags.

4. Verantwortlichkeit und Weisungsbefugnis

(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO). Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Etwas anderes gilt nur in dem in Absatz 2 genannten Umfang.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn es besteht eine anderweitige Verpflichtung durch Unionsrecht oder dem Recht des Mitgliedsstaates, dem der Auftragnehmer unterliegt. Im Falle einer anderweitigen Verpflichtung teilt der Auftragnehmer dem Auftraggeber vor der Verarbeitung unverzüglich die entsprechenden rechtlichen Anforderungen mit.

(3) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

(4) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den Auftraggeber. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

5. Vertraulichkeit

Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO auf die Vertraulichkeit verpflichtet worden sind 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.

6. Datensicherheit

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Dazu wird der Auftragnehmer

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten.

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 DSGVO zu berücksichtigen.

(2) Die Vertragsparteien vereinbaren die in dem Anlage 2 zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen.

(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 und dem Auftraggeber mitzuteilen.

7. Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)

(1) Als Subunternehmer im Sinne dieser Regelung gelten vom Auftragnehmer beauftragte Auftragsverarbeiter, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen und Reinigung 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 hiermit die allgemeine Genehmigung zur Hinzuziehung von Subunternehmern (Anlage 1). Über den geplanten Einsatz

eines weiteren Subunternehmers oder den Austausch eines bestehenden Subunternehmers hat der Auftragnehmer den Auftraggeber rechtzeitig vorab zu informieren. Die Zustimmung zur Untervergabe gilt als erteilt, wenn der Auftraggeber nicht innerhalb von 6 (sechs) Wochen, beginnend mit Zugang der Information in vorstehendem Sinne, dem Einsatz des betreffenden Subunternehmers widerspricht. Ein solcher Widerspruch ist nur aus berechtigten Gründen zulässig, wie z. B. nicht ausreichende Zuverlässigkeit des Subunternehmers.

Widerspricht der Auftraggeber dem Einsatz eines vom Auftragnehmer gewünschten Subunternehmers, so ist der Auftragnehmer berechtigt, den Hauptvertrag ohne Einhaltung einer Kündigungsfrist und mit sofortiger Wirkung zu kündigen.

(3) Mit dem Subunternehmer ist eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 3 und 4 DSGVO abzuschließen, die den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit dieser Vereinbarung entspricht.

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

(5) Die Verarbeitung der Daten durch den Auftragsverarbeiter und durch die vom Verantwortlichen genehmigten Subdienstleister findet grundsätzlich in Mitgliedstaaten der Europäischen Union, Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und/oder solchen Ländern statt, für die ein gültiger, auf die Verarbeitung anwendbarer Angemessenheitsbeschluss der Kommission im Sinne des Art. 45 Abs. 3 DSGVO vorliegt. Es ist dem Auftragsverarbeiter gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb der EU/ des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und sicherstellt, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU- Standarddatenschutzklauseln).

(6) Eine weitere Auslagerung durch den Subunternehmer bedarf der ausdrücklichen Zustimmung des Auftragnehmers (mind. Textform). Sämtliche vertragliche Regelungen in der Vertragskette sind auch dem weiteren Subunternehmer aufzuerlegen.

8. Unterstützung bei der Wahrung von Betroffenenrechten

(1) Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO). Insbesondere wird der Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche Betroffener auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen.

(2) Der Auftragnehmer darf personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken (Art. 28 Abs. 3 S. 2 lit. g DSGVO). Auskünfte an Dritte oder den betroffenen Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(3) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

9. Unterstützung bei Dokumentations- und Meldepflichten

(1) Ist der Auftragnehmer nach Art. 37 DSGVO, § 38 BDSG gesetzlich dazu verpflichtet, einen Daten- schutzbeauftragten zu benennen, teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten des Datenschutzbeauftragten auf Anfrage zum Zweck der direkten Kontaktaufnahme mit.

(2) Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Auftraggeber unverzüglich Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2 DSGVO. Das Gleiche gilt, wenn beim Auftragnehmer beschäftigte Personen gegen diese Vereinbarung verstoßen.

(3) Nach Absprache mit dem Auftraggeber trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen.

(4) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Erfüllung der Informationspflichten gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DSGVO und ggf. gegenüber den von der Verletzung des Schutzes personenbezogener Daten Betroffenen gemäß Art. 34 DSGVO.

(5) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei einer vorherigen Konsultation der zuständigen Aufsichtsbehörde gemäß Art. 36 DSGVO.

(6) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

10. Beendigung des Auftrages

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

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

11. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitungsleistungen und währenddessen regelmäßig die technischen und organisatorischen Maßnahmen sowie die Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zu kontrollieren.

(2) 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 und unter Berücksichtigung einer angemessenen Vorlaufzeit (mindestens 72 Zeitstunden, werktäglich) durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem direkten Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist diejenigen Auskünfte zu erteilen, die zum Nachweis der Einhaltung der Pflichten unter diesem Auftragsverarbeitungsvertrag sowie zum Nachweis der technischen und organisatorischen Maßnahmen erforderlich sind. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit vorlegen. Der Auftraggeber hat dem Auftragnehmer den durch die Erteilung der Auskünfte entstehenden Aufwand zu vergüten.

12. Haftung

Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen solchen Schaden gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz, oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung entspricht.

13. Schlussbestimmungen

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

(2) Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrere Regelungen werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine solche Regelung ersetzen,

die der unwirksamen Regelung wirtschaftlich und datenschutz- rechtlich am ehesten entspricht.

(3) Im Falle eines Widerspruchs zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.

(4) Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:

- Anlage 1: Auflistung genehmigter Subunternehmer
- Anlage 2: Technische und organisatorische Maßnahmen

Anlage 1

Genehmigte Subunternehmer

Enit erklärt, dass die nachfolgenden Subunternehmer eingesetzt werden:

Subunternehmer	**Verarbeitungstätigkeit**	**Ort der Datenverarbeitung**	**Geeignete Garantien, Art. 44 ff. DSGVO (falls erforderlich)**	**Zusätzliche Maßnahmen zum Schutz personenbezogener Daten (falls erforderlich)**
Amazon Web Services EMEA SARL38 "AWS Europe"	Bereitstellung von Cloud Computing	EU (Avenue John F. Kennedy, L-1855 Luxembourg Sitz der Gesellschaft: L-1855 Luxemburg eingetragen im Luxemburgischen Handelsregister unter R.C.S. B186284)		-
Amazon Web Services EMEA SARL "AWS Europe"	Bereitstellung von Cloud Computing	EU (Niederlassung Deutschland Marcel-Breuer-Str. 12, 80807 München, Deutschland Sitz der Zweigniederlassung: München eingetragen im Handelsregister des Amtsgerichts München unter HRB 242240, USt-ID: DE317013094)		-
Prefab, Inc	Steuerung der Anzeige von Features über Feature Flags	USA	EU-Standarddatenschutzklauseln Modul 3, inkl. Transfer Impact Assessment (Beschluss 2021/914 der EU-Kommission vom 04. Juni 2021)	Verschlüsselte Datenübermittlung
PostHog Inc.	Bereitstellung von Software-Nutzungsanalysen (SaaS)	EU (Frankfurt am Main)	Datenverarbeitung innerhalb der EU	TLS-Verschlüsselung bei Übertragung; Zugriffskontrollen
Oso Security, Inc.	Bereitstellung von Software zur	EU (Frankfurt am Main)	Standard Contractual Clauses (SCC) in aktueller	TLS-Verschlüsselung, rollenbasierte

	Autorisierungsverwaltung und Zugriffskontrolle (SaaS)		Fassung; ergänzend Anbieter-DPA	Zugriffskontrolle, weitere technische und organisatorische Maßnahmen lt. Anbieter-DPA
Auth0, Inc.	Benutzerauthentifizierung, Autorisierungsmanagement (Identity as a Service)	USA	EU-Standardvertragsklauseln (SCC), Modul 2; ergänzend DPA von Auth0 (inkl. Transfer Impact Assessment nach Beschluss 2021/914)	TLS-Verschlüsselung bei Übertragung; rollenbasierte Zugriffskontrollen; Logging; weitere technische und organisatorische Maßnahmen lt. Anbieter-DPA

Anlage 2

Technische und organisatorische Maßnahmen

In der hier vorliegenden Beschreibung über den aktuellen Stand der grundlegenden Maßnahmen zum Schutz der Daten wird einschränkend darauf hingewiesen, dass verständlicherweise nicht alle Sicherheitsmaßnahmen im Detail offengelegt werden können. Gerade in Bezug auf Datenschutz und Datensicherheit ist der Verzicht auf vertrauliche und detaillierte Beschreibungen unabdingbar, da der Schutz der Sicherheitsmaßnahmen gegen unbefugte Offenlegung mindestens genauso wichtig ist wie die Sicherheitsmaßnahmen selbst.

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

Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

- Alarmanlage
- Sicherheitsschlösser
- Zutrittsberechtigungskonzept
- Manuelles Schließsystem
- Schlüsselregelung / Schlüsselbuch
- Rechenzentren mit Standort in Deutschland oder der EU
- Rechenzentren zertifiziert nach ISO 27001
- separate Serverräume
- Hochsicherheitszugang
- Sorgfältige Auswahl von Reinigungspersonal

Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.

- Getrenntes Gäste-WLAN
- Detaillierte Benutzerprofile
- Authentifikation mit Benutzer + Passwort
- Passwortregelungen
    - Verwendung von individuellen Passwörtern
    - Passwörter mit einer Mindestlänge
    - Anzahl von aufeinanderfolgenden Fehlversuchen ist begrenzt
    - Passworthistorie
- Schlüsselregelung
- Verschlüsselung von mobilen Datenträgern
- Autonome Fernwartung
- Bestandteil des Sicherheitskonzeptes der pA Gruppe
- Zugriff nur per VPN auf internem Server
- Zentrale Änderung der Zugangsberechtigungen durch IT-Verantwortliche
- Protokollierung der Serverzugriffe auf Benutzerebene

Zugriffskontrolle
Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

- Detailliertes Berechtigungskonzept
- Sichere Aufbewahrung von Datenträgern
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduzieren
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Einsatz von Dienstleistern zur Akten- und Datenvernichtung (i.d.R. Möglichkeit mit Zertifikat)
- Einsatz von Intrusion-Detection-Systemen
- Einsatz von VPN-Technologie
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall
- Einsatz von Anti-Viren-Software

Trennungskontrolle
Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

- Festlegung von Datenbankrechten
- Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt
- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)

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

Weitergabekontrolle
Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln.

- Elektronische Übertragung, Datentransport, sowie deren Kontrolle.
- Einsatz von verschlüsselten Verbindungen (z.B. VPN, HHPS)
- Sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- Shredder für die sichere Vernichtung von Daten

Eingabekontrolle
Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Folgende Aktivitäten werden protokolliert: Hoch- und Herunterfahren von zentralen Rechnern (v.a. Servern und Firewalls)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

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

Verfügbarkeitskontrolle und Belastbarkeit
Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Systeme müssen die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.

- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Testen von Datenwiederherstellung
- Serverräume nicht unter sanitären Anlagen
- Backup- & Recoverykonzept
- Unterbrechungsfreie Stromversorgung (USV)
- Aufbewahrung von Datensicherung an einem sicheren, separaten Ort

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

Kontrollverfahren
Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren.

- Unternehmensrichtlinien (Code of Conduct) vorhanden
- Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
- Datenschutz-Management vorhanden
- Datenschutz-Konzept vorhanden

5 Technische und Organisatorische Maßnahmen im Home Office

Enit ermöglicht ihren Mitarbeitenden, anfallende Arbeiten via Remote-Zugang durchzuführen. Hierfür wurden Maßnahmen ergriffen, um dem Sicherheitsstandard des allgemeinen Sicherheitskonzeptes zu entsprechen. Dieses gilt, soweit anwendbar und wird um die folgenden Maßnahmen ergänzt.
Die Maßnahmen unterteilen sich in **technische Maßnahmen**, die den Zugang zum System betreffen sowie in **organisatorische Maßnahmen**, die den Umgang des jeweiligen Mitarbeiters mit Daten an seinem Heimarbeitsplatz betreffen.

Technische Maßnahmen
Die nachfolgenden Maßnahmen stellen die zusätzlich ergriffenen Maßnahmen dar. Für den Zugriff auf das System hat Enit folgende Maßnahmen getroffen:

- Zugang ausschließlich über dienstliche Endgeräte
- Endgeräte werden IT-seitig regelmäßigen Updates unterzogen
- Applikationen dürfen ausschließlich nach Konsultation der hierfür vorliegenden Whitelist installiert werden. IT-seitig nicht zugelassene Applikationen dürfen nicht installiert werden
- Ein Zugriff erfolgt ausschließlich durch eine verschlüsselte VPN-Verbindung
- Windows Clients
    - Endpoint Security
    - Antivirus Software
    - Systemverschlüsselung
- Kontrolle über das Gerät mit Möglichkeit zum remote „wipe" bzw. „lock"
    - komplette Verschlüsselung des Gerätes
    - geschützt durch sechsstelligen Pass Code
    - restriction policy
- nicht vertrauenswürdige Zertifikate können nicht manuell akzeptiert werden
- keine Diagnosedaten an Apple
- Benutzer kann keinen 3rd-Party Apps manuell vertrauen

Organisatorische Maßnahmen

In organisatorischer Hinsicht wurden in Ergänzung zu den Maßnahmen der allgemeinen TOM verschiedene Zusatzvereinbarungen sowie interne Richtlinien erlassen. Dies umfasst unter anderem Folgende Regelungen und Verpflichtungen:

- Zutritts- und Kontrollrecht des Arbeitsplatzes durch interne beauftragte Prüfer (z.B. Fachkraft für Arbeitssicherheit oder betrieblicher Datenschutzbeauftragter)
- Verpflichtung auf interne Richtlinie zur Nutzung technischer Einrichtungen
- Verpflichtung zum Schutz des Zugriffs unbefugter Dritter auf Arbeitsmittel
- Untersagung der Verwendung eigener technischer Einrichtungen (Ausgenommen WLAN, Peripheriegeräten wie Tastatur und Maus ohne Treiberinstallation)
- Verpflichtung, vertrauliche dienstliche Dokumente unter Verschluss zu halten
- Verpflichtung auf Vertraulichkeit / zur Geheimhaltung
- Verpflichtung, Wohnortswechsel mitzuteilen