Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen der / dem

_____

- Verantwortlicher - nachstehend *Auftraggeber* genannt -

und der Firma

Ypsilon.dev UG (haftungsbeschränkt), Abensstraße 8, 93059 Regensburg - Auftragsverarbeiter

- nachstehend *Auftragnehmer* genannt -

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zur Datenverarbeitung ist das Domain-/Webhosting und der Webservice sowie die damit in Zusammenhang stehenden Leistungen durch den Auftragnehmer. Im Rahmen dieser Tätigkeit kann dabei nicht ausgeschlossen werden, dass der Auftragnehmer als IT-Dienstleister bei der Erbringung seiner vertraglichen Leistungen für den Auftraggeber auch Zugriff auf personenbezogene Daten des Auftraggebers erhält. Diese Anlage konkretisiert die gegenseitigen Pflichten im generellen Umgang mit Daten.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinaus gehende Verpflichtungen ergeben. Die Möglichkeiten einer fristlosen Kündigung aus wichtigem Grund 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 im Leistungsvertrag beschrieben.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten können folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien) sein.

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Daten von Webseitenbesuchern und Onlinekunden

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Interessenten
- Abonnenten
- Beschäftigte
- Lieferanten
- Handelsvertreter
- Ansprechpartner
- Webseitenbesucher

3. Ort der Leistungserbringung

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 Art. 44 ff. DSGVO erfüllt sind.

4. 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.

5. 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.

6. 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:

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet.
b) 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.
c) 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].
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) 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.
f) 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.
g) 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.

7. 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) Erfolgt eine Verarbeitung im Auftrag, so arbeitet der Auftragnehmer nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Der Auftraggeber stimmt der Beauftragung von Unterauftragnehmern zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO. Die jeweils aktuelle Liste der Unterauftragsunternehmer ist im Internet unter der folgenden Adresse aufrufbar:

https://ypsilon.dev/policies/sub-processors

Die Auslagerung auf Unterauftragnehmer oder ein 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 Unterbeauftragung von Unterauftragnehmer, welche die vereinbarte Leistung außerhalb der EU/des EWR erbringen, ist nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers zulässig.

8. 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.
Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der

Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.
Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich vorstehender Absätze entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.
(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 angemessenen Vergütungsanspruch geltend machen.

9. 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.

a) 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
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) 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
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) 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.

10. 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.

11. 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.

12. Anfragen betroffener Personen

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

Unterschriften

_____ ,den_____	_____ ,den_____
Auftraggeber	**Auftragnehmer**
Name:	Name:
Titel:	Titel:

Anlage – Technisch-organisatorische Maßnahmen

Zu unterscheiden ist einerseits zwischen der Verarbeitung personenbezogener Daten durch Speicherung auf dem Hostingserver (Ziffer 1 Hosting), sowie die Verarbeitung personenbezogener Daten des Auftraggebers in der Betriebsstätte des Verantwortlichen, z.B. im Rahmen von Supportleistungen oder Hotlines oder zur Vertragsabwicklung (Ziffer 2 - Verarbeitung personenbezogener Daten im Betrieb des Verantwortlichen selbst)

1. Hostingserver

Die Verarbeitung von Daten für die Webpräsenz /Shop und e-Mail für den Auftraggeber, findet ausschließlich in Rechenzentren in der EU statt. Die Domain wird bei einem externen Dienstleister gehostet. Die Rechenzentren der eingesetzten Provider sind nach ISO/IEC 27001 zertifiziert. Durch den Einsatz mehrerer unabhängiger Rechenzentren wird die Belastbarkeit der Veranstaltungssoftware gewährleistet – redundante Systemauslegung. Dadurch kann auch kurzfristig auf einen Ausfall oder nutzungsverhindendes Fehlverhalten der Veranstaltungsplattform reagiert werden. Die Rechenzentren sind 24 / 7 besetzt und bearbeiten Störungsmeldung sofort ab.

Die Rechenzentren verfügen als zertifizierte Hochleistungsserverzentren über entsprechende Zutrittskontrollen, Zugriffskontrollen, Alarmanlagen, Kameraüberwachung, Virenschutz, Firewall, USV, Überspannungsschutz, Schutz gegen Umwelteinflüsse, Klimatisierung, Feuer/Rauchmeldeanlagen, Brandlöschanlagen, Incident-Response-Management.

Ein Zugriff auf den Server erfolgt ausschließlich über Login mit Benutzernamen und sicheren Passwörtern über Hypertext Transfer Protocol Secure (Transportverschlüsselung).

Für jeden Kunden wird Seitens des Verantwortlichen eine eigene Instanz und ein eigenes Verzeichnis aufgesetzt, so dass sichergestellt ist, dass Daten, die zu unterschiedlichen Zwecken erhoben werden, auch getrennt verarbeitet werden (Trennungskontrolle).

Eine Verarbeitung von personenbezogenen Daten außerhalb der EU findet nicht statt.

2. Verarbeitung personenbezogener Daten im Betrieb des Verantwortlichen selbst

2.1. Zutrittskontrolle:

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen.
Zutritt zum Betriebsgebäude nur mittels Schlüssel - Sicherheitsschlösser.
Begleitpflicht für Besucher
Ansprache unbekannter Personen
Trennung von Bearbeitungs- und Publikumszonen

2.2. Zugangskontrolle:

Keine unbefugte Systembenutzung,
Login mit Benutzernamen und sicherem langen Passwort.
Einsatz sichere Kennwörter;
Einsatz von Anti-Viren Software, Firewall.
Einsatz von VPN bei Remote Zugriffen.

2.3. Zugriffskontrolle:

Bereithalten getrennter Test- und Produktivsysteme für Wartungsarbeiten
Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte;
Differenzierte Berechtigungen;
Minimale Anzahl an Administratoren;
Verwaltung Benutzerrecht durch Administrator.
Protokollierung von Löschungen von Daten auf dem Server.
Sichere Aufbewahrung von Datenträgern; für Unberechtigte nicht zugänglich.
Datenschutzkonforme Vernichtung / Löschung von Daten, die eine Kenntnisnahme durch Unbefugte ausschließt.

2.4. Weitergabekontrolle:

Verschlüsselung bei Versand von personenbezogenen vertraulichen Anhängen per e-Mail.
Einsatz von VPN
Firewall, Virenscanner
Bereitstellung über verschlüsselte Verbindungen wie sftp, https.
Verschlüsselung mobiler Datenträger

2.5. Eingabekontrolle/Verarbeitungskontrolle

Protokollierung der Löschung von Daten.
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts.

2.6. Auftragskontrolle

Verarbeitung von Daten nur im Rahmen des Auftrags und nur auf ausdrückliche Weisung des Auftraggebers.
Sofern personenbezogene Daten im Auftrag des Auftraggebers verarbeitet, schließen die Parteien schriftliche Vereinbarungen, die zumindest die gesetzlichen Mindestanforderungen beinhalten zur Auftragsverarbeitung.
Werden dem Speichermedien für die Erfüllung von Verpflichtungen übergeben, so werden diese nach Erfüllung unverzüglich an den Auftraggeber zurückzugeben.
Regelmäßige Überprüfung durch Geschäftsleitung.

2.7. Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.
Feuermelder, Feuerlöscher,
Backups
Virenschutz
Firewall

2.8. Trennungskontrolle:

Trennung von Produktiv- und Testumgebung.
Physikalische Trennung von Hostingdaten und internen Daten.
Steuerung über Berechtigungskonzept.

3. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

• **Datenschutz-Maßnahmen:**

Datenschutzfolgeabschätzung wird bei Bedarf durchgeführt.
Mitarbeiter auf Vertraulichkeit / Datengeheimnis verpflichtet.

• **Auftragskontrolle**:

Strenge Auswahl von Subunternehmern und Abschluss von AV-Verträgen,
Verpflichtung der Mitarbeiter auf das Datengeheimnis;
keine Verarbeitung personenbezogener Daten außerhalb der EU.

• **Incident-Response-Management:**

Einsatz von Firewall und regelmäßige Aktualisierung,
Einsatz von Spamfiltern,
Einsatz von Virenscanner,

• **Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DS-GVO):

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind. Privacy by Design und privacy by default.