AUFTRAGSVERARBEITUNGSVEREINBARUNG

GESCHÄFTSZEITEN: MONTAG BIS DONNERSTAG 08:00 BIS 12:00 UHR, SOWIE 13:00 BIS 17:00 UHR; FREITAGS 08:00 BIS 14:00 UHR

Auftraggeber (Verantwortlicher):

Fachpartnername:	
Straße und Hausnummer:	
PLZ und Ort:	
Ansprechpartner:	
E-Mail-Adresse:	

Auftragnehmer (Auftragsverarbeiter):

DieEnergieFabrik DEF GmbH
Am Hang 2a
84048 Mainburg

1. Gegenstand der Vereinbarung

Gegenstand der Vereinbarung ist die Verarbeitung von Personendaten, die im Zusammenhang mit dem Kaufvertrag mit dem Auftragsnehmer und der Weitergabe der Namen und der Adresse der Endkunden des Auftraggebers wegen Direktlieferung des Auftragnehmers an den jeweiligen Endkunden inklusive der Serviceleistung bei der Installation durch Online-Zugriff auf das jeweilige Produkt beim Endkunden des Auftraggebers anfallen. Die Datenverarbeitung erfolgt ausschließlich auf Grundlage eines gesonderten Vertragsverhältnisses zwischen Auftraggeber und Auftragnehmer („Kaufvertrag inklusive optionaler Direktlieferung und Serviceleistung bei der Installation durch Online-Zugriff auf das jeweilige Produkt beim Endkunden des Auftraggebers. “), der Grundlage der vorliegenden Auftragsverarbeitungsvereinbarung ist.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 Datenschutz-Grundverordnung (DS-GVO) auf Grundlage dieser Vereinbarung.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2. Dauer der Vereinbarung, Kündigung

Die Laufzeit dieser Vereinbarung richtet sich nach dem Kaufvertrag inklusive optionaler Direktlieferung und Serviceleistung bei der Installation durch Online-Zugriff auf das jeweilige Produkt beim Endkunden des Auftraggebers, die auf die Lebensdauer des gekauften Produkts abstellt, es sei denn, der Auftraggeber kündigt diesen Vertrag und die Auftragsdatenverarbeitungsvereinbarung mit einer Frist von zwei (2) Wochen zum Monatsende. zwischen Auftraggeber und Auftragnehmer, sofern sich aus der vorliegenden Vereinbarung nichts Abweichendes ergibt.

Der Auftraggeber kann die vorliegende Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine zulässige und zumutbare Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer vertragswidrig die Wahrnehmung von Kontrollrechten durch den Auftraggeber verweigert. Insbesondere die Nichteinhaltung der in dieser Vereinbarung vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schwerwiegenden Verstoß im vorbenannten Sinne dar.

3. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Der Zweck der Datenverarbeitung durch den Auftragnehmer für den Auftraggeber, die verarbeiteten Datenarten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS-GVO) sowie die Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO) ergeben sich aus dem Kaufvertrag inklusive optionaler Direktlieferung und Serviceleistung bei der Installation durch Online-Zugriff auf das jeweilige Produkt beim Endkunden des Auftraggebers. und werden nachfolgend näher beschrieben:

Login-Daten

Name und Anschrift des Endkunden

4. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen.

Die Kommunikation zwischen Auftraggeber und Auftragnehmer erfolgt ausschließlich per E-Mail.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen des Kaufvertrags inklusive optionaler Direktlieferung und Serviceleistung bei der Installation durch Online-Zugriff auf das jeweilige Produkt beim Endkunden des Auftraggebers. sowie nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

AUFTRAGSVERARBEITUNGSVEREINBARUNG

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenverarbeitung erfolgt ausschließlich elektronisch mittels verschlüsselter Datenübertragung über den HTTPS-Standard (SSL-Verschlüsselung); physische Datenträger werden nicht verwendet. Eingang und Ausgang der Daten werden dokumentiert. Die Daten werden ausschließlich im Moment der Verarbeitung (Abgleich) genutzt, nicht gespeichert und auch nicht in irgendeiner Weise Personen oder Orten zugeordnet.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DS-GVO).

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in gespeicherte Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres folgendes vereinbart:

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist gestattet, soweit die Umsetzung der Maßnahmen nach Art. 32 DS-GVO auch in diesem Fall sichergestellt ist.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung der Vereinbarung fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz bestellt:

Secjur GmbH
Steinhöft 9, 20459 Hamburg
E-Mail: datenschutz@bachner.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieser Vereinbarung durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss.

Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind [z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln].

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

8. Technische / organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DS-GVO ergriffen hat und ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewähreistet. Dazu werden die die Schutzziele von Art. 32 Abs. 1 DS-GVO wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Maßnahmen das Risiko auf Dauer eingedämmt wird. Einzelheiten zu den vom Auftragnehmer ergriffenen Maßnahmen sind der Anlage „Technisch-organisatorische Maßnahmen“ zu entnehmen.

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieser Vereinbarung aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung der Vereinbarung

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, wie folgt datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Haftung

Für Haftung und Schadensersatz gilt Art. 82 DS-GVO.

11. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von den Parteien für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Nebenabreden existieren nicht. Für Änderungen und Ergänzungen dieser Vereinbarung ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Diese Vereinbarung gilt mit Unterschrift des Auftraggebers unter dem Wartungsvertrag als angenommen.

ANLAGE
„Technisch-organisatorische Maßnahmen“

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

- Zutrittskontrolle

  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, wobei der Begriff räumlich zu verstehen ist.

  Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

  - Zutrittskontrollsystem mit Ausweislesern für Chipkarten
  - Schlüssel / Schlüsselvergabe
  - Türsicherung (elektrische Türöffner usw.)
  - Empfang für Besucher

  Der Zutritt zu den Gebäuden / Gebäudeteilen bei Bachner erfolgt mittels elektronischer IF-Zutrittskontrolle. Besucher / Fremde können die Gebäudeteile von Bachner nur nach Registrierung und Freigabe betreten. Sie werden vom Besuchten begleitet.

- Zugangskontrolle

  Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

  Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

  - Kontrolliertes Kennwortverfahren (Syntax mindestens 1 Sonderzeichen oder 1 Großbuchstabe, 1 Ziffer, Kleinschreibung, Mindestlänge = 8, regelmäßiger Kennwortwechsel alle 90 Tage, Wiederholzyklus = 24)
  - Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
  - Einrichtung eines Benutzerstammsatzes pro User und Funktion
  - Verschlüsselung von Datenträgern mit AES 256 Bit Zip-Programm oder VeraCrypt oder ähnlichen Programmen
  - Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)

  Für die Anmeldung an den Rechnersystemen verwendet jeder Mitarbeitende einen individuellen Benutzernamen und Kennwort (bzw. Administratoren-Login für Administratoren). Bei Bedarf werden sie manuell mittels Active Directory mit dem Intranet verbunden. Ein externer Zugang zum Intranet ist ausschließlich via VPN möglich. Zugang wird nur gewährt, wenn die Identifikationsdaten des Rechners, Benutzernamen und Passwort dort bekannt sind und übereinstimmen. Die Syntax der, in regelmäßigen Abständen zu wechselnden Passwörter, besteht aus 8 Stellen, Sonderzeichen oder Großbuchstabe, Kleinschreibung sowie mindestens eine Ziffer. Der Wiederholzyklus beträgt 24. Diese Bedingungen werden beim Passwortwechsel automatisch kontrolliert, und bei Nichteinhaltung erfolgt die Ablehnung des neuen Passworts. Wird ein Passwort nicht rechtzeitig geändert, erlischt es und der Zugang wird verwehrt.

- Trennungskontrolle

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

  Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

  - "Interne Mandantenfähigkeit" / Zweckbindung

- Funktionstrennung / Produktion / Test

Kundendaten werden strikt getrennt von anderen Kundendaten gespeichert und bearbeitet.

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen .

  Personenbezogene Daten können für einen etwaigen Datenexport bei Bedarf pseudonymisiert oder anonymisiert werden.

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

- Weitergabekontrolle

  Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle. Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen.

  Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

  - Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
  - Datensicherungen mittels Zip-Programm (z.B. WinZip oder ähnlichen Programmen) und 256 Bit AES- Verschlüsselung mit Passwort auf CD/DVD
  - Protokollierung

  Eine Weitergabe der Daten erfolgt im Regelfall nicht, außer wenn die Problemlösung eine Mitwirkung des Entwicklungsbereiches beim Auftragnehmer erfordert. Sollte diese erforderlich sein, so wird die Datensicherung entweder mittels Zip-Programm, 256 Bit AES- Verschlüsse- lung und mit Passwort auf CD/DVD gebrannt und per Post versendet, oder bei geringen Daten- mengen im Intranet mittels Zip-Programm und 256 Bit AES- Verschlüsselung direkt übertragen. Die Weitergabe von Datensicherungen wird in Dokumenten protokolliert.

- Eingabekontrolle

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

  Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

  Protokollierung mittels Logfile

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

- Verfügbarkeitskontrolle

  Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

  Maßnahmen zur Datensicherung (physikalisch / logisch):

  - Backup-Verfahren gemäß Leistungsvereinbarung

- Virenschutz / Firewall
- USV für Server

Alle Rechnersysteme sind mit einer Antiviren-Lösung ausgestattet. Die Aktualisierung der Antivirensignaturen erfolgt zeitnah nach deren Erscheinung über die zentral gesteuerte Endpoint Protection Lösung.

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

  Sicherheitskonzept (einschließlich Disaster Recovery Programm) und Service-Level-Agreements gemäß Leistungsvereinbarung

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

- Datenschutz-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- Rücksicherungen von Backups zu Testzwecken (dedizierte Kundendaten)
- Auftragskontrolle

  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers

  Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

  - Eindeutige Vertragsgestaltung gemäß Art. 28 DSGVO
  - Formalisierte Auftragserteilung (Managed Services Vertrag bzw. Einzelbeauftragungen in Textform)

  Der Auftragnehmer führt den beauftragten Leistungsumfang grundsätzlich selbst nach den Weisungen des Auftraggebers durch oder, soweit einschlägig, unter Zuhilfenahme von Unterauftragnehmer nach entsprechender Genehmigung durch den Auftraggeber. Grundsätzlich erfolgen beauftragte Änderungen nur in den Programmen und in der Auswertelogik.