Allgemeine Nutzungsbedingungen Datenschutz (ANB)

Vereinbarung zur Auftragsverarbeitung nach Art. 28 EU DS-GVO

Version	***Stand vom***	***Autor***	***Änderungen zur Vorversion***
1.1	*31.08.2022*	*GDI mbH Lau*	*Erstellung der ANB über die Auftragsverarbeitung nach Art. 28 DS-GVO*

Allgemeine Nutzungsbedingungen Datenschutz zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

der

Velser Bürokommunikation

GmbH & Co. KG

Im Erlengrund 4

46149 Oberhausen

– Auftragnehmer –

Der Kunde, der einen individuellen Kundenvertrag mit dem Auftragnehmer geschlossen hat, wird im Rahmen dieser Vereinbarung als

– Auftraggeber –

bezeichnet.

Präambel

Diese Bedingung beschreibt die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den dem individuellen Kundenvertrag / Leistungsvereinbarung / Aufträge des Kunden - **im Weiteren »Auftrag« genannt** - ergeben.

Sie findet Anwendung auf alle Tätigkeiten, die mit einem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Anwendungsbereich und Verantwortlichkeit

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im jeweiligen Vertrag und ggf. in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen jedes Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

Die datenschutzrechtlichen Pflichten des Auftragnehmers sind durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 2 Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung

Gegenstand und Dauer des Auftrags ergeben sich aus dem individuellen Dienstleistungsvertrag mit dem Kunden. Die Laufzeit dieser ANB richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser ANB nicht darüberhinausgehende Verpflichtungen ergeben.

Art und Zweck der Verarbeitung ergeben sich aus dem Leistungsumfang des Hauptvertrages mit dem Kunden.

§ 3. Kategorien von betroffenen Personen, Art der personenbezogenen Daten

a. Welcher Kreis von Personen durch die Datenverarbeitung betroffen ist, ergibt sich aus der Vorgabe des Auftraggebers bzw. aus dem Nutzungsumfang des Auftraggebers. In der Regel sind folgende Betroffenengruppen aufzuzeigen:

   Mitarbeiter des Auftraggebers
   Kunden des Auftraggebers
   Lieferanten des Auftraggebers
   Geschäftspartner des Auftraggebers

b. Die im Rahmen der Datenverarbeitung verarbeiteten Art der personenbezogenen Daten werden durch den Kunden bestimmt und vorgegeben. Regelmäßig umfasst die Datenverarbeitung die folgenden Kategorien personenbezogener Daten:

   - Kurzwahlziele

- Teilnehmer Namen und Durchwahlen
- E-Mail-Adressen, Benutzernamen
- Kontaktdaten von Ansprechpartnern

c. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jegliche Verlagerung in ein Drittland bedarf der Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

§ 4 Pflichten des Auftragnehmers

a. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 lit. a DS-GVO vor. In diesem 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.

b. Die Weisungen werden anfänglich durch eine Anlage zum Auftrag und die bestehende Praxis festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die in dem Auftrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

c. Die Weisungsempfänger des Auftragnehmers sind in der **Anlage 3** zu dieser Vereinbarung definiert.

d. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

e. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen **(Anlage 1)**. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Die Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass ein angemessenes oder vertraglich vereinbartes Schutzniveau nicht unterschritten wird. Eine Beschreibung der technisch-organisatorischen Maßnahmen des Auftragnehmers findet sich im Anschluss an diese Bedingungen.

f. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten.

g. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen

untersagt ist, die Daten außerhalb der Weisungen zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

h. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

i. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d DS-GVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

j. Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO, die er im Auftrag eines Verantwortlichen durchführt.

k. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

l. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

m. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

n. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Die vorstehend geschilderten Aufwände sind vom Auftraggeber an den Auftragnehmer zu dessen jeweils gültigen Preisen gemäß Preisliste zu vergüten.

§ 5 Pflichten des Auftraggebers

1. Der Auftraggeber benennt dem Auftragnehmer

    a) den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen,
    b) die weisungsberechtigten Personen, sowie
    c) den Umfang, in dem diese Personen nach b) weisungsberechtigt sind.

2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. daten- schutzrechtlicher Bestimmungen feststellt.

3. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt § 4 lit. l entsprechend.

4. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 6 Anfragen betroffener Personen

a. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO.

b. 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.

c. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 7 Nachweismöglichkeiten

a. Der Auftragnehmer weist dem Auftraggeber auf Verlangen die Einhaltung der in diesem Vertrag niedergelegten Pflichten, insbesondere der Einhaltung der technischen und organisatorischen Maßnahmen mit geeigneten Mitteln nach. Der Nachweis über die die Umsetzung der technischen und organisatorischen Maßnahmen kann erfolgen durch:
   i. Zertifikat zum Datenschutz
   ii. aktuelle Berichte des Datenschutzbeauftragten

b. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber oder ein von diesem beauftragter Prüfer jederzeit nach Absprache und mindestens 21-tägiger Voranmeldung berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme sowie Betreten und Besichtigung der Räumlichkeiten des Auftragnehmers, welche die Leistungserbringung für den Auftraggeber betreffen. Der Auftragnehmer verpflichtet sich insoweit, dem Auftraggeber oder einem von diesem beauftragten Dritten zu diesem Zwecke Zugang zu den Firmenräumen zu gewähren.

c. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

d. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

e. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 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.

§ 8 Subunternehmer (weitere Auftragsverarbeiter)

a. Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht (allgemeine schriftliche Genehmigung gem. Art. 28 Abs. 2 DS-GVO).

b. Die von dem Auftragnehmer hinzugezogenen Subunternehmer laut **Anlage 2** (mit Vertragsgrundlage) zu diesen ANB gelten mit Vertragsunterzeichnung als genehmigt.

c. Änderungen (Hinzuziehung oder Ersetzung) der Subunternehmer werden durch Veröffentlichung mitgeteilt. Der Auftragnehmer kann innerhalb von 14 Tagen nach Veröffentlichung der Änderung aus wichtigem Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben. Die Auftragserteilung an den Subunternehmer erfolgt erst nach Ablauf der Frist.

d. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus dem Dienstleistungsvertrag und diesen ANB dem Subunternehmer zu übertragen.

Der Auftragnehmer überzeugt sich von der Einhaltung der vertraglich zugesicherten Sicherheitsmaßnahmen nachweislich und gewissenhaft.

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

f. Der Sitz der hinzugezogenen Subunternehmer befindet sich in einem oder mehreren Mitgliedsstaaten der EU.

§ 9 Datenschutzbeauftragte(r) des Auftragnehmers

Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen ist

Herr Dipl. Inform. Olaf Tenti

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH
als externer Datenschutzbeauftragter
Körnerstr. 45, 58095 Hagen
Tel: +49 (0) 2331 / 35 68 32-0
Fax: +49 (0) 2331 / 35 68 32-1
E-Mail: datenschutz@gdi-mbh.eu
Internet: www.gdi-mbh.eu

Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

§ 10 Informationspflichten, Schriftformklausel, Rechtswahl

a. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

b. Änderungen und Ergänzungen dieser Bedingungen und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

c. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Bedingungen unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

d. Es gilt deutsches Recht.

Anlage 1: Beschreibung der technischen und organisatorischen Maßnahmen – Datensicherungsmaßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der **Vertraulichkeit, Integrität, Belastbarkeit und Verfügbarkeit** der im Auftrag verarbeiteten Informationen.

Die verarbeiteten personenbezogenen Daten unterliegen bei der Verarbeitung der Schutzkategorie „Normal“.

A. Vertraulichkeit

1. Zutrittskontrolle

(Kein unbefugter Zutritt zu Räumlichkeiten und Datenverarbeitungsanlagen)

1.1. Eingangstüren Gebäude und Büroräume:

- Die Türen nach außen sind
  - nur mit starrem Türknauf anstelle einer Klinke ausgestattet
  - mit einem automatischen Zuzieher ausgestattet
  - stets geschlossen, außer zum Betreten und Verlassen
  - während der Geschäftszeiten, außer zum Betreten und Verlassen geschlossen

- außerhalb der Geschäftszeiten fest abgesperrt
- Die Türen sind mit elektronischen Zutrittskontrollsystemen ausgestattet
- Es existieren biometrische Zugangssperren

1.2. Fenster:

- Fenster sind in allen Lagen außerhalb der Geschäftszeiten geschlossen
- Fenster sind mit zusätzlichen Sicherheitsschlössern gesichert
- Fenster sind in von außen zugänglichen Erdgeschoss- und Kellerlagen ganztags gesichert (Gitter u. ä.)

1.3. Serverräume:

- Es existiert ein manuelles Schließsystem
- Die Reinigung der Serverräume erfolgt innerhalb der Arbeitszeit durch internes Reinigungspersonal
- Serverräume sind mit einer Alarmanlage ausgestattet

1.4. Gebäudesicherung außerhalb der Geschäftszeiten:

- Es besteht eine Zugangsbeschränkung für Büro- und Geschäftsräume
- Die Gebäudesicherung außerhalb der Geschäftszeiten erfolgt
  - durch Videoüberwachung
  - durch Geländeüberwachung
- Das Gebäude wird an Wochenenden/Feiertagen bewacht
- Es existiert ein Einbruchsmeldesystem
- Es gibt Bewegungsmelder / Lichtschranken
- Die Gebäudesicherung erfolgt außerhalb der Geschäftszeiten
  - Durch eine Alarmanlage

1.5. Zutrittsregelung für betriebsfremde Personen:

- Ein zentraler Empfangsbereich (Sekretariat) ist vorhanden
- Zu- und Abgänge von betriebsfremden Personen werden festgestellt
  - oder Mitarbeiter und Videoüberwachung
  - und protokolliert
- **Hilfspersonen** (z.B. Reinigungsunternehmen) werden sorgfältig ausgewählt
- Betriebsfremden Personen ist der Aufenthalt im gesamten Unternehmensgebäude nur in Anwesenheit von Mitarbeitern gestattet

1.6. Zutrittsregelung für Mitarbeiter:

- Zutrittsmittel werden ausschließlich an Berechtigte ausgegeben
- Zutrittsmittel werden sofort eingezogen, wenn die Berechtigung erlischt
- Ein Generalschlüssel wird sicher verwahrt
- Bei Verlust eines Zutrittsmittels oder wenn ein ehemals Berechtigter ein Zutrittsmittel nicht freiwillig zurückgibt, wird das Zutrittsmittel individuell gesperrt
- Falls eine individuelle Sperrung des Zutrittsmittels nicht möglich ist, wird das Schließsystem ausgetauscht
- Es existiert ein Berechtigungskonzept zur Feststellung der Kopierberechtigung der Zugangsschlüssel

2. Zugangskontrolle

(Verhinderung der unbefugten Benutzung der Datenverarbeitungssysteme)

2.1 Sicherstellung des berechtigten Zugangs:

- Ein *Passwortsystem* für den Zugriff auf die Datenverarbeitungssysteme ist eingerichtet
- Jeder Berechtigte erhält eine individuelle Benutzerkennung und ein persönliches, geheim zu haltendes Passwort, das nicht an Dritte weitergegeben werden darf
- Es existiert organisatorisch eine Richtlinie zur Passwortsicherheit
- Zur Anmeldung muss ein Passwort eingegeben werden
  - Das Passwort besteht aus wenigstens 8 Zeichen (zufällig ausgewählten Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen)
- Generische Begriffe oder Eigennamen dürfen verwendet werden
- Eine Authentifizierung erfolgt über Benutzername *und* Passwort
- Es besteht eine Regelung für den Fall der Abwesenheit (Urlaub, Krankheit etc.)
- Berechtigungen werden regelmäßig kontrolliert
- Das Passwort wird sofort gesperrt, falls die Berechtigung erlischt
- Die dargestellten Passwortkonventionen werden *technisch* durch Systemeinstellungen gestaltet
- Die Nutzung von Datenverarbeitungssystemen durch Unbefugte wird verhindert durch:
  - Teilnehmerkennung

- An und Abmeldung zu Datenverarbeitungssystemen werden protokolliert

2.2 Schutz vor unberechtigtem Zugang von außen:

- Interne Netze werden nach dem Stand der Technik gegen Zugriffe von außen durch Firewalls abgeschottet
- Private Speichermedien sind vertraglich oder durch Organisationsanweisung verboten
- Es besteht eine Organisationsanweisung zum Download von Apps auf dienstliche Endgeräte
- Interne Netze werden nach dem Stand der Technik gegen Zugriffe von außen durch Verschlüsselung abgeschottet
- Bestimmungsgemäße Zugriffe von außen werden durch Virtual Private Network (VPN) abgesichert
- Daten / Festplatten von mobilen Endgeräten (Blackberry, Notebook, USB-Stick etc.) werden verschlüsselt
- Schutzprogramme und Administrationsprogramme auf Smartphones und Tablet-PCs sind im Einsatz
- Der Download von Apps auf dienstliche Endgeräte erfolgt nur durch die IT

3. Zugriffskontrolle

(Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entferne innerhalb des Datenverarbeitungssystems)

3.1 Berechtigungskonzept

- Der Zugriff auf Computersysteme und Netzlaufwerke ist auf berechtigte Benutzer beschränkt
- Der Zugriff auf Backup-Datenträger ist auf Systemadministratoren beschränkt
- Es existiert ein Berechtigungskonzept
- Es werden Benutzerprofile erstellt und den Datenverarbeitungssystemen zugeordnet
- Nicht benötigte Ports (USB) und Wechselmedien (CD/DVD-Geräte) werden deaktiviert und gesichert
- Datenträger werden vor einer Wiederverwendung mit geeigneter Software überschrieben
- Die Internet- und E-Mail-Nutzung erfolgt kontrolliert und organisiert
- Erfolgte / versuchte Sicherheitsverletzungen werden gemeldet und ausgewertet

Es bestehen differenzierte Zugriffe auf:

- Dateien
- Anwendungsprogramme

Es bestehen differenzierte Verarbeitungsberechtigungen:

- lesen
- ändern
- löschen

- Es besteht eine Trennung von Test- und Produktionsbetrieb
- Die Zugriffsmöglichkeiten sind zeitlich begrenzt (Nachtabschaltung)
- Die einzelnen Datenbanken sind verschlüsselt
- Datenträger werden zum Transport und zur Archivierung verschlüsselt
- Es wird mindestens eine 256bit-Verschlüsselung eingesetzt.

3.2 Trennungskontrolle und Pseudonymisierung

(Art. 32 Abs. 1 a DSGVO)

- Daten werden physisch getrennt auf gesonderten Systemen, Laufwerken und Datenträgern gespeichert
- Daten für mehr als einen Verantwortlichen werden in einer mandantenfähigen Datenbank verarbeitet
- Daten für mehr als einem Verantwortlichen werden mit eindeutiger Festlegung der Zugriffsrechte verarbeitet
- Entwicklungs-, Test- und Produktivsysteme sind getrennt
- Zugriffsschranken für einzelne Ordner, Datensätze, Felder (Datenbankrechte) sind festgelegt
- Besonders schützenswerte Daten (z. B. Personalbereich, besondere Datenarten) werden auf separaten Servern gespeichert

3.3 Zugriff auf Datenträger und Datenträgervernichtung:

- Nicht mehr benötigte Datenträger und Fehldrucke werden datenschutzgerecht entsorgt
- Datenträger werden ordnungsgemäß vernichtet, durch physische Zerstörung
- Papier wird vernichtet durch Reißwolf, Schredder
- Bei Lagerung von nicht mehr benötigten Datenträgern und Fehldrucken sind geeignete Datenschutzbehälter zur Verhinderung unbefugter Entnahmen im Einsatz
- Bereiche, in denen Datenträger aufbewahrt werden, sind besonders abgesichert

Datenträger werden ordnungsgemäß vernichtet durch

- Überschreiben (zertifiziertes Verfahren)
- zertifizierte Fremdfirma

- Die Entsorgung von Daten wird protokolliert (Vernichtungszertifikat etc.)

B. Integrität, Weitergabekontrolle, Auftragskontrolle und Fernwartung (Art. 32 Abs. 1 b DSGVO)

1. Weitergabekontrolle

(Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)

- Bei den zur Verarbeitung von Daten eingesetzten Systemen sind Bildschirme oder andere Ausgabegeräte so angeordnet, dass unbefugte Dritte keinen Einblick in Daten nehmen können
- Als Sicherheitsmaßnahmen werden Firewalls eingesetzt
- Auch bei der Weitergabe von Daten werden Passwörter mit Vorgaben für die Passwortsicherheit eingesetzt
- die Beauftragung zuverlässiger Transportunternehmen
- E-Mails werden TLS-verschlüsselt
    - Anhänge von E-Mails werden verschlüsselt
    - Passwörter werden auf getrennten Kommunikationswegen (z.B. Telefon, SMS) übermittelt
- Daten auf mobilen Datenträgern und auf Datenträgern in mobilen Endgeräten werden verschlüsselt

2. Eingabekontrolle und Protokollierung:

(Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungs-

systemen eingegeben, verändert oder entfernt worden sind)

- Unbefugte Eingaben, Veränderungen und Löschungen werden durch ein Passwortsystem verhindert
- Zugriffe sind anhand der *Benutzergruppen* nachvollziehbar

3. Fernwartung

- Eine Fernwartung von Datenverarbeitungsanlagen und/oder Software findet statt
- Es besteht eine gesicherte Verbindung bei Fernwartung
- Es wurde ein Wartungsvertrag abgeschlossen

Folgende Maßnahmen werden zur Sicherung der Fernwartung angewendet

- Ereignisauslösung vom Auftraggeber
- Virtual Private Network (VPN)

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

1. Verfügbarkeitskontrolle

(Schutz der Datenverarbeitungssysteme gegen Zerstörung bzw. Verlust)

Hardwareschutz wird durch folgende Maßmaßnahmen gewährleistet

- unterbrechungsfreie Stromversorgung (USV)
- Feuerlöschgerät im oder unmittelbar vor dem Serverraum
- Schutzsteckdosenleisten in Serverräumen und Archiven
- Einhaltung der einschlägigen Brandschutzvorschriften
- automatische Feuer- und Rauchmeldeanlagen

Die Ausführung arbeitsplatzfremder Software wird verhindert durch

- vertragliche Verbote und/oder
- Spamfilter
- Aktualisierung des Betriebssystems, der vorhandenen Betriebs- und Sicherheitssoftware (Updates und Patches)
- Lizenzüberwachung

Hardwareschutz wird außerdem durch folgende Maßnahmen gewährleistet

- Feuer- und Rauchmeldeanlagen
- Überwachung der Temperatur und Feuchtigkeit in Serverräumen
- Klimaanlage in Serverräumen
- Überspannungsfilter
- Sonstige Maßnahmen: Temperaturüberwachung, Einbruchmeldeanlage
  - Spezielle Schutzprogramme sind im Einsatz
  - Schutzprogramme werden regelmäßig aktualisiert (Update)

2. Belastbarkeitskontrolle

- Prüfungen der eigenen IT
- Kontrollen des betrieblichen Datenschutzbeauftragten
- Datenwiederherstellungs-Tests werden durchgeführt
  - Einsatz von spezieller Datensicherheitssoftware

D. Wiederherstellbarkeit der Daten und des Datenzugangs nach physischem oder technischem Zwischenfall und Kontrollverfahren

1. Datensicherung (Art. 32 Abs. 1 c DSGVO)

Normales Datenschutzniveau:

- Sicherungskopien werden nach dem Generationenprinzip in geeigneten zeitlichen Abständen erstellt

Der Datenbestand wird wenigstens

  - einmal täglich inkrementell
  - einmal wöchentlich vollständig auf externen Speichermedien

gesichert

- Sicherungsdatenträger werden betriebsextern sicher verwahrt
- Backup-Verzeichnisse werden geführt bzw. es existiert eine Backup-Verzeichnisstruktur
- Es gibt einen Notfallplan bzw. ein Recovery-Konzept
- Das Administrator-Passwort wird sicher aufbewahrt
- Die Eintrittspunkte für Schadsoftware sind minimiert (Abschaltung verzichtbarer Dienste)

2. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 d DSGVO)

- Die vorhandenen Dokumentationen der Datensicherheit werden regelmäßig auf Aktualität geprüft
- Es erfolgt mindestens jährlich ein technischer Check der Datenverarbeitungssysteme
- Sicherheitsvorfälle werden dokumentiert und ausgewertet
- Es besteht ein für Sicherheitsvorfälle geschultes Krisenteam
- Es erfolgen interne Audits durch den betrieblichen Datenschutzbeauftragten oder die IT

3. Organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs-1 d DSGVO)

3.1. Datenschutzbeauftragter:

- Ein betrieblicher Datenschutzbeauftragter ist erforderlich
- Ein betrieblicher Datenschutzbeauftragter wurde bestellt
- Stellung des betrieblichen Datenschutzbeauftragten:
  - extern

- Der Datenschutzbeauftragte oder von ihm oder der Geschäftsleitung beauftragte Mitarbeiter führen regelmäßig interne Kontrollen der Einhaltung der technischen und organisatorischen Maßnahmen der Datensicherheit durch

3.2. Vertraulichkeit der Mitarbeiter

- Alle Mitarbeiter, die personenbezogene Daten verarbeiten, sind auf Vertraulichkeit (das Datengeheimnis) verpflichtet
- Fremdpersonal ist ebenfalls auf Vertraulichkeit verpflichtet
- Datenschutzschulungen für die Mitarbeiter werden regelmäßig durchgeführt
- Die private Nutzung betrieblicher Kommunikationstechnik ist verboten
- Es wird Cloud-Computing nach datenschutzrechtlichen Vorgaben eingesetzt
- Es existiert ein dokumentiertes Datenschutzkonzept

E. Internetauftritt

- Es existiert eine Datenschutzerklärung/Datenschutzhinweise
- Es existiert eine Anbieterkennzeichnung
- kommerzielle Kommunikation / Inhalte werden gekennzeichnet
- Werden Cookies eingesetzt?
  - Auf Cookie-Sicherheit geachtet (HttpOnly Flag, Secure Cookie etc.) wird geachtet
- Es wird Google Analytics eingesetzt
  - Es erfolgt der Einsatz von Google Analytics unter folgenden Voraussetzungen:
  - Schriftlicher Vertrag zur Auftragsdatenverarbeitung
  - Hinweis in Datenschutzerklärungen
  - Widerspruchsmöglichkeit
- Es wird Social Media eingesetzt
  - es existieren Social Media Guidelines für den Umgang mit Facebook, Google+, Twitter etc.

Anmerkungen zum Internetauftritt:

Der Internetauftritt und die darin verwendeten Mechanismen wie Cookies, Google Analytics, etc. werden nicht bei Velser Bürokommunikation gespeichert oder ausgewertet, sondern lediglich vom Hoster der Online-Präsenz (11880.com) verwendet

Anlage 2: Subunternehmer des Auftragnehmers

Name/Firma	Adresse	Art der Verarbeitung	Kontaktdaten
ALE Deutschland GmbH	Stammheimer Straße 10 - 70806 Kornwestheim	Hersteller-Support	www.al-enterprise.com
WatchGuard Technologies GmbH	Wendenstraße 379 - 20537 Hamburg	Hersteller-Support	www.watchguard.de
New Voice Systems GmbH	Mörikestraße 17 – 71636 Ludwigsburg	Hersteller-Support	www.newvoice.de
Wortmann AG	Bredenhop 20 32609 Hüllhorst		www.wortmann.de
Microsoft		Office 365	www.microsoft.com

Anlage 3: Weisungsempfänger beim Auftragnehmer

Name	Kontaktdaten	Position
Beck, Petra	+49 (0)521 52409-0	Geschäftsführerin
Brosend, Daniel	+49 (0)208 941988-16	Geschäftsführer
Velser, Björn	+49 (0)208 941988-15	Handlungsbevollmächtigter