Vertrag über die Auftragsverarbeitung personenbezogener Daten

1) Einleitung, Geltungsbereich, Definition

1.1 Dieser Vertrag regelt die Rechte und Pflichten der Vertragsparteien (Auftraggeber und -nehmer) bei der Verarbeitung personenbezogener Daten im Auftrag.

1.2 Die Verarbeitung personenbezogener Daten erfolgt im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO.

1.3 Der Vertrag findet auf all die Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers in dessen Auftrag verarbeiten.

1.4 Die in diesem Vertrag verwendeten Begriffe beziehen sich auf die Definitionen in der EU-Datenschutzgrundverordnung (DSGVO). Danach versteht sich der Auftraggeber als „Verantwortlicher“ und der Auftragnehmer als „Auftragsverarbeiter“.

2) Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand: Der Auftragnehmer übernimmt folgende Verarbeitungen:Evaluation von 8D-Reports. Im Übrigen ergibt sich der Gegenstand der Auftragsverarbeitung aus dem zugrundeliegenden Hauptvertrag. Der Verarbeitung liegt der Vertrag zwischen den Parteien vom 22.07.2025im Folgenden „Hauptvertrag“) zugrunde.

2.2 Dauer

Die Verarbeitung beginnt mit Abschluss des Hauptvertrages und erfolgt auf unbestimmte Zeit. Sie endet mit Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei. Die Kündigungsfrist dieses Vertrages ist 4 Wochen.

3) Spezifizierung der Auftragsverarbeitung

3.1 Die Verarbeitung der Daten erfolgt durch:

* Erfassen
* Speichern
* Anpassen
* Verwenden
* Löschen

3.2 Der zugrundeliegende Zweck der Verarbeitung ist in der Leistungsbeschreibung des Hauptvertrages geregelt.

3.3 Es werden folgende Daten verarbeitet:

* Name
* Adressdaten
* Kommunikationsdaten (z.B. Telefon, E-Mail)
* Mitarbeiterdaten

8D-relevante Daten (u.a. Problembeschreibung, Ursachen, Maßnahmen)

3.4 Von der Verarbeitung betroffen sind:

* Mitarbeiter
* Kunden
* Lieferanten
* Ansprechpartner

3.5 Die Auftragsverarbeitung erfolgt grundsätzlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der DSGVO enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

4.) Pflichten des Auftragnehmers

4.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und der dokumentierten Weisungen des Auftraggebers, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer diese rechtliche Verpflichtung dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten.

4.2 Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

4.3 Der Auftragnehmer erstellt keine Kopien oder Duplikate der personenbezogenen Daten, ohne dass der Verantwortliche dazu eingewilligt hat.

4.4 Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

4.5 Der Auftragnehmer sichert zu, dass er die für den Verantwortlichen verarbeiteten personenbezogenen Daten von seinen anderen Datenbeständen strikt trennt.

4.6 Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

4.7 Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

4.8 Der Auftragnehmer gewährleistet, dass die zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Er trägt dafür Sorge, dass die zur Auftragsverarbeitung eingesetzten Personen in Bezug auf die Datenschutzanforderungen stets angemessen angeleitet und überwacht werden.

4.9 Bei der Erfüllung der datenschutzrechtlichen Pflichten des Auftraggebers, insbesondere bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten, bei Durchführung der Datenschutzfolgeabschätzung und bei einer notwendigen Konsultation der Aufsichtsbehörde hat der Auftragnehmer im erforderlichen Maße mitzuwirken und den Auftraggeber angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO). Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

4.10 Der Auftragnehmer verpflichtet sich den Auftraggeber im erforderlichen Umfang zu unterstützen, wenn der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen wird oder betroffene Personen ihm gegenüber Rechte geltend machen, soweit die Verarbeitung im Auftrag betroffen ist.

4.11 Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

4.12 Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

4.13 Die datenschutzrechtliche Beratung, Schulung und Unterstützung übernimmt "Dieter macht den Datenschutz", www.dieter-datenschutz.de.

5) Rechte und Pflichten des Auftraggebers

5.1 Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

5.2 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

5.3 Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte zu kontrollieren. Solche Kontrollen können insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch sonstige Kontrollen vor Ort vorgenommen werden. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.

5.4 Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Grundsätzlich finden Kontrollen nach angemessener Vorankündigung des Auftraggebers und zu den Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate, statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

6) Weisungsbefugnis

6.1 Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

6.2 Der Auftraggeber erteilt Weisungen in dokumentierter Form. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen sind vom Auftraggeber unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

6.3 Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

7) Technische und organisatorische Maßnahmen

7.1 Der Auftragnehmer gestaltet seine innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Er trifft insbesondere geeignete technische und organisatorische Maßnahmen, um einen dem Risiko angemessenen Schutz der Daten des Auftraggebers zu gewährleisten (Art. 32 Abs. 1 DSGVO). Er trifft diese technischen und organisatorischen Maßnahmen so, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sind. Die entsprechenden technischen und organisatorischen Maßnahmen ergeben sich aus der Anlage.

7.2 Die Maßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Diese Änderungen sind dem Auftraggeber unverzüglich mitzuteilen.

7.3 Wesentliche Änderungen an den technischen und organisatorischen Maßnahmen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

7.4 Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

7.5 Der Auftragsverarbeiter darf die Verarbeitung personenbezogener Daten im Rahmen des Auftrags auch durch Mitarbeiter in Privatwohnungen (Remote-Arbeit) durchführen lassen. Dabei verpflichtet sich der Auftragsverarbeiter, sicherzustellen, dass die Vorgaben des Datenschutzes und der Datensicherheit, wie sie in diesem Vertrag und den geltenden gesetzlichen Bestimmungen festgelegt sind, auch bei der Remote-Arbeit eingehalten werden.

8) Regelungen zur Berichtigung, Löschung und Sperrung von Daten

8.1 Der Auftragnehmer wird Daten nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

8.2 Den diesbezüglichen Weisungen wird der Auftragnehmer jederzeit Folge leisten. Dies gilt auch über das Vertragsende hinaus.

9) Unterauftragnehmer

9.1 Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

9.2 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall hinzuziehen.

9.3 Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

9.4 Der Auftraggeber muss seine Rechte, insbesondere auch das Kontrollrecht, auch gegenüber dem Unterauftragnehmer ausüben können.

9.5 Eine weitere Unterbeauftragung durch den Unterauftragnehmer ist nicht zulässig.

9.6 Der Auftragnehmer gewährleistet, bei der Auswahl des Unterauftragnehmers auf dessen Einhalten der erforderlichen technischen und organisatorischen Mindestanforderungen zu achten. Er leitet die im Auftrag verarbeiteten Daten erst dann an der Unterauftragnehmer weiter, wenn er sich davon überzeugt hat, dass der Unterauftragnehmer seine Verpflichtungen vollständig erfüllt hat. Dies hat der Auftragnehmer zu dokumentieren und dem Auftraggeber unaufgefordert vorzulegen.

9.7 Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel V der DSGVO enthaltenen Bedingungen sowie bei Einhaltung der sonstigen Bestimmungen dieses Vertrages möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.

9.8 Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

9.9 Die Unterauftragnehmer, die bei Abschluss des Vertrages mit der Verarbeitung personenbezogener Daten beschäftigt sind und mit Unterzeichnung dieses Vertrages als genehmigt gelten, sind hier gelistet: Anlage 1: Unterauftragnehmer

10) Mitteilungspflichten

10.1 Der Auftragnehmer teilt dem Auftraggeber unverzüglich mit, wenn der Schutz der im Auftrag verarbeiteten Daten aufgrund von Verstößen des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen verletzt wurde.

10.2 Der Auftragnehmer teilt dem Auftraggeber ebenso unverzüglich begründetet Verdachtsfälle auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten mit.

10.3 Die Mitteilung hat spätestens 24 Stunden nach Kenntniserlangung an eine vom Auftraggeber benannte Adresse zu erfolgen.

10.4 Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO darf der Auftragnehmer für den Auftraggeber nur nach vorheriger Weisung gem. Nr. 6 dieses Vertrages durchführen.

10.5 Ebenfalls mitzuteilen sind erhebliche Störungen bei der Auftragsverarbeitung.

10.6 Der Auftragnehmer informiert den Auftraggeber unverzüglich über angekündigte oder unangekündigt bereits stattgefundene Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit ein Bezug zur Auftragsverarbeitung besteht.

11) Beendigung des Auftrags

11.1 Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten oder Kopien derselben noch in der Verfügungsgewalt des Auftragnehmers, hat dieser die Daten nach Wahl des Auftraggebers entweder zu vernichten oder an ihn zu übergeben. Die Wahl hat der Auftraggeber innerhalb von 2 Wochen nach entsprechender Aufforderung durch den Auftragnehmer zu treffen. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399.

11.2 Der Auftragnehmer hat die unverzügliche Vernichtung bzw. Rückgabe der personenbezogenen Daten auf bei den Unterauftragnehmern zu erwirken.

11.3 Über die ordnungsgemäße Vernichtung der Daten führt der Auftragnehmer einen dokumentierten Nachweis, den er dem Auftraggeber auf Verlangen jederzeit vorzulegen hat.

11.4 Die Dokumentationen des Auftragnehmers über die ordnungsgemäße Datenverarbeitung hat dieser mindestens bis zum Ablauf des dritten Kalenderjahres nach Vertragsende aufzubewahren.

12) Haftung

12.1 Es gelten die Haftungsregelungen gemäß Art. 82 DSGVO.

13) Sonderkündigungsrecht

13.1 Wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, kann der Auftraggeber den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“).

13.2 Ein außerordentliches Kündigungsrecht steht dem Auftraggeber auch dann zu, wenn der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

13.3 Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

13.4 Handelt es sich nicht um einen schwerwiegenden Verstoß, sondern vielmehr um einen unerheblichen, setzt der Auftraggeber dem Auftragnehmer zunächst eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

13.5 Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrages oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Aufraggeber entstehen.

14) Sonstiges

14.1 Die Einrede des Zurückbehaltungsrechts i.S.d. § 273 BGB, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern, wird ausgeschlossen.

14.2 Auftraggeber und Auftragnehmer verpflichten sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages hinaus vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

14.3 Sollten die im Auftrag verarbeiteten Daten 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 an den personenbezogenen Daten des Auftraggebers bei dem Auftraggeber liegt.

14.4 Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

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

Anlage 1: Unterauftragnehmer

Die textelligence GmbH (Auftragnehmer) nimmt für die Datenverarbeitung im Auftrag der textelligence-Kunden (Auftraggeber) Leistungen von Dritten in Anspruch, die im Auftrag der textelligence GmbH Daten verarbeiten (Subunternehmer).

Die folgenden Unternehmen sind als Subunternehmer genehmigt:

|  |  |  |  |
| --- | --- | --- | --- |
| Name des Unternehmens | Standort | Dienstleistung | Anwendbares Datenschutzrecht/Zertifizierung |
| Centron GmbH Heganger 29 D-96103 Hallstadt | D | Cloud GPU | DSGOV, dt. Datenschutzrecht, ISO 27001 |
| Widas ID GmbH Maybachstraße 2 D-07044 Wimsheim | D | CIDAAS: Identity & Access Management | DSGOV, dt. Datenschutzrecht, ISO 27001 |
| Formbricks GmbH Kuhnkestraße 6 D-24119 Kiel | D | Umfragen | DSGOV, dt. Datenschutzrecht |
| Hetzner GmbH Industriestraße 25 D-91710 Gunzenhausen | D | Didicated Server | DSGOV, dt. Datenschutzrecht, ISO 27001 |
| Stripe Payments Europe 1 Grand Canal Street Lower Dublin D02 H210, Irland | EU | Bezahlsystem | DSGVO |
| Usercentrics GmbH Sendlinger Straße 7 D-80331 München | D | Consent Management | DSGOV, dt. Datenschutzrecht, ISO 27001 |

Anlage 2: Technische und organisatorische Maßnahmen

Der Verantwortliche hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert. Der allgemeine Teil (Grundsätzliche Maßnahmen) beschreibt technische und organisatorische Maßnahmen die unabhängig von den jeweiligen Dienstleistungen und Services, Standorten und Kunden gelten. In den darauf folgenden Abschnitten sind Maßnahmen beschrieben, die über die im allgemeinen Teil dokumentierten Maßnahmen hinaus gelten.

1) Grundsätzliche Maßnahmen

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

* Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung systematisch überwacht sowie anlassbezogen und mindestens halbjährlich evaluiert wird.
* Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und alle notwendigen Umsetzungsverfahren.
* Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe und Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren.
* Die an Mitarbeiter, im Hinblick auf die Verarbeitung personenbezogener Daten erteilten Berechtigungen, sowie ausgegebenen Schlüssel, Zugangskarten oder Codes jeglicher Art, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten, gemäß eines Berechtigungskonzeptes, eingezogen, bzw. entzogen.
* Alle Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden (z.B. Reinigungs-, Wachpersonal, etc.), werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten. Bei Dienstleistern, die nicht nebengeschäftlich tätig werden, wird der Schutz von personenbezogenen Daten und die Sicherung der Rechte und Pflichten von Auftraggebern/Auftragnehmern einer Auftragsverarbeitung gewährleistet. Dies gilt auch für vergleichbare Situationen mit einem Datentransfer in sogenannte Drittstaaten.
* Mitarbeiter werden im Hinblick auf den Datenschutz geschult, belehrt und instruiert, auf Verschwiegenheit verpflichtet, wie auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen bzw. sind solche konkret geplant. Der Schutz der Daten in diesen Konstellationen ist gewährleistet.
* Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).
* Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.

2) Zutrittskontrolle

Alle Maßnahmen, die dazu geeignet sind, den Zutritt für Unbefugte zu den Datenverarbeitungsanlagen zu verhindern.

Umgesetzte Maßnahmen:

* Automatisches Zugangskontrollsystem
* Chipkarten / Transpondersysteme
* Türen mit Knauf Außenseite dauerhaft Personal anwesend
* Regelung der Schlüsselausgabe
* Besucherbuch / Protokoll der Besucher
* Zutrittsregelungen für Besucher
* Besucher in Begleitung durch Mitarbeiter
* Sorgfalt bei Auswahl der Reinigungsdienste

Geplante Maßnahmen:

* Manuelles Schließsystem
* Sicherheitsschlösser

3) Zugangskontrolle / Zugriffskontrolle

Alle Maßnahmen, die geeignet sind, die Nutzung der Datenverarbeitungssysteme durch Unbefugte zu verhindern sowie alle Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Umgesetzte Maßnahmen:

* Login mit Benutzername + Passwort
* Login mit biometrischen Daten
* stets aktueller Virenschutz
* stets aktuelle Softwareversionen
* Verschlüsselter Datentransfer über https/TLS oder vergleichbare Schutzsysteme
* Personal Firewall
* Netzwerk Firewall
* Verschlüsselung Smartphones
* Automatische Desktopsperre
* Verschlüsselung von Notebooks / Tablet
* Verwalten von Benutzerberechtigungen
* Erstellen von Benutzerprofilen
* Richtlinie „Sicheres Passwort“
* Richtlinie „Löschen / Vernichten“
* Richtlinie „Clean desk“
* Richtlinie zum Einsatz von USB-Sticks
* Richtlinie zur Bildschirmsperrung
* Allg. Richtlinie Datenschutz und / oder Sicherheit
* Mobile Device Policy
* Anleitung „Manuelle Desktopsperre“
* Aktenschredder
* Physische Löschung von Datenträgern
* Einsatz Berechtigungskonzepte
* Minimale Anzahl an Administratoren
* Verwaltung Benutzerrechte durch Administratoren

4) Weitergabekontrolle

Alle Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Umgesetzte Maßnahmen:

* E-Mail-Verschlüsselung (S/MIME, PGP, TLS, vergleichbar)
* Daten werden nur an autorisierte Dritte weitergegeben
* Pseudonymisierung
* Dedizierte Weitergabeberechtigungen
* Bereitstellung über verschlüsselte Verbindungen wie sftp, https

5) Eingabekontrolle

Alle Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Umgesetzte Maßnahmen:

* Protokollierung von Dateneingaben-, Änderungen und Löschungen
* Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
* Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
* Klare Zuständigkeiten für Löschungen
* Administratoren- und Stellvertreterkonzept

6) Auftragskontrolle

Alle Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Umgesetzte Maßnahmen:

* Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
* Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
* Schriftliche Weisungen an den Auftragnehmer
* Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
* Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
* Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
* Regelung zum Einsatz weiterer Subunternehmer
* Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

7) Verfügbarkeitskontrolle / Integrität

Alle Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Umgesetzte Maßnahmen:

* Feuer- und Rauchmeldeanlagen
* Technischer Schutz vor Datenverlust und unbefugten Zugriffen durch Virenschutz, Anti-Spyware und Spamfilter

Geplante Maßnahmen:

* Backup & Recovery-Konzept (ausformuliert)
* Ständige Kontrolle des Backup- und Recoverykonzepts

8) Gewährleistung des Zweckbindungs-/Trennungsgebotes

Alle Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Umgesetzte Maßnahmen:

* Physikalische Trennung (Systeme / Datenbanken / Datenträger)
* Steuerung über Berechtigungskonzept
* Festlegung von Datenbankrechten