Anlage 1
zum Vertrag zur Auftragsverarbeitung
Allgemeine technische und organisatorische Maßnahmen

Präambel

Die in dieser Anlage 1 aufgeführten technischen und organisatorischen Maßnahmen werden allgemein aufgeführt. Es versteht sich von selbst, dass die TecArt GmbH entsprechende detaillierte Maßnahmen ergreift die Daten des Auftraggebers im Rahmen des Hauptauftrages sowie des Vertrages zur Auftragsverarbeitung besonders sorgfältig durch geeignete Maßnahmen zu schützen. Hierzu zählt insbesondere, dass wir in dieser Anlage nicht alle Details in der Form offen legen, da diese sicherheitsrelevant sind. Die TecArt GmbH hält detaillierte technische und organisatorische Maßnahmen bereit und wird diese im Rahmen von Audits, Prüfungen und Zertifizierungen den entsprechenden Institutionen zur Verfügung stellen.

Hierzu verweisen wir auf die Regelungen des Vertrages § 6 Abs. 2.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DS-GVO)

a) Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz, Alarmanlagen, Videoanlagen;

Maßnahmen zur Zutrittskontrolle bei der TecArt:

- Die Gebäude der TecArt sind an den systemkritischen Punkten über Zutrittskontrollfunktionen nur den autorisierten Personen zugänglich.
- Alle Etagentüren sind permanent verschlossen, ebenso unbesetzte Büros. Eingangsbereiche und Fenster sind außerhalb der Geschäftszeiten fest verschlossen.
- Zusätzlich hierzu ist der Rechenzentrumsbereich speziell gesichert. Der Zutritt ist nur solchen Mitarbeitern gestattet, deren Aufgabengebiet sich auf die Betreuung des Rechenzentrumsbetriebes erstreckt. Nur diesen Mitarbeitern wird der Zutritt nach vorheriger Anmeldung freigeschaltet. Die Zutritte werden protokolliert.
- Unter Berücksichtigung der geltenden Besucherregelung der TecArt können sich Besucher, Gäste und Schulungsteilnehmer nur im Bereich der TecArt Akademie frei bewegen. Der Zutritt zu den Büroetagen ist nur in Begleitung von TecArt-Personal gestattet. Der Zutritt zum Rechenzentrum ist diesem Personenkreis untersagt.
- Personal von Fremdfirmen ist der Zutritt zu Wartungszwecken nur in Begleitung und unter ständiger Beobachtung befugter Mitarbeiter(innen) der TecArt gestattet. Mit diesen Fremdunternehmen ist eine Vereinbarung zur Auftragsdatenverarbeitung abgeschlossen.
- Außerhalb der Bürozeiten sind die Gebäude entsprechend gesichert und werden regelmäßig überprüft.

b) Zugangskontrolle
Keine unbefugte Systembenutzung, z.B.: sichere Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

Maßnahmen zur Zugangskontrolle bei der TecArt:

- Alle Systeme der TecArt werden ständig aktualisiert und regelmäßig gesichert. Systeme zur Datenverarbeitung unterliegen nochmals besonderen Sicherheitsmechanismen und werden entsprechend geloggt, um bei Bedarf entsprechende Auswertungen vornehmen zu können.
- Das Netzwerk der TecArt ist gegen externe Zugriffe durch eine Firewall abgeschirmt. Aus fremden Netzen kann und darf nur unter bestimmten Voraussetzungen zugegriffen werden.
- Server, die eine Verbindung zum Internet haben stehen in einer DMZ und werden ständig Überwacht mit entsprechender Protokollierung von Ereignissen.
- Alle Rechner sind nur über Useranmeldung mit persönlichem Passwort zugänglich. Die Anmeldungen werden protokolliert und können im Bedarfsfall ausgewertet werden.
- Passwörter werden ausschließlich durch den Benutzer erstellt und können nicht durch Administratoren eingesehen werden.

c) Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

Maßnahmen zur Zugriffskontrolle bei der TecArt:

- Sämtlicher Zugriff auf die Server der TecArt sowie die Arbeitsplatzrechner und Notebooks der Außendienstmitarbeiter erfolgt ausschließlich über persönliche Authentifizierung. Anhand der Userkennung werden spezielle, persönliche Nutzungsrechte für bestimmte Programme und Netzwerkverzeichnisse erteilt.
- Die Zuweisung von Rechten und Rollen erfolgt benutzerindividuell (abgestufte Zugriffsberechtigung).
- TecArt setzt entsprechende Passwortregelungen ein.
- Zugänge werden nach einer entsprechenden Anzahl von Fehlversuchen gesperrt.
- Es ist verboten, Passwörter an andere Personen weiter zu geben.
- Die Zugriffe auf die Server der TecArt werden protokolliert und können bei Bedarf durch berechtigte Personen ausgewertet werden.
- Innerhalb der TecArt werden die Zugriffsmöglichkeiten auf das „Need to Know"-Prinzip beschränkt.
- Es finden regelmäßig Schulungen zum Datenschutz und zur Datensicherheit statt.

d) Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

Maßnahmen zur Trennungskontrolle bei der TecArt:

- Die unterschiedlichen Anwendungen erfüllen dies auf unterschiedliche Art und Weise, die das Prinzip der Datenminimierung garantieren.
- Für unterschiedliche Anwendungen gibt es separate Verzeichnisstrukturen, deren Verwaltung ebenfalls sicherstellt, dass nur berechtigte Zugriffe erfolgen können.
- Weitergehende Maßnahmen, wie z.B. Netzwerksegmentierung, der Einsatz kundenspezifischer, virtueller Serversysteme, die Vergabe von Zugriffsrechten, sind im Hauptvertrag geregelt.

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a) DS-GVO; Art. 25 Abs. 1 DS-GVO)
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.

Maßnahmen zur Pseudonymisierung bei der TecArt:

- Da personenbezogene Daten in den Anwendungen der TecArt ursächlich entstehen und im Rahmen der Bearbeitung stets nach den Attributen aufgerufen werden, die als erste zu pseudonymisieren wären, würde eine Pseudonymisierung in diesen Anwendungen zu nicht tragbaren Behinderungen der Sachbearbeitung und mangelhaftem Antwortzeitverhalten führen und wird deshalb nicht durchgeführt.

2. Integrität (Art. 32 Abs. 1 lit. b) DS-GVO)

a) Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

Maßnahmen zur Weitergabekontrolle bei der TecArt:

- Personenbezogene Daten werden im Online Verfahren ausschließlich über VPN-Verbindungen bzw. über SSL/TLS verschlüsselte Verbindungen übertragen.
- In begründeten Ausnahmefällen kann nach Rücksprache mit und Genehmigung durch den Auftraggeber eine passwortgeschützte oder verschlüsselte Datei per E-Mail versandt werden. Die Übermittlung des Schlüssels erfolgt auf einem anderen Weg.

- Personenbezogene Daten, die über Datenträger weitergegeben werden, werden komprimiert und verschlüsselt gespeichert.
- Mit allen Auftragsverarbeitern wird eine schriftliche Vereinbarung zur Auftragsverarbeitung abgeschlossen.
- Ausschussmaterial, Testausdrucke sowie defekte oder ausgesonderte Speichermedien werden durch ein zertifiziertes Entsorgungsunternehmen bzw. zum Teil durch Schredder der Schutzklasse 2 nach DIN 66399 datenschutzgerecht vernichtet.
- Daten, die aufgrund von gesetzlichen Vorgaben an die entsprechenden Stellen zu übertragen sind, wie zum Beispiel Steuer- und Sozialversicherungsdaten werden auf den durch den Gesetzgeber vorgeschrieben Wegen und mit den dort vorgegeben Verschlüsselungen übertragen.
- Alle Mitarbeiter, die mit personenbezogenen Daten Umgang haben, sind schriftlich zur Verschwiegenheit verpflichtet.

b) Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

Maßnahmen zur Eingabekontrolle bei der TecArt:

- In dem von der TecArt eingesetzten Programm TecArt ist implementiert, dass jederzeit, insbesondere auch nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in dem System eingegeben, verändert oder gelöscht wurden.
- Hierzu werden diese Informationen in einer speziellen Tabelle innerhalb der Datenbank abgespeichert.
- Bei Fernwartungen hat die Protokollierung auf der Auftraggeberseite zu geschehen.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DS-GVO)

a) Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

Maßnahmen zur Verfügbarkeitskontrolle bei der TecArt:

- Die Sicherheit der Daten und deren Verfügbarkeit wird durch ein mehrstufiges Backup- und Recovery-Konzept gewährleistet, sowie die redundante Auslegung zentraler Systeme und ihrer Komponenten.
- Systeme und Datenbanken werden online gesichert, um eine größtmögliche Verfügbarkeit im Rahmen der vereinbarten Leistungserbringung zu gewährleisten.
- Die Server der TecArt sind durch intelligente USV gegen einen plötzlichen Ausfall der Stromversorgung geschützt.
- Im gesamten Gebäude existiert eine Brandmeldeanlage. Der Serverraum ist durch eine automatische Feuerlöschanlage gesichert.
- Im gesamten Gebäude besteht Rauchverbot.
- Das gesamte Gebäude ist durch eine Alarmanlage mit automatischer Benachrichtigung des Sicherheitsunternehmens geschützt.
- Es erfolgen regelmäßige Datensicherungen sowie permanente Datenspiegelung.
- Der Zugang zu den Servern ist durch mehrstufige Sicherheitskomponenten abgesichert.
- Die Zugriffe auf die zentrale Anwendung im Rechenzentrumsbetrieb erfolgt über redundante Leitungen. .

b) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DS-GVO);

Maßnahmen zur raschen Wiederherstellbarkeit bei der TecArt:

- Systeme und Datenbanken werden online gesichert, um eine größtmögliche Verfügbarkeit zu gewährleisten.
- Zusätzlich werden die Daten des Rechenzentrumsbetriebs ohne Zeitversatz auf separaten Systemen gespiegelt gespeichert.

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

a) Datenschutz-Management

Datenschutz-Management bei der TecArt:

- Es gelten die Grundsätze:
  - Datenschutz ist Aufgabe des gesamten Unternehmens.
  - Es werden datenschutzfreundliche Technologien eingesetzt, wo immer das möglich und wirtschaftlich ist.
  - Die IT-Sicherheit muss auf dem aktuellen Stand der Technik sein.
- Das Unternehmen legt Strategien fest hinsichtlich:
  - Zuweisung von Zuständigkeiten.
  - Risikobewertung.
  - Durchführung von Kontrollen.
  - Sensibilisierung und Schulung der Mitarbeiter.
- Wenn immer das erforderlich ist, werden die eingesetzten Verfahren einer dokumentierten Datenschutz-Folgenabschätzung unterzogen, bestehend aus:
  - Schutzbedarfsfeststellung.
  - Risikoanalyse.
  - Sicherheitskonzept.
- Durchgeführte Verarbeitungstätigkeiten – auch als Auftragsverarbeiter – werden einheitlich und nachweisbar dokumentiert.
- Weisungen von Kunden im Rahmen einer Auftragsverarbeitung werden kundenbezogen dokumentiert.
- Ausgeführte Tätigkeiten im Rahmen der Auftragsverarbeitung werden kundenbezogen dokumentiert.
- Alle von der TecArt eingesetzten Auftragsverarbeiter werden Prüfungen unterzogen. Dabei werden die gleichen Maßstäbe angesetzt, die für die eigene Verarbeitung auch gelten.

b) Incident-Response-Management

Incident-Response-Management bei der TecArt:

Es bestehen interne Richtlinien, Handlungsanweisungen und Prozesse zum Datenschutz, die bei Bedarf oder sich ändernden Voraussetzungen erweitert bzw. ergänzt werden.

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Das Treffen geeigneter technischer und organisatorischer Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Maßnahmen zu datenschutzfreundlichen Voreinstellungen bei der TecArt:

- Es werden von der TecArt für den jeweiligen Verarbeitungszweck geeignete technische und organisatorische Maßnahmen getroffen, die jedem Auftraggeber im Rahmen der Vereinbarung einer Auftragsverarbeitung zugesichert werden. Spätere Änderungen dieser Maßnahmen können nur zu besseren Zuständen führen, niemals zu einer Verschlechterung.
- In den von der TecArt erstellten aktuellen Lösungen gilt stets die höchste Schutzstufe bei der Erstellung neuer Objekte in der Berechtigungs- und Zugriffsverwaltung. So hat beispielsweise eine neu erstellte Kennung zunächst keinerlei Rechte im System und erhält diese erst, wenn ihr ein Profil (Sammlung von Rechten) zugeordnet wird.
- Berechtigungsobjekte ohne Zuordnung einer Satzebenen-Berechtigung dürfen zunächst keine Daten-Inhalte sehen. Erst durch Zuweisung einer Satzebene werden die dort definierten Dateninhalte zur Benutzung freigegeben.
- Erstellte Auswertungsergebnisse und Listen – ob im Einzelfall oder fallübergreifend – können nur von daraufhin berechtigten Personen eingesehen werden.

- Der Betrieb des TecArt-eigenen Rechenzentrums für Application Service Providing (ASP; Daten der Kunden werden im TecArt-Rechenzentrum aufbewahrt und gewartet), ist BSI-Grundschutz zertifiziert nach ISO 27001. Somit gelten für diesen Geschäftsbereich alle Schutz- und Sicherungsmaßnahmen, die diese Norm vorgibt. Es erfolgen jährliche Reviews bzw. Nachprüfungen.

d) Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Maßnahmen zur Auftragskontrolle bei der TecArt:

- Im Rahmen der Geschäftsprozesse liegt es in der Verantwortung der Führungskräfte der TecArt, in deren Aufgabenbereich die jeweiligen datenschutzrelevanten Dienstleistungen fallen, sicherzustellen, dass personenbezogene Daten nur entsprechend der Weisungen der Auftraggeber (grundsätzlich schriftlich vereinbart) und in Einklang mit den geltenden Rechtsvorschriften verarbeitet werden.
- Darüber hinaus stellt auch der betriebliche Datenschutzbeauftragte der TecArt sicher, dass der Auftragskontrolle genüge getan wird.
- Schriftliche Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO mit Regelungen zum Auftragsablauf.
- Eindeutige Regelung der Zuständigkeiten und Verantwortlichkeiten sowie zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers.
- Sorgfältige Auswahl von Lieferanten und Unterauftragnehmern. Die angemessene Etablierung und die Einhaltung eines Datenschutz-Managements sind – nach Möglichkeit – durch die Einhaltung von Verhaltensregeln und/oder Zertifizierungen nachzuweisen.
- Alle Mitarbeiter werden regelmäßig geschult, um die Einhaltung der Vorschriften der DS-GVO und die Einhaltung von Weisungen sicherzustellen. Es erfolgen regelmäßig Nachschulungen.
- Regelmäßige Prüfung der vereinbarten Regelungen durch den betrieblichen Datenschutzbeauftragten.
- Ansprechpartner und verantwortliche Projektmanager werden für den konkreten Auftrag bestimmt und schriftlich fest gehalten.

Hinweis zu den weiteren Anlagen:

Sind die Anlagen 2 und 3 kein Bestandteil des Vertrages zur Auftragsverarbeitung, gelten die Regelungen, wie in den §§ 2 und 7 dieses Vertrages beschrieben. Werden Regelungen zu Subauftragnehmern (Anlage 2) oder weiteren Weisungsberechtigten bzw. Weisungsempfangsberechtigten (Anlage 3) vereinbart, werden die Parteien entsprechende Anlagen erstellen und diesem Vertrag anhängen.