Anlage 2 zum Auftragsverarbeitungsvertrag

mit der opta data motion GmbH

Diese Auflistung der bei opta data motion GmbH getroffenen technischen und organisatorischen Maßnahmen im Datenschutz (TOMs) orientiert sich an den Vorgaben des § 9 BDSG(alt) und der Anlage zu § 9 Satz 1 BDSG(alt), diese Dokumentation ermöglicht eine strukturierte Dokumentation der TOMs, da es weder in der EU-Datenschutzgrundverordnung (DSGVO) noch im neuen Bundesdatenschutzgesetz (BDSG-Neu) dazu Vorgaben für nicht öffentliche Stellen gibt (§ 64 BDSG-Neu gilt findet bei nicht öffentlichen Stellen keine Anwendung). Diese Angaben dokumentieren auch die Forderungen des § 78a SGB X und des Art. 32 der DSGVO. Es soll Verantwortlichen (Auftraggebern) dazu dienen, ihren Prüf- und Dokumentationspflicht bei Auftragsverarbeitung gem. Art. 28 und 29 DSGVO, §29 KDG, §29 KDR-OG, §30 DSG-EKD und §80 SGB X zu erleichtern.

Auch entspricht die Auflistung der technischen und organisatorischen Maßnahmen im Datenschutz den Anforderungen der §26 KDG, §26 KDR-OG, §27 DSG-EKD.

Diese Aufstellung ist auch als Ergänzung zu einem bestehenden oder neuen, Art. 28, 29 DSGVO konformen, Dienstleistungsvertrag gedacht und kann jedem Verantwortlichen (Auftraggeber) auf Anforderung zur Verfügung gestellt werden. Die getroffenen Maßnahmen unterliegen den technischen Fortschritt und werden somit fortlaufend aktualisiert, wobei das bisher vorhanden Sicherheitsniveau nicht verringert wird. Erwähnenswert ist noch, dass die opta data motion GmbH ein nach DIN ISO 9001 zertifiziertes QM-System hat.

Die Daten, die bei der die opta data motion GmbH im Auftrag (Fernwartungsarbeiten) eingesehen werden können, sind als besonders sensibel eingestuft. Es handelt sich um personenbezogene Daten gemäß Art. 4 Nr. 1 und um Sozialdaten gemäß § 67 Abs. 2 SGB X in Verbindung mit besonderen Daten gemäß Art. 4 Nr. 15 DSGVO (Gesundheitsdaten).

Allgemeiner Teil

1. Name und Anschrift des Unternehmens:
   opta data motion GmbH
   Wilhelmshöher Allee 273
   34131 Kassel
2. Ansprechpartner mit Telefon, Fax und E-Mail:
   Frau Maya Leise
   Tel.: 0201 / 695049 00
   Fax: 0201 / 695049 35
   E-Mail: motion@optadata-gruppe.de
3. Name der Geschäftsführer:
   Martin Jöllenbeck, Rainer Strassl
4. Name und Kontaktdaten des Datenschutzbeauftragten:
   Joachim Kramer
   Datenschutz Kramer & Kramer GmbH
   Elsternweg 24
   42555 Velbert
   Tel.: 02052 / 92897 -66
   Fax: 02052 / 92897 -67
   E-Mail: info@datenschutz-kramer.de
5. Datenschutzbeauftragter:

   5.1. Bestellung Datenschutzbeauftragter:
   - Firma Datenschutz Kramer & Kramer GmbH besitzt über 35 Jahre Erfahrung im Datenschutz externer Datenschutzbeauftragter gem. § 4 f Abs. 2 BDSG(alt) bzw. Art.37
   - DSGVO und § 38 BDSG(neu)
   - schriftliche Bestellung vom 31.10.2013 liegt vor

   5.2. Qualifikation:
   - Datenschutz-Auditor (TÜV) Zertifizierungsstelle für Personal TAR-ZERT der TÜV Akademie Rheinland Nr. 19553
   - über 17 Jahre Erfahrung im IT-Bereich
   - regelmäßige Fortbildungen
   - Mitglied im Erfa-Kreis für Datenschutzbeauftragte der Region MEO
   - GDD Mitglied
   - Firma Datenschutz Kramer & Kramer GmbH besitzt über 35 Jahre
   - Erfahrung im Datenschutz

6. Mitarbeiter der opta data motion GmbH:
   - alle Mitarbeiter sind schriftlich zur Wahrung des Datengeheimnisses, der Schweigepflicht nach § 203 StGB, der Vertraulichkeit nach DS-GVO, BDSG(neu) und auf das Sozialgeheimnis nach § 35SGB I verpflichtet worden
   - die Verpflichtung erfolgte auf einem extra Formular
   - die der Verpflichtung zugrunde liegenden Gesetzestexte wurden allen Mitarbeitern gegen Unterschrift ausgehändigt
   - alle Mitarbeiter werden in regelmäßigen Abständen durch den bDSB geschult

7. Verzeichnis der Verarbeitungstätigkeiten:
   - das „Verzeichnis der Verarbeitungstätigkeiten" liegt vor und ist Bestandteil eines integrierten Managementsystems

Technische und organisatorische Maßnahmen:

Vertraulichkeit (Art. 32 Abs. 1b DSGVO)

8. In unserem Haus ist die räumliche **Zutrittskontrolle** folgendermaßen sichergestellt:
   - separater Empfangsbereich
   - zentrales Schließsystem
   - Besucher müssen klingeln
   - Haupteingangstür wird nachts zusätzlich mit einem extra Schlüssel verschlossen
   - Schlüsseldokumentation

9. Um das unbefugte Eindringen in unsere Systeme und Datenverarbeitungssysteme zu verhindern, verwenden wir folgende Zugangskontrollen:
   - verschlossener Serverschrank in einem separaten Serverraum, zudem nur ein eingeschränkter Personenkreis Zutritt (Mutterkonzern DIN ISO 27001 zertifiziert)
   - Benutzername und Kennwort
   - automatische Sperrung (Pausenschaltung)
   - Sperrung des Accounts bei wiederholter Falschanmeldung
   - datenschutzgerechte Passwortrichtlinien gem. BSI, Komplexität technisch erzwungen
   - Server mit zusätzlichen Administrator Passwörtern
   - Festplattenverschlüsselung mobiler Datenträger und mobiler Endgeräte

10. Wie wird der Zugriff (Zugriffkontrolle) auf verschiedene Daten bzw. Systeme geregelt:
    - durch differenzierte Berechtigungen, gesteuert durch die Anmeldung
    - extra Administrationspasswörter
    - Auswertung von Zugriffsprotokollen durch den Administrator möglich
    - programmierbare Firewalls regeln den Zugriff von außen
    - durch Zugriffsmöglichkeiten auf Benutzerebene im Rahmen der Fernwartungsmöglichkeiten (keine Adminrechte auf Server)

- VPN-Verbindung via TeamViewer mit telefonisch übermittelter
- Sitzungsnummer

11. Um Daten die zu unterschiedlichen Zwecken erhoben wurden oder um die Daten von Mandanten voneinander zu trennen (Trennungskontrolle), haben wir folgende Maßnahmen ergriffen:
    - es wird eine logische Trennung der einzelnen Systeme sowie der Daten vorgenommen (VM Server)
    - Kundendatenbanken werden getrennt voneinander gehalten
    - jeder Kunde erhält eine eindeutige Kundennummer
    - personelle Trennung einzelner Fachbereich (Verwaltung, CareMan Office, CareMan Dienstplan, VISION, IntraRett, CareMan FibuNet)

Integrität (Art. 32 Abs. 1b DSGVO)

12. Wir kontrollieren die Weitergabe (**Weitergabekontrolle**) personenbezogener Daten bei Übermittlung bzw. Übertragung oder bei Transport mit folgenden Maßnahmen:
    - für die Übermittlungen von bzw. zu Auftraggebern wird das Internet genutzt
    - bei den Verbindungen werden verschlüsselte Verbindungen genutzt
    - bei Fernwartungsarbeiten wird entweder Citrix GoToAssist oder Teamviewer benutzt
    - Fernwartungsarbeiten werden vom Auftraggeber freigeschaltet
    - VPN-Verbindung via TeamViewer mit telefonisch übermittelter Sitzungsnummer, der Kunde muss der Sitzung beiwohnen

    Nicht mehr benötigte Daten in Papierform bzw. nicht mehr gebrauchte oder defekte Datenträger, werden bei uns wie folgt entsorgt:
    - Daten in Papierform werden im Papierschredder der Sicherheitsstufe P- 4 gemäß DIN 66399 geschreddert
    - elektronische und optische Datenträger werden mechanisch zerstört
    - Daten von Auftraggeber, die zu Wartungsarbeiten bzw. Reparaturarbeiten zur odm überspielt wurden werden sofort nach Behebung des Fehlers zum Auftraggeber zurück übertragen und dort getestet. Ist der Test erfolgreich werden die Daten des Auftraggebers bei der odm umgehend gelöscht.
    - Tägliche Backups werden nach 4 Wochen überschrieben. Ausgelagerte Backups werden 10 Jahre aufbewahrt und dann gemäß DIN 66399 bzw. ISO IEC 21964 mechanisch vernichtet.
13. Wir gewähren die Nachvollziehbarkeit bzw. Dokumentation der Wartungsarbeiten bzw. Systemzugriffe mit folgenden Maßnahmen (Eingabekontrolle). Dadurch kann nachvollzogen werden, wer auf ein System bzw. Daten zugegriffen hat und wann:
    - durch Protokolle in den entsprechenden Programmen
    - durch Server Protokolle
    - Supportanfragen werden in Ticketsystemen protokolliert
14. Die Aufträge (Auftragskontrolle) unserer Kunden kontrollieren wir anhand folgender Möglichkeiten:
    - Fernwartungsarbeiten werden immer vom Auftraggeber aus initiiert
    - die odm kann nur nach vorheriger Freischaltung durch den Auftraggeber Fernwartungsarbeiten durchführen
    - durch die direkte Kontrolle des Kunden bei Fernwartungsarbeiten
    - Softwarewartungsverträge sowie Verträge gemäß Artt. 28, 29 DSGVO der so genannten Auftragsverarbeitung sind vorhanden

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

15. Folgende Sicherheitsmaßnahmen (Verfügbarkeitskontrolle) haben wir gegen zufällige oder mutwillige Zerstörung und gegen Verlust bzw. Sabotage von Daten ergriffen:
    - alle Server sind mit Raid-Systemen ausgestattet, die die Daten permanent spiegeln
    - automatisiertes Backupverfahren / Datensicherungskonzept
    - Dokumentation der Datensicherung
    - Sicherungskopien werden ausgelagert
    - alle Server sind an USVs angeschlossen
    - Virenschutz zentral auf Servern und Clients über die IT-Abteilung des Mutterkonzerns (DIN-ISO 27001 zertifiziert)
    - Firewalls zentral über die IT-Abteilung des Mutterkonzerns
    - 24h Rufbereitschaft
    - IT-Notfallplan vorhanden

Verfahren zur regelmäßigen Überprüfung und Bewertung der technischen und organisatorischen Maßnahmen im Datenschutz gem. Art. 32 Abs. 1d und Art. 25 Abs. 1 DSGVO

16. Datenschutzmanagement
    - Es ist zu gewährleisten, dass Verantwortlichkeiten festgelegt werden und die technischen und organisatorischen Maßnahmen regelmäßig überprüft und evaluiert werden.
    - eine Datenschutzleitlinie ist vorhanden
    - regelmäßige Schulungen der Mitarbeiter durch den Datenschutzbeauftragten
    - interne Audits werden regelmäßig durch den Datenschutzbeauftragten & das QM durchgeführt
17. Incident-Response-Management
    - Gibt es Richtlinien, Handlungsanweisungen und Prozesse zum Datenschutz, die bei Bedarf oder bei geänderten Voraussetzungen erweitert bzw. ergänzt werden?
    - Grafisch visualisierte Handlungsanweisungen für verschiedene Datenschutzprozesse wie z. B. Einbindung des DSB, Meldewege, Betroffenenrechte etc.