Anlage – Technisch-organisatorische Maßnahmen

Aufstellung für Auftraggeber der SPRINGER AKTIV AG zu den bei der SPRINGER AKTIV AG getroffenen technischen und organisatorischen Maßnahmen im Datenschutz.

Diese Auflistung, der bei der SPRINGER AKTIV AG getroffenen technischen und organisatorischen Maßnahmen, orientiert sich am Art. 32 DSGVO. Sie soll es ermöglichen, dem Auftraggeber seine Prüf- und Dokumentationspflicht bei Auftragsverarbeitung gem. Art. 28 und 29 DSGVO zu erleichtern. Die Bestimmungen des BDSG neu wurden berücksichtigt. Gleichzeitig ermöglicht diese Aufstellung eine strukturierte, übersichtliche und transparente Dokumentation der technischen und organisatorischen Maßnahmen.

Diese Aufstellung ist zudem als Ergänzung zu einem bestehenden oder neuen, Art. 28 und 29 DSGVO konformen, Auftragsverarbeitungsvertrag gedacht und kann jedem Auftraggeber/Verantwortlichen auf Anforderung zur Verfügung gestellt werden.

1 Allgemeiner Teil:

1.1. Name und Anschrift des Unternehmens:

SPRINGER AKTIV AG
Lengeder Str. 52
13407 Berlin

1.2. Ansprechpartner mit Telefon, Fax und E-Mail:

Herr Martin Hepper
Telefon: +49 30 4900030
Fax: +49 30 49000388

1.3. Name des Vorstandes:

Herr Martin Hepper, Herr Frank Hepper

1.4. Name und Kontaktdaten des Datenschutzbeauftragten:

Herr Joachim Kramer

Kramer Datenschutz OHG
Elsternweg 24
42555 Velbert

Tel.: 02052 / 92897-66
Fax: 02052 / 92897-67
E-Mail: j.kramer@datenschutz-kramer.de

1.5. Datenschutzbeauftragter:

1.5.1. Bestellung:

- *externer Datenschutzbeauftragter gem. Art. 37 DSGVO*
- *schriftliche Benennung vom 01.06.2009 liegt vor*

1.5.2. Qualifikation:

- *Datenschutz-Auditor (TÜV) Zertifizierungsstelle für Personal TAR-ZERT der TÜV Akademie Rheinland Nr. 19553*
- *über 30 Jahre Erfahrung im IT-Bereich*
- *regelmäßige Fortbildungen*
- *Mitglied im Erfa-Kreis für Datenschutzbeauftragte der Region MEO*
- *GDD Mitglied*
- *Firma Kramer Datenschutz OHG besitzt über 25 Jahre Erfahrung im Datenschutz*

1.6. Mitarbeiter der SPRINGER AKTIV AG:

- *alle Mitarbeiter sind nach § 5 BDSG schriftlich auf das Datengeheimnis verpflichtet, ab dem 25.05.2018 werden neue Mitarbeiter auf die Wahrung der Vertraulichkeit verpflichtet*
- *die Verpflichtung erfolgte auf einem extra Formular*
- *der Verpflichtung zugrunde liegenden Gesetzestexte wurden allen Mitarbeitern gegen Unterschrift ausgehändigt*
- *alle Mitarbeiter werden regelmäßig durch den bDSB bzw. von einem seiner Erfüllungsgehilfen zum Thema „Datenschutz und Datensicherheit“ geschult • nach EN ISO 13485:2012 zertifiziert*

1.7. Verfahrensverzeichnisse und Datenschutzbericht:

- *das „Verzeichnis der Verarbeitungstätigkeiten“ gem. Art. 30 DSGVO wird geführt und kann der zuständigen Aufsichtsbehörde für den Datenschutz zur Einsicht zugänglich gemacht werden*
- *für Verfahren, bei denen besondere Kategorien von Daten gem. Art. 9 Abs. 1 DSGVO (Gesundheitsdaten nach Art. 4 Nr. 15 DSGVO und) verarbeitet werden, wird eine Datenschutzfolgeabschätzung durchgeführt*
- *Ein Datenschutzbericht des externen Datenschutzbeauftragten liegt vor.*

2.Technisch - organisatorische Maßnahmen:

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

2.1.1. Zutrittskontrolle

Maßnahmen, durch die Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

- *Der Gebäudekomplex der SPRINGER AKTIV AG ist komplett umzäunt*
- *Der Haupteingang im Hauptgebäude ist immer verschlossen.*
- *Im EG befindet sich der Empfang, welcher zu den Geschäftszeiten besetzt ist. Besucher und Wartungspersonal müssen am Eingang klingeln, um in das Gebäude zu gelangen. Am Empfang werden sie dann von dem jeweiligen Mitarbeiter abgeholt und betreut.*
- *Die Büros der leitenden Angestellten werden beim Verlassen immer abgeschlossen.*
- *Der komplette Gebäudekomplex verfügt über ein Transponder-System mit den Zugangsberechtigungen festgelegt werden können.*
- *Es ist eine Dokumentation für die ausgegebenen Transponder vorhanden.*

2.1.2. Zugangskontrolle

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert werden:

- *Kabelgebundenes Netzwerk sowie W-Lan ○ W-Lan-Verschlüsslung WPA2 PSK*
- *Benutzername und Kennwort notwendig, um sich im Netzwerk anzumelden*
- *Die Server befinden sich in einem separaten Raum.*
- *Anmeldung ebenso in der Branchenlösung notwendig*

2.1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung 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:

- *durch differenzierte Berechtigungen, gesteuert durch die Anmeldung extra Administrationspasswörter*
- *Administrator vergibt auf ihm weisungsberechtigter Personen die entsprechenden Befugnisse*

- *Zugriffskontrolle findet ausschließlich über die Authentifizierung des Nutzers statt.*
- *Zugriff auf die Branchenlösung ebenfalls nur mit Benutzername und Passwort möglich*
- *VPN-Zugänge*

2.1.4. Trennungskontrolle

Maßnahmen, die sicherstellen, dass Daten, die zu unterschiedlichen Zwecken übermittelt wurden, auch getrennt verarbeitet werden:

- *verschiedene Systeme sind auf verschiedenen Servern installiert*
- *verschiedene Systeme sind auf verschiedenen VM Servern installiert*
- *durch Nutzeranmeldung am Netzwerk*
- *zentraler Domaincontroller sorgt für die Authentifizierung und Autorisierung der berechtigten Computer und Benutzer*

2.2. Integrität (Art. 32 Abs. 1 lit. b DSGVO

2.2.1. Weitergabekontrolle

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. Das überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- *Hardwarefirewalls kontrollieren den Internetverkehr.*
- *Es erfolgt keinerlei Datenweitergabe an unberechtigte Dritte.*
- *Für den Schutz des Netzwerkes wird eine Hardware Firewall und ein Virenschutz Business Software genutzt.*
- *automatische Updates sind aktiviert*

2.2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

- *durch die Netzwerkanmeldung*
- *in den Branchenlösungen durch die Miterfassung der Nutzerkennung*

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

2.3.1. Verfügbarkeitskontrolle

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

- *automatisiertes tägliches Backupverfahren (Datensicherung) auf NAS und auf Magnetbänder*
- *Datensicherung in einem anderen Brandabschnitt*
- *Datensicherungsdokumentation des automatisierte Backupverfahren*
- *Alle Server sind mit RAID-Systemen ausgestattet die die Daten permanent spiegeln*
- *alle Server sind an USV's angeschlossen*
- *Der Serverraum ist mit einer Klimaanlage und Rauchmelder ausgestattet.*

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

2.4.1. Auftragskontrolle

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

- *dokumentierte Prozessabläufe*
- *AV-Verträge*

Velbert, 08.05.2018

Ort, Datum *externer betrieblicher Datenschutzbeauftragter*