Konzept für Datenschutz und Datensicherheit

Stand: 13.01.2021

Datenschutz und Datensicherheit im Scan-Zentrum der IngA Service GmbH

1. Unser Verständnis von Datenschutz

Die IngA Service GmbH fühlt sich und ist als Anbieter von Dienstleistungen im Bereich Dokumentendigitalisierung (Scan-Zentrum) den gesetzlichen und hohen ethischen Standards an Datenschutz und Datensicherheit verpflichtet. Berücksichtigung findet dabei insbesondere der Schutz personenbezogener Daten, vor allem, wenn diese in besonders sensibler Form, z. B. Sozialdaten oder Gesundheitsdaten, vorliegen. Ein ebenso hohes Schutzniveau stellen wir für Geschäftsdaten unserer Kunden sicher, insbesondere unter dem Blickwinkel, dass diese auch Geschäftsgeheimnisse enthalten können.

Unsere internen Regeln zum Datenschutz und zur Datensicherheit beinhalten verbindliche Vorgaben zu Verfahren, Verantwortlichkeiten und Schutzmaßnahmen zur Sicherung eines angemessenen Schutzniveaus. Unser internes Datensicherheitsmanagement stellt durch regelmäßige Schulungen die Vermittlung des entsprechenden Wissens sicher.

Im Interesse unserer Kunden und unserer Mitarbeitenden gewährleistet die IngA Service GmbH gemäß den Grundwerten der IT-Sicherheit die Verfügbarkeit der IT-Systeme, Programme und Daten. Sie schützt deren Integrität und verhindert Missbrauch. Sie stellt die Funktionsfähigkeit und Vertraulichkeit von Arbeitsergebnissen und Produkten sicher und hält rechtliche Bestimmungen zu Datenschutz und IT strikt ein.

Die Geschäftsführung steuert den Sicherheitsprozess, entwickelt gemeinsam mit den IT-Verantwortlichen und dem Datenschutzbeauftragten, die Maßnahmen weiter und prüft die Einhaltung von Sicherheitsvorkehrungen.

2. Unser Datenschutzbeauftragte

Datenschutzbeauftragter der IngA Service GmbH ist Herr Rechtsanwalt Jörg Leuchtner, Freiburger Datenschutzgesellschaft. Er gewährleistet die Erfüllung der gesetzlichen Aufgaben eines betrieblichen Datenschutzbeauftragten aus Art. 39 EU-DSGVO.

3. Besondere Hinweise zum Schutz personenbezogener Daten (EU-DSGVO)

Um den Schutz personenbezogener Daten im Sinne der EU-DSGVO zu gewährleisten, wurde anhand der gesetzlichen Vorgaben der Handlungsbedarf eruiert. Als Ergebnis wurden insbesondere die folgenden Aspekte umgesetzt:

- *Rechtsgrundlagen der Datenverarbeitung*

Datenverarbeitung erfolgt ausschließlich aufgrund einer Legitimationsgrundlage. Diese ergibt sich regelmäßig aus der vertraglichen Dienstleistungsbeziehung in Verbindung mit Art. 4 EU-DSGVO.

- *Betroffenenrechte*

Die datenschutzrechtlichen Betroffenenrechte werden konsequent umgesetzt. Von Datenverarbeitung betroffene Personen erhalten, sofern dafür die Verantwortung bei IngA Service GmbH liegt, Informationen zur Datenverarbeitung im Sinne der Art. 13 und 14 EUDSGVO. Die IngA Service GmbH gewährleistet zudem, dass das Auskunftsrecht nach Art. 15 EU-DSGVO, Recht auf Berichtung nach Art. 16 EU-DSGVO, Recht auf Löschung nach Art.17 EU-DSGVO, Recht auf Datenübertragbarkeit nach Art. 20 EU-DSGVO und gegebenenfalls das Widerspruchsrecht nach Art. 21 EU-DSGVO in eigener Verantwortung oder bei Verantwortung der Kunden unterstützend umgesetzt werden kann.

- *Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung*

Die IngA Service GmbH stellt durch die Definition spezifischer Rahmenbedingungen für die Art und Weise der Datenverarbeitung sicher, dass die Prozessgestaltung den Vorgaben des Art. 25 EU-DSGVO (Data Protection By Design und Data Protection By Default) folgt. Dabei werden neue Entwicklungen im Bereich der Digitaltechnik beachtet.

- *Dienstleistungsbeziehungen*

In den Dienstleistungsbeziehungen wird Datenschutz sichergestellt, in dem die technischen und organisatorischen Maßnahmen konsequent umgesetzt werden. Die Kunden der IngA Service GmbH im Bereich Scandienstleistungen erhalten entsprechende Zusicherungen über einen Vertrag über Auftragsverarbeitung nach Art. 28, 29 EU-DSGVO. Die IngA Service GmbH schließt ihrerseits mit etwaigen Dienstleistern Verträge über Auftragsverarbeitung ab.

- *Dokumentationspflichten*

Die IngA Service GmbH gewährleistet eine konsequente Umsetzung der Dokumentationspflichten im Sinne einer Rechenschaftspflicht auf Grundlage von Art. 5 Abs. 2 EU-DSGVO, um den Nachweis der ausschließlich rechtmäßigen Verarbeitung personenbezogener Daten zu erbringen. Dazu wird das gesetzlich vorgeschriebene Verzeichnis der Verarbeitungstätigkeiten (Art. 30 EU-DSGVO) geführt.

- *Datenschutzfolgenabschätzung*

Die IngA Service GmbH stellt sicher, dass bei entsprechenden Risiken für die Rechte und Freiheiten natürlicher Personen eine Datenschutzfolgeabschätzung unter Einbeziehung des Datenschutzbeauftragten durchgeführt wird.

- *Meldepflichten*

Die IngA Service GmbH stellt sicher, dass der Datenschutzbeauftragte unter Angabe seiner Kontaktdaten nach Art. 37 Abs. 7 EU-DSGVO gemeldet ist. Zudem ist ein Prozess etabliert, der die Registrierung und Meldung von Datenpannen nach Art. 33 Abs. 1 EU-DSGVO an die Aufsichtsbehörde sicherstellt.

- *Datensicherheit*

Unter Beachtung von Art. 24 und 32 EU-DSGVO wird ein angemessenes Schutzniveau in Bezug auf die Sicherheit der Verarbeitung personenbezogener Daten gewährleistet, wobei die implementierten Sicherungsmaßnahmen einer regelmäßigen Prüfung unterzogen werden.

4. Unsere Maßnahmen für Datenschutz und Datensicherheit

4.1 Schutz der Daten des Auftraggebers

Zum Schutz der Daten unserer Kunden wurden angemessene organisatorisch-technische Maßnahmen i. S. d. Art. 24, 32 EUDSGVO getroffen, um die entsprechenden Ausführungen der Gesetzesvorschriften, zu gewährleisten.

Dazu haben wir uns an der in Deutschland seit vielen Jahren bewährten Systematik der Aufgaben nach § 9 BDSG und Anlage orientiert, insbesondere aber auch die zusätzlichen Aspekte der EUDSGVO berücksichtigt.

Eine Zusammenfassung der von uns ergriffenen technischen und organisatorischen Maßnahmen enthält die nachfolgende Tabelle:

Nr.	Bezeichnung	Inhalt	Umsetzung im Scan-Zentrum
1	Zutrittskontrolle	Gewährleistung, dass Unbefugten der Zutritt zum Unternehmen und zu Datenverarbeitungsanlagen verwehrt wird.	Der Zutritt zum Gebäude ist tagsüber über einen offenen Eingang in die Flurbereiche möglich, von denen im 1. Stock das Scan-Zentrum nur über stets geschlossene Türen betreten werden kann. Die Zutrittskontrolle ist über ein Schließsystem gewährleistet. Die zentrale Datenverarbeitungsanlage (Server, Firewall, USV, etc.) befinden sich in einem gesonderten Raum, die durch ein weiteres Zutrittskontrollsystem geschützt sind. Nur der dedizierte Personenkreis hat eine Zutrittsberechtigung.
2	Zugangskontrolle	Gewährleistung, dass Unbefugten der Zugang zu und die Nutzung von Datenverarbeitungssystemen verwehrt wird.	Die Zugangskontrolle erfolgt durch eine zentrale Benutzervergabe mit Benutzerkennung und Passwort. Zudem gibt es weitere Maßnahmen, die den Zugang zum Unternehmensnetzwerk regeln. Die Zugangskontrollmaßnahmen unterliegen dabei einer stetigen Überprüfung hinsichtlich der aktuellen Gefahrensituation.
3	Zugriffskontrolle	Gewährleistung eines angemessenen Zugriffskontrollsystems; d.h., dass jeder nur über die Rechte verfügt, die er zu seiner Arbeit braucht.	Das Arbeiten auf dem Netzwerk erfordert Zugänge zu unterschiedlichen, dem Aufgabenbereich zugeordneten Systemen. Nur die Mitarbeitenden des Scan-Zentrums haben Zugriff auf die Dateien, die sich in einem lokalen Netzwerk ohne Internetanbindung befinden.

4	Weitergabekontrolle	Gewährleistung, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Die elektronische Übertragung von vertraulichen und personenbezogenen Daten zum Auftraggeber findet über eine verschlüsselte Datenleitung statt. Die Bereitstellung der Daten erfolgt über einen Server, auf den der Zugriff mit den Zugangsdaten nur für eine begrenzte Zeit möglich ist. Anschließend befinden sich die Daten nur noch auf einem lokalen Server ohne Internetanbindung. Papierdokumente werden entweder durch unternehmenseigene Mitarbeitende oder durch geprüfte Dienstleister transportiert. Je nach Vertragssituation können Papierdokumente auch durch zertifizierte Dienstleister entsprechend der vereinbarten Sicherheitsstufe DIN 66399 nachweisbar vernichtet werden.
5	Eingabekontrolle	Gewährleistung der nachträglichen Überprüfbarkeit hinsichtlich der Eingabe, Veränderung oder Entfernung personenbezogener Daten; Gewährleistung einer nutzerbezogenen Zuordnung von Aktivitäten.	Ausschließlich autorisierter Zugriff auf Daten über eindeutige Benutzeridentitäten. Es ist bei jedem Verarbeitungsschritt nachweisbar, wer welchen Arbeitsschritt vollzogen hat. Damit kann nachträglich überprüft werden, von wem wann welche personenbezogenen Daten des Kunden vorbereitet, gescannt, verändert oder gelöscht worden sind.
6	Auftragskontrolle	Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.	Mit den beauftragten Dienstleistern werden im Rahmen der Auftragsdatenverarbeitung klare Absprachen bezüglich Aufgabenumfang und -inhalt getroffen.
7	Verfügbarkeitskontrolle	Gewährleistung, dass personenbezogene Daten vor Zerstörung und Verlust geschützt sind.	Alle personenbezogenen Daten sind im Hinblick auf Verfügbarkeit und Wiederherstellbarkeit besonders gesichert. Hierfür werden Backup-Systeme und brandschutzgesicherte Lagerräume genutzt.
8	Datentrennung	Gewährleistung, dass Daten, die zu unterschiedlichen Zwecken erhoben worden sind, getrennt verarbeitet werden.	Die Erhebung und Verarbeitung von personenbezogenen Daten erfolgt stets zweckgebunden. Insbesondere ist durch organisatorische Maßnahmen und präzise Datentrennung sichergestellt, dass Daten unterschiedlicher Kunden getrennt erhoben und verarbeitet werden.

4.2 Weitere Maßnahmen zum Datenschutz

Nr.	Bezeichnung	Inhalt
1	Verpflichtung der Mitarbeiter	Jeder Mitarbeitende des Scan-Zentrums der IngA Service GmbH wird schriftlich zur Einhaltung der Datenschutzgrundverordnung (DSGVO) verpflichtet, wozu auch eine Verschwiegenheitsklausel gehört. Ergänzend muss noch eine Dienstanweisung unterschrieben werden, die das datenschutzgerechte Verhalten konkreter beschreibt.
2	Schulungen der neuen Mitarbeiter	Jeder Mitarbeitende des Scan-Zentrums wird bei Eintritt in das Arbeitsverhältnis im Rahmen einer Schulung mit den Inhalten der DSGVO und deren Auswirkungen auf den jeweiligen Arbeitsplatz vertraut gemacht.
3	Verfahrensverzeichnisse	Durch die permanente Pflege und Aktualisierung von Verfahrensverzeichnissen (Prozessbeschreibungen) ist die Einbindung des Datenschutzes in alle relevanten Entwicklungen sichergestellt.
4	Datenschutzfolgeabschätzung	Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Wir ziehen zur Durchführung unseren Datenschutzbeauftragten hinzu.
5	Auftragsverarbeitung	Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser EUDSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Die weiteren Regelungen des Art. 28 EUDSGVO werden beachtet.