Technisch Organisatorische Maßnahmen

Solvere gGmbH

Leitbild, Zielsetzung und allgemeine Maßnahmen

Um sicherzustellen, dass personenbezogene Daten nur in Übereinstimmung mit den gesetzlichen Grundlagen erfolgt, richten wir unsere Prozesse und technische Gestaltung an den Gewährleistungszielen des Art. 32 sowie der Regelung des Art. 25 der Datenschutzgrundverordnung (DSGVO) sowie der Datenschutzgrundverordnung im Allgemeinen, des Bundesdatenschutzgesetzes und der weiteren relevanten datenschutzrechtlichen Gesetze aus. Insbesondere sollen nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind und einfache Ausübung der Betroffenenrechte sichergestellt werden.

In diesem Sinne wird bei der Solvere gGmbH die Vertraulichkeit gem. Art. 32 Abs.1 DSGVO durch Zutrittskontrollen (wie Alarmanlage, Schließsystem, Videoüberwachung, Besucherkontrollen), Zugangskontrollen (wie Einsatz von Antivieren-Software und Firewalls), Verschlüsselung von Datenträgern, Benutzerberechtigungsverwaltung, sichere Passwortvergabe), Zugriffskontrollen (wie Verwendung von Aktenschreddern und Aktenvernichtern, Datenschutztresor) und Trennungskontrollen (wie abgeschlossene Laufwerke, Festlegung von Datenbankrechten, getrennte digitale Archive) gewährleistet.

Weiterhin wird die Integrität gem. Art. 32 Abs.1 DSGVO gewährleistet durch Weitergabekontrollen (wie eine E-Mail-Verschlüsselung, Protokollierung aller Zugriffe und Abrufe, Dokumentation der Datenempfänger und der Dauer der Überlassung) und eine Eingabekontrolle (wie die Aufbewahrung von Formularen nach automatisierter Verarbeitung und klaren Strukturen und Zuständigkeiten bei der Löschung von Daten).

Die Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 DSGVO wird gewährleistet durch eine Verfügbarkeitskontrolle (wie technisch und tatsächlich gesicherte Serverräume, RAID System, Backup- und Recovery-Konzepte mit sicherer Aufbewahrung, Existenz eines Notfallplans).

Darüber hinaus werden Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit.d) und Art. 25 Abs. 1 DSGVO eingesetzt (wie Software-Lösung für das Datenschutzmanagement, Zentrale Dokumentationen zum Datenschutz, jährliche Überprüfungen der Wirksamkeit technischer Schutzmaßnahmen, ein bestellter externer Datenschutzbeauftragter sowie regelmäßig geschulte, sensibilisierte und auf Vertraulichkeit verpflichtete Mitarbeiter*innen). Es existiert auch ein Incident-Response-Management zur Unterstützung bei der Reaktion auf Sicherheitsverletzungen (wie regelmäßig aktualisierte Firewalls, Spamfilter und Antivieren-Software). Weiterhin werden stets die datenschutzfreundlichsten Voreinstellungen gem. Art. 25 Abs. 2 DSGVO verwendet, indem nicht mehr personenbezogenen Daten erhoben werden, wie für den jeweiligen Zweck notwendig sind. Auch werden beim Outsourcing an Dritte Auftragskontrollen durch vorherige Überprüfungen und eine sorgfältige Auswahl der Subunternehmer sowie des Abschlusses der gesetzlich notwendigen vertraglichen Regelungen mit diesen und der Weisungen an sie durchgeführt.

Die folgend aufgeführten technischen und organisatorischen Maßnahmen speziell zu den einzelnen Dienstleistungen der Solvere gGmbH richten sich ebenso an den Gewährleistungszielen des Art. 32 sowie der Regelung des Art. 25 der Datenschutzgrundverordnung aus:

Anhang 1a: Akten- und Datenträgervernichtung

Beschreibung der Datenverarbeitung

Im Rahmen des Vertrages werden durch den Aufraggeber regelmäßig Datenträger (Papier, Mikrofilme/Fiches, Magnetkarten, Chipkarten, Flash-Speichermedien, CDs/DVDs usw.) zur Vernichtung an die Solvere gGmbH übergeben. Diese werden in speziellen Sicherheitsbehältern gesammelt, zur Vernichtungsanlage in der Werkstatt transportiert und dort unverzüglich entsprechend der Vorgaben der DIN 66399 Teil 1 und 2 fachgerecht vernichtet. Eine über das Vernichten hinausgehende Verarbeitung, Nutzung oder Weitergabe der Daten durch die Solvere gGmbH erfolgt nicht.

Maßnahmen

Zutrittskontrolle

Die eingerichteten Maßnahmen zur Zugriffskontrolle gewährleisten, dass Unbefugten der Zutritt zu dem Vernichtungsbereich als Sicherheitsbereich verwehrt wird. Die Solvere gGmbH schützt ihre für die Verarbeitung von personenbezogenen Daten kritischen Bereiche durch angemessene Zutrittskontrollsysteme. Zutrittsrechte für berechtigte Personen werden gemäß festgelegten Kriterien individuell erteilt. Dies gilt auch hinsichtlich externer Personen. Der Vernichtungsbereich ist ein baulich abgetrennter Bereich innerhalb der jeweiligen Werkstattgebäude. Die Türen zu diesem Bereich sind nur mit Zugangskarten, Codes oder –schlüsseln zu öffnen. Der Zutritt ist nur für berechtigte Mitarbeiter, die auf den Datenschutz besonders verpflichtet wurden, möglich. Die Überwachung des Bereiches erfolgt per Videoüberwachung des Zugangs, des Bereiches an sich oder durch besonders geschultes permanent anwesendes Fach-/Aufsichtspersonal. Die zutrittsberechtigten Mitarbeiter werden regelmäßig über die datenschutzrechtlichen Vorgaben belehrt. Diese Belehrung wird durch den Datenschutzbeauftragten veranlasst. Es erfolgt eine Dokumentation und, sofern aufgrund der Behinderung möglich, die Unterzeichnung einer Verpflichtungserklärung durch die Mitarbeiter. Das Hauptgebäude sowie das Nebengebäude (Aktenvernichtung) sind alarmanlagengesichert, um den Zutritt unberechtigter Personen zu unterbinden. Bei Auslösen eines Alarms gibt es eine vorgeschriebene Alarmkette in Form von Benachrichtigung und entsprechender Verhaltensweise, wie in diesem Falle zu verfahren ist. Dieser Alarmkette unterlieget die Sicherheitsfirma selbst sowie 3 Mitarbeiter.

Zugangs-, Zugriffs- und Datenübertragungskontrolle

Der Zugang zu den Datenträgern wird durch entsprechende Sicherheitsbehälter verhindert, die verschlossen an den jeweiligen Lokationen des Auftraggebers aufgestellt werden. Im Einzelfall können Schlüssel für die jeweiligen Sicherheitsbehälter an verantwortliche Mitarbeiter*innen des Auftraggebers auf dessen Wunsch hin ausgehändigt werden, der diese intern verwaltet. Durch Materialwahl und Konstruktion der Sicherheitsbehälter wird sichergestellt, dass Unbefugte keinen Zugriff auf die in den Sicherheitsbehältern befindlichen Datenträger erhalten können. Sofern Sicherheitsbehälter 2 oder mehr Schließmöglichkeiten haben, werden alle vorhandenen Schlösser geschlossen bzw. entsprechende Vorhängeschlösser angebracht.

Bei dem Transport der Sicherheitsbehälter vom Auftraggeber zur Werkstatt der Solvere gGmbH werden Fahrzeuge mit geschlossenem Sicherheitsaufbau eingesetzt, so dass von außen kein Einblick auf die Sicherheitsbehälter möglich ist. Der Transport wird durch wenigstens 2 Mitarbeiter durchgeführt und die Transportfahrzeuge selbst werden verschlossen, sofern sich kein Mitarbeiter im oder unmittelbar am Fahrzeug befindet.

In der Werkstatt der Solvere findet die Entladung, Entleerung und Vernichtung der Sicherheitsbehälter in einem Vernichtungsbereich als Sicherheitsbereich statt, zu dem auch speziell autorisiertes Personal gehört. Alle Vorgänge werden stets überwacht und beaufsichtigt. Sofern aus betrieblichen Gründen eine vorrübergehende Zwischenlagerung in einem Lager notwendig ist, so wird dieses entsprechend der Vorgaben der DIN 66399 – Teil 3 überwacht. Die Räume des Vernichtungsbereiches sind derart

beschaffen, dass Aktenmaterial vor der Vernichtung auch bei Durchzug nicht nach außen gelangen kann.
Autorisierte Besucher sind vor Betreten des Vernichtungsbereiches auf die Einhaltung der datenschutzrechtlichen Vorgaben hinzuweisen und schriftlich darauf zu verpflichten. Dies erfolgt mit entsprechender Unterschrift des Besuchers auf dem Dokument „Verpflichtung zur Einhaltung der Vertraulichkeit und der datenschutzrechtlichen Anforderungen für Besucher“. Es wird sichergestellt, dass kein Einblick in die Unterlagen der Auftraggeber möglich ist. Die Besucherzutritte werden dokumentiert.

Eingabekontrolle

Alle vom Auftraggeber übergebenden Datenträger werden entsprechend der Leistungsbeschreibung der Vernichtung an den jeweiligen Sicherheitsstufen zugeführt. Es werden die Behälteranzahl, ggfs. das Gewicht und die Art der übergebenen Datenträger erfasst und dokumentiert. Eine unbeabsichtigte Mischbefüllung, die erst nach Öffnung der Sicherheitsbehälter in der Werkstatt erkannt wird, wird auf den Lieferpapieren nachträglich dokumentiert. Eine Trennung der Datenträger zur Vernichtung in den entsprechenden Sicherheitsstufen erfolgt im Sicherheitsbereich der Werkstatt.
Eine Trennung der Datenträger von unterschiedlichen Auftraggebern bzw. deren Filialen oder Niederlassungen ist bis zur Öffnung der Sicherheitsbehälter im Vernichtungsbereich gewährleistet. Nach der Öffnung und der Zuführung zur eigentlichen Vernichtungsanlage werden die Datenträger mit Material anderer Filialen/Niederlassungen oder Auftragnehmer zusammengeführt, um so ein höheres Sicherheitsniveau durch Vermischen, Verwirbeln und ggfs. Verpressen zu erreichen.

Trennungskontrolle

Durch eine Trennung der Daten gewährleistet die Solvere gGmbH, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet bzw. vernichtet werden können. Eine Trennung der Datenträger von unterschiedlichen Auftraggebern bzw. deren Filialen oder Niederlassungen ist bis zur Öffnung der Sicherheitsbehälter im Vernichtungsbereich gewährleistet. Nach der Öffnung und der Zuführung zur eigentlichen Vernichtungsanlage werden die Datenträger mit Material anderer Filialen/Niederlassungen oder Auftragnehmer zusammengeführt, um so ein höheres Sicherheitsniveau durch Vermischen, Verwirbeln und ggfs. Verpressen zu erreichen.

Verfügbarkeitskontrolle

Die Solvere gGmbH ergreift Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und nur der ordnungsgemäßen Vernichtung im Rahmen der Beauftragung zugeführt werden.

- Vernichtungsanlage:

Die Vernichtungsanlagen sind eigens für diesen Zweck konstruierte Maschinen. Diese gewährleisten eine Vernichtung nach den materialabhängigen Sicherheitsstufen der DIN 66399 – Teil 1 gemäß den vertraglichen Vereinbarungen. Die Maschinen werden regelmäßig gemäß den Herstellervorgaben gewartet. Das Material wird vor der Vernichtung sortiert, um mögliche Fremdstoffe und große Gegenstände wie Ordner oder Hefter zu entfernen und eine hohe Qualität des entstehenden Recyclinggutes zu gewährleisten. Das Aktenmaterial wird im Anschluss an die Vernichtung verwirbelt bzw. verpresst und abhängig von den örtlichen Gegebenheiten dem Recycling durch die Papierindustrie zugeführt.

- Behandlung der Sicherheitsbehälter:

Die gefüllten Sicherheitsbehälter werden nach der Annahme unmittelbar in den Sicherheitsbereich der Werkstatt gebracht. Danach werden sie entleert, wobei vollständig kontrolliert wird, dass keinerlei Papiermaterial mehr im Sicherheitsbehälter enthalten sind (kleine Zettel, Haftnotizen o.ä.). Danach werden diese bis zur nächsten Verwendung zwischengelagert.
Vor dem nächsten Einsatz erfolgt erneut eine Sichtkontrolle der Sicherheitsbehälter auf Beschädigungen oder eventuell vorhandenes restliches Altpapier. Ggfs. werden die Sicherheitsbehälter gereinigt bzw. Instand gesetzt.

Incident-Response-Management

Im Fall von Datenschutzpannen besteht ein dokumentierter Prozess zur Meldung auch im Hinblick auf die Meldepflicht gegenüber der Aufsichtsbehörde, welcher die Einbeziehung der Betroffenen Abteilung, der IT-Abteilung und des Datenschutzbeauftragten umfasst. Der Prozess umfasst ebenso, in formaler Weise, die Bestimmung der Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen.

Kontrolle der Auftragsverarbeiter

Sofern Auftragsverarbeiter eingesetzt werden, ergreift die Solvere gGmbH Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Es erfolgt ggf. eine sorgfältige Auswahl des Auftragnehmers in Bezug auf Datenschutz und Datensicherheit und die Sichtung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation.

Datenschutzmanagementsystem

Die Solvere gGmbH unterhält ein Kontrollverfahren auf der Grundlage eines risikomanagementbasierten Ansatzes zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Damit wird der Schutz der relevanten Daten gewährleistet. Die Solvere gGmbH ist nach ISO 9001:2015 für den Geltungsbereich Datenschutzgerechte Akten- und Datenträgervernichtung, digitale Archivierung von Kundenakten sowie Büro- und allgemeine Dienstleistungen zertifiziert. Durch das systematische Erfassen und Beseitigen von Schwachstellen werden damit die Schutzmaßnahmen kontinuierlich hinterfragt und verbessert. Die Vorgaben der DIN 66399 werden eingehalten.

Darüber hinaus wird ein Datenschutzmanagementsystem auch durch eine zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter*innen im Betrieb aktiv gelebt. Die Übernahme und Zuführung der Sicherheitsbehälter wird mit einem Übernahmeprotokoll dokumentiert. Die Bestätigung der ordnungsgemäßen Vernichtung erfolgt je nach Vereinbarung im Rahmen der Rechnungsstellung. Diese Maßnahmen werden durch die Bestellung des Datenschutzbeauftragten, der Schulung der Mitarbeiter*innen und der Verpflichtung auf Vertraulichkeit sowie das Datengeheimnis gefestigt. Anlassbezogen kommt die Solvere gGmbH ihren Informationspflichten gemäß Art. 13 und 14 DSGVO, dem Widerrufsrecht der Betroffenen, der Pflicht zur Durchführung einer Datenschutz-Folgeabschätzung und der Bearbeitung von Auskunftsanfragen seitens Betroffener nach. Zu diesem Zweck wurden entsprechen Prozesse geschaffen.

Anhang 1b: Digitalisierung von Dokumenten

Beschreibung der Datenverarbeitung

Im Rahmen des Vertrages/Auftrages werden durch den Aufraggeber regelmäßig (jährlich, monatlich oder wöchentlich) oder einmalig Datenträger in Papierform als Akten oder Ordner zur Digitalisierung an die Solvere gGmbH übergeben. Die Solvere gGmbH erfasst die überlassenen Dokumente nach vereinbarten Indizierungskriterien oder vereinbarter Benamung digital im gewünschten Dateiformat und übergibt das fertige digitale Produkt dem Auftraggeber. Die Datenträger in Papierform können infolge auf Wunsch des Auftraggebers der Aktenvernichtung zugeführt werden oder sie werden im Originalzustand wiederhergestellt und zurück geliefert. Eine darüberhinausgehende Verarbeitung, Nutzung oder Weitergabe der Daten durch die Solvere gGmbH erfolgt nicht.

Maßnahmen

Zutrittskontrolle

Die eingerichteten Maßnahmen zur Zutrittskontrolle gewährleisten, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird. Die Solvere gGmbH schützt ihre für die Verarbeitung von personenbezogenen Daten kritischen Bereiche durch angemessene Zutrittskontrollsysteme. Zutrittsrechte für berechtigte Personen werden gemäß festgelegten Kriterien individuell erteilt. Dies gilt auch hinsichtlich externer Personen. Das Hauptgebäude sowie das Nebengebäude (Aktenvernichtung) sind alarmanlagengesichert, um den Zutritt unberechtigter Personen zu unterbinden. Bei Auslösen eines Alarms gibt es eine vorgeschriebene Alarmkette in Form von Benachrichtigung und entsprechender Verhaltensweise, wie in diesem Falle zu verfahren ist. Dieser Alarmkette unterlieget die Sicherheitsfirma selbst sowie 3 Mitarbeiter.

- Berechtigte Mitarbeiter*innen und Beschäftigte:

Der Digitalisierungsbereich ist ein abgetrennter Bereich innerhalb des Hauptgebäudes und befindet sich auf dem gesamten 1. Obergeschoss und Teilen des 2. Obergeschosses. Die Überwachung des Bereiches erfolgt durch besonders geschultes und permanent anwesendes Fach- und Aufsichtspersonal. Die Türen zu diesem Bereich sind nur mit Zugangscodes oder –schlüsseln zu öffnen und sind videoüberwacht. Schlüssel für diesen Bereich besitzen im Rahmen eines rollenbezogenen Berechtigungskonzepts ausschließlich berechtigte Mitarbeiter*innen. Die Dokumentierung erfolgt durch eine Schlüsselliste, der Empfang des Schlüssels ist mit der Unterschrift zu bestätigen. Die Schlüssel können auch nur mit einer eigenen Sicherheitskarte nachgemacht werden. Beschäftigte ohne eigenen Schlüssel erhalten Zutritt zum Digitalisierungsbereich erst nach Klingeln und Öffnen der Tür durch das Fach- und Aufsichtspersonal. Die zutrittsberechtigten Mitarbeiter/Beschäftigten werden regelmäßig über die datenschutzrechtlichen Vorgaben durch den Datenschutzbeauftragten belehrt. Es erfolgt eine Dokumentation dessen und, sofern aufgrund der Behinderung möglich, die Unterzeichnung einer Verpflichtungserklärung zum Datenschutz und der Verschwiegenheit durch die Mitarbeiter*innen.

- Angemeldete Besucher:

Besucher erhalten Einlass erst nach Klingeln am Haupteingang des Gebäudes. Die Besucherzutritte werden in der Besucherliste am Empfang des Hauptgebäudes mit genauer Zeitangabe des Aufenthaltes dokumentiert. Autorisierte Besucher werden vor Betreten des Digitalisierungsbereiches auf die Einhaltung der datenschutzrechtlichen Vorgaben hingewiesen und schriftlich durch ihre Unterschrift darauf verpflichtet. Dies erfolgt mit entsprechender Unterschrift des Besuchers auf dem Dokument „Verpflichtung zur Einhaltung der Vertraulichkeit und der datenschutzrechtlichen Anforderungen für Besucher“. Nach Identifikation erhalten sie einen Besucherausweis für die Zeit Ihres Aufenthaltes, der bei Verlassen wieder eingezogen wird. Besucher werden dem Empfangspersonal

vorab angekündigt und entsprechend von einem Mitarbeiter am Empfang abgeholt. Die Besucher werden während des gesamten Aufenthaltes in den Sicherheitsbereichen der Solvere gGmbH von einem*r Mitarbeiterin begleitet.

Zugangs-, Zugriffs- und Datenübertragungskontrolle

Die Datenträger werden in Sicherheitsbehältnissen, die durch Materialwahl und Konstruktion gegen unberechtigten Zugriff geschützt sind oder auf ausdrücklichem schriftlichem Wunsch des Auftraggebers auch in vom Auftraggeber selbst zusammengestellten und gepackten Kartons/Einheiten, transportiert. Sofern Sicherheitsbehälter 2 oder mehr Schließmöglichkeiten haben, werden alle vorhandenen Schlösser geschlossen bzw. entsprechende Vorhängeschlösser angebracht. Die Übergabe vom Auftraggeber zum Auftragnehmer wird gegenseitig auf dem Aktenübernahmeprotokoll durch Unterschrift bestätigt. Für den Transport der Datenträger vom Auftraggeber zur Werkstatt werden Fahrzeuge mit geschlossenem Sicherheitsaufbau eingesetzt, so dass von außen kein Einblick auf die abgeholten Datenträger bzw. Sicherheitsbehälter möglich ist. Der Transport wird durch wenigstens 2 Mitarbeiter*innen durchgeführt. Das Transportfahrzeug selbst ist ebenfalls verschlossen, sofern sich kein*e Mitarbeiterin im oder unmittelbar am Fahrzeug befindet.

Die Datenträger und/oder verschlossenen Sicherheitsbehälter werden direkt und ohne Verzögerung vom LKW in den Sicherheitsbereich verbracht. Außerhalb der geschlossenen Sicherheitsbereiche werden ggf. die Sicherheitsbehälter bzw. die Fahrzeuge ständig durch autorisiertes Personal der Werkstatt beaufsichtigt. Die eingerichteten Maßnahmen zur Zugriffskontrolle 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.

Kundenaufträge werden in einem nach Außen abgeschlossenen Laufwerk bearbeitet. Somit ist sichergestellt, dass kein Zugriff bzw. Zugang zu den verarbeiteten Daten von Dritten möglich ist. In den Sicherheitsbereichen der Digitalisierung besteht ein Verbot von Mobilen Aufnahmegeräten (wie Mobiltelefonen und Fotoapparaten) für alle Beschäftigten.
Alle PCs sind auf Windows -Ebene Passwort geschützt. Der Benutzer muss sich mit Benutzernamen und Passwort zur Bearbeitung einloggen. Zum Scannen der Dokumente wird je nach Auftrag entweder eine DMS-Software oder eine reine Scansoftware verwendet. Bei Verwendung einer DMS-Software einzelnen Benutzer werden mit unterschiedlichen Rechten ausgestattet. Mit Hilfe eines Aktivitäten Reports in der DMS-Software kann jedes einzelne Ereignis im DMS-System zurückverfolgt und gespeichert werden. Bei dreimaliger Falscheingabe eines Passworts wird der Benutzer vom User Management gesperrt. Es muss eine Freigabe vom Administrator zur erneuten Anmeldung erfolgen. Bei Einsatz einer reinen Scan-Software ist die Nachverfolgbarkeit der Bearbeitung durch eine schriftliche Dokumentation der einzelnen Arbeitsschritte gesichert.

Eingabekontrolle

Zur Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, findet eine weitgehende Eingabekontrolle statt. Alle übergebenden Datenträger werden anhand von vorab übermittelten Einlagerungslisten durch Kennzeichnung auf der Liste als Eingang sichergestellt. Die abgeschlossene Eingangsregistrierung ist Arbeitsgrundlage der digitalen Archivierung und stellt den Erhalt der physischen Akte/Datenträger zu der in Auftrag gegebenen Verarbeitung sicher. In die abgeschlossene Eingangsregistrierung kann jederzeit vom Auftraggeber Einsicht genommen werden.

Kann vom Auftraggeber keine Auflistung zur Verfügung gestellt werden, wird ein detailliertes Aktenübernahmeprotokoll erstellt, in welchem die einzelnen Ordnernamen/Aktennamen aufgelistet

werden. Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten erfolgt auf Basis eines Berechtigungskonzepts. Insbesondere hinsichtlich der Löschung von Daten werden die Zuständigkeiten in einem jedenfalls bereichsgebundenen Konzept definiert. Dadurch wird die Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten sichergestellt.

Trennungskontrolle

Die unterschiedlichen Aufträge lagern in auftragsbezogenen und gekennzeichneten Regalen und/oder eigens dafür vorgesehenen Bearbeitungsräumen bzw. rollbaren Aktenschränken. Die zu bearbeitenden Dokumente werden täglich durch das Fachpersonal eingesteuert und ausgegeben und nach Dienstschluss wieder zurückgestellt. Durch diese logische und physikalische Trennung der Daten gewährleistet die Solvere gGmbH, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Verwendete Test- und Live-Systeme sind vollständig getrennt. Die relevanten Anwendungen zur Speicherung von Mitarbeiter und Kundendaten sind mandantenfähig.

Verfügbarkeitskontrolle

Die Solvere gGmbH ergreift Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Alle Aufträge zur digitalen Archivierung werden gemäß unserer Prozessbeschreibung zur Auftragsdurchführung bearbeitet. Im Prozess sind verschiedene Kontrollinstanzen der Auftragsbearbeitung einschließlich einer Stichprobenkontrolle vor Auslieferung der digitalen Daten an den Auftraggeber festgeschrieben. Die Solvere gGmbH ist nach ISO 9001:2015 für den Geltungsbereich Datenschutzgerechte Akten- und Datenträgervernichtung, digitale Archivierung von Kundenakten sowie Büro- und allgemeine Dienstleistungen zertifiziert. Das Zertifikat kann auf Wunsch eingesehen werden.

- Datensicherung:

Das digitale Produkt bleibt bis zur endgültigen Freigabe zur Datenlöschung durch den Auftraggeber bei Solvere gGmbH gespeichert. Der Auftraggeber erhält eine Freigabebescheinigung, in welcher er schriftlich den Auftrag gibt, das digitale Produkt zu löschen oder weiterhin zu sichern. Ebenso wird hier die Rückgabe der physischen Dokumente oder eine Datenträgervernichtung in Auftrag gegeben. Eine gewünschte Datensicherung über die Solvere gGmbH beinhaltet eine Sicherung auf verschlüsselter Festplatte sowie die Lagerung von 2 gleichen DVDs in unterschiedlichen Wertschränken/Tresoren an räumlich getrennten Standorten sowie eine jährliche Prüfung anhand verschiedener dokumentierter Prüfkriterien.

- Auslieferung des digitalen Produktes:

Die Auslieferung des digitalen Produktes wird vom Auftraggeber vorgegeben und entsprechend vereinbart. Angeboten wird eine Speicherung auf verschlüsselter DVD, USB-Stick oder Festplatte. Die Auslieferung kann persönlich durch unsere Mitarbeiter*innen mit Lieferschein erfolgen oder durch persönliche Abholung. Auf Wunsch des Auftraggebers werden einzelne Unterlagen auch während der digitalen Erfassung zugestellt. Dies wird als Rückgabe/Entnahme auf der Eingangsregistrierung vermerkt und somit dokumentiert.

Incident-Response-Management

Im Fall von Datenschutzpannen besteht ein dokumentierter Prozess zur Meldung auch im Hinblick auf die Meldepflicht gegenüber der Aufsichtsbehörde, welcher die Einbeziehung der Betroffenen Abteilung, der IT-Abteilung und des Datenschutzbeauftragten umfasst. Der Prozess umfasst ebenso, in formaler Weise, die Bestimmung der Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen.

Kontrolle der Auftragsverarbeiter

Sofern Auftragsverarbeiter eingesetzt werden, ergreift die Solvere gGmbH Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend

den Weisungen des Auftraggebers verarbeitet werden können. Es erfolgt ggf. eine sorgfältige Auswahl des Auftragnehmers in Bezug auf Datenschutz und Datensicherheit und die Sichtung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation.

Datenschutzmanagementsystem

Die Solvere gGmbH unterhält ein Kontrollverfahren auf der Grundlage eines risikomanagementbasierten Ansatzes zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Damit wird der Schutz der relevanten Daten gewährleistet. Die Solvere gGmbH ist nach ISO 9001:2015 für den Geltungsbereich Datenschutzgerechte Akten- und Datenträgervernichtung, digitale Archivierung von Kundenakten sowie Büro- und allgemeine Dienstleistungen zertifiziert. Durch das systematische Erfassen und Beseitigen von Schwachstellen werden damit die Schutzmaßnahmen kontinuierlich hinterfragt und verbessert. Die Vorgaben der DIN 66399 werden eingehalten.

Darüber hinaus wird ein Datenschutzmanagementsystem auch durch eine zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter*innen im Betrieb aktiv gelebt. Die Übernahme und Zuführung der Sicherheitsbehälter wird mit einem Übernahmeprotokoll dokumentiert. Die Bestätigung der ordnungsgemäßen Vernichtung erfolgt je nach Vereinbarung im Rahmen der Rechnungsstellung. Diese Maßnahmen werden durch die Bestellung des Datenschutzbeauftragten, der Schulung der Mitarbeiter*innen und der Verpflichtung auf Vertraulichkeit sowie das Datengeheimnis gefestigt. Anlassbezogen kommt die Solvere gGmbH ihren Informationspflichten gemäß Art. 13 und 14 DSGVO, dem Widerrufsrecht der Betroffenen, der Pflicht zur Durchführung einer Datenschutz-Folgeabschätzung und der Bearbeitung von Auskunftsanfragen seitens Betroffener nach. Zu diesem Zweck wurden entsprechen Prozesse geschaffen.

Anhang 1c: Einlagerung und digitale Datenarchivierung (Datensicherung)

Beschreibung der Datenverarbeitung

Eine über die nachfolgend dargestellte Verarbeitung, Nutzung oder Weitergabe der Daten des Auftraggebers durch die Solvere gGmbH erfolgt nicht.

- Einlagerung:

Im Rahmen des Vertrages/Auftrages werden durch den Aufraggeber vertraglich vereinbarte Datenträger in Papierform (Akten/Ordner) zur Einlagerung an die Solvere gGmbH übergeben.

- Langfristige Datenarchivierung:

Im Rahmen eines Datensicherungsvertrags beauftragt der Auftraggeber den Auftragnehmer, bereits digitalisierte Auftragsdaten weiterhin digital zu sichern und zu archivieren. Hierfür ist eine technische Aufbewahrung der digitalisierten Auftragsdaten auf externen verschlüsselten Datenträgern (wie Festplatten, DVD's, USB-Sticks) möglich. Die digitalen Auftragsdaten werden identisch zum ausgelieferten Produkt erstellt.

Maßnahmen

Zutrittskontrolle

- Einlagerung

Der Ort der Einlagerung der physischen Ordner/Akten ist ein baulich abgetrennter Bereich innerhalb der jeweiligen Werkstattgebäude.

- Langfristige Datenarchivierung:

Der Ort der Einlagerung der digitalen Sicherungskopien ist in gesicherten Wertschränken an zwei baulich und räumlich voneinander getrennten Standorten.

Die eingerichteten Maßnahmen zur Zutrittskontrolle gewährleisten, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird. Die Solvere gGmbH schützt ihre für die Verarbeitung von personenbezogenen Daten kritischen Bereiche durch angemessene Zutrittskontrollsysteme. Zutrittsrechte für berechtigte Personen werden gemäß festgelegten Kriterien individuell erteilt. Dies gilt auch hinsichtlich externer Personen (Besucher). Die Einlagerungsorte sind durch eine elektronische Alarmanlage gesichert mit direkter Aufschaltung zur Sicherheitsfirma. Die Überwachung des Bereiches erfolgt durch besonders geschultes Fach- und Aufsichtspersonal. Die zutrittsberechtigten Mitarbeiter*innen und Beschäftigte werden regelmäßig über die datenschutzrechtlichen Vorgaben durch den Datenschutzbeauftragten belehrt. Es erfolgt eine Dokumentation und die Unterzeichnung einer Verpflichtungserklärung durch die Mitarbeiter*innen und Beschäftigten. Schlüssel für diese Bereiche und die entsprechenden Wertschränke besitzen ausschließlich berechtigte Mitarbeiter*innen. Dies ist auf einer Schlüsselliste dokumentiert, der Empfang des Schlüssels wird durch Unterschrift bestätigt. Die Schlüssel können nur mit einer eigenen Sicherheitskarte nachgemacht werden. Beschäftigte ohne eigenen Schlüssel erhalten Zutritt zum Arbeitsbereich der Einlagerung und Digitalisierung durch das Fach- und Aufsichtspersonal auf Anfrage. Das Hauptgebäude sowie das Nebengebäude (Aktenvernichtung) sind alarmanlagengesichert. Bei Auslösen eines Alarms gibt es eine vorgeschriebene Alarmkette in Form von Benachrichtigung und entsprechender Verhaltensweise, wie in diesem Falle zu verfahren ist. Dieser Alarmkette unterlieget die Sicherheitsfirma selbst sowie 3 Mitarbeiter.

Die Besucherzutritte werden in der Registrierungsliste für Besucher am Empfang des Hauptgebäudes mit genauer Zeitangabe des Aufenthaltes in der Solvere gGmbH dokumentiert. Autorisierte Besucher sind vor Betreten des Einlagerungsbereiches und des Datensicherungsbereiches auf die Einhaltung der datenschutzrechtlichen Vorgaben hinzuweisen und schriftlich darauf zu verpflichten. Dies erfolgt mit entsprechender Unterschrift des Besuchers auf dem Dokument „Verpflichtung zur Einhaltung der

Vertraulichkeit und der datenschutzrechtlichen Anforderungen für Besucher“. Nach einer Identifikation erhalten diese einen Besucherausweis für die Zeit Ihres Aufenthaltes, der bei Verlassen wieder eingezogen wird. Besucher werden dem Empfangspersonal vorab angekündigt und entsprechend von einem Mitarbeiter am Empfang abgeholt. Die Besucher werden während des gesamten Aufenthaltes in den Sicherheitsbereichen der Solvere gGmbH von einem*r Mitarbeiterin begleitet.

Zugangs-, Zugriffs- und Datenübertragungskontrolle

Die Datenträger werden in Sicherheitsbehältnissen, die durch Materialwahl und Konstruktion gegen unberechtigten Zugriff geschützt sind oder auf ausdrücklichem schriftlichem Wunsch des Auftraggebers auch in vom Auftraggeber selbst zusammengestellten und gepackten Kartons/Einheiten, transportiert. Eine Kontrolle der übergebenden Datenträger vom Auftraggeber an die die Solvere gGmbH erfolgt zunächst anzahlmäßig pro Karton vor Ort bei Übernahme. Diese Übergabe wird gegenseitig auf dem Aktenübernahmeprotokoll zur Einlagerung unterschrieben.
Der Transport erfolgt ohne außerplanmäßige Verzögerungen direkt zur Werkstatt. Die Datensicherungskopien werden im abschließbaren Sicherheitsbehältnis transportiert. Durch Materialwahl und Konstruktion der Sicherheitsbehälter wird ausgeschlossen, dass Unbefugte ohne weitere Hilfsmittel und Vorsatz Zugriff auf die in den Sicherheitsbehältern befindlichen Datenträger erhalten. Sofern Sicherheitsbehälter 2 oder mehr Schließmöglichkeiten haben, werden alle vorhandenen Schlösser geschlossen bzw. entsprechende Vorhängeschlösser angebracht. Für den Transport der Datenträger (in Papierform) vom Auftraggeber zur Werkstatt werden Fahrzeuge mit geschlossenem Sicherheitsaufbau eingesetzt, so dass von außen kein Einblick auf die abgeholten Datenträger bzw. Sicherheitsbehälter möglich ist. Der Transport wird durch wenigstens 2 Mitarbeiter*innen/Beschäftigte durchgeführt. Das Transportfahrzeug wird stets verschlossen, sofern sich kein*e Mitarbeiter*inn/Beschäftigter im oder unmittelbar am Fahrzeug befindet.

Eingabekontrolle

Für alle übergebenen Datenträger wird nach dem Transport in die Räume der Solvere gGmbH eine Eingangskontrolle durchgeführt und der Erhalt der physischen Akten/Datenträger wird in einer Lagerliste je Kunde dokumentiert. In die abgeschlossene Eingangsregistrierung kann jederzeit vom Auftraggeber Einsicht genommen werden. In der Eingangsregistrierung wird detailliert das Jahr und die Ordner- oder Aktenbezeichnung aufgenommen.

Die Entladung der Datenträger und/oder verschlossenen Sicherheitsbehälter vom Fahrzeug erfolgt auf dem Betriebsgelände der Solvere gGmbH. Die Datenträger werden direkt und ohne Verzögerung vom LKW in den Sicherheitsbereich gebracht. Außerhalb der geschlossenen Sicherheitsbereiche werden die Sicherheitsbehälter bzw. die Fahrzeuge ständig durch autorisiertes Personal der Werkstatt beaufsichtigt.

In den Bearbeitungsräumen der Einlagerung/Datenarchivierung besteht ein Verbot von mobilen Aufnahmegeräten (wie Mobiltelefonen und Fotoapparaten) für alle Mitarbeiter/Beschäftigten.

Trennungskontrolle

Die unterschiedlichen Einlagerungsaufträge lagern in auftragsbezogenen gekennzeichneten Regalen bzw. Fächern in Kartons. Auf Auftragsgeberwunsch kann auch eine Einlagerung lediglich in Ordnern im Regalfach vorgenommen werden. Für alle Aufträge der Datenarchivierung werden je Auftraggeber getrennte und entsprechend gekennzeichnete Datenträger verwendet.

Verfügbarkeitskontrolle

Bei allen Aufträgen zur Einlagerung ist ein Zugriff auf die eingelagerten Dokumente innerhalb von 24 Stunden an Werktagen während den Geschäftszeiten möglich. Die benötigten Dokumente werden der Einlagerung entnommen und mit dem Dokument Aktenrückgabequittung wieder an den Auftraggeber ausgehändigt. Dies wird als Rückgabe bzw. Entnahme auf der Eingangsregistrierung vermerkt. Die Übergabe der Dokumente erfolgt persönlich durch Abholung durch den Auftraggeber oder durch Überbringung durch den Auftragnehmer und wird schriftlich dokumentiert sowie bestätigt.

Bei mehrjährig geschlossenen Datenarchivierungen findet eine jährliche Kontrolle aller gesicherten Datenträger je Auftraggeber mit Dokumentation auf einem Prüfprotokoll statt. Bei Auftreten eines Mangels wird aus Haltbarkeitsgründen der entsprechende Datenträger neu zur Sicherung erstellt. Nach Ablauf einer 5 Jahresfrist werden alle Datenträger auch ohne Vorhandensein eines Mangels neu erstellt.

Jedes digitale Produkt wird bis zur endgültigen Freigabe zur Datenlöschung durch den Auftraggeber bei Solvere gespeichert. Der Auftraggeber erhält eine Freigabebescheinigung, in welcher er schriftlich den Auftrag gibt, das digitale Produkt zu löschen oder weiterhin zu sichern ist. Zur langfristigen Datenarchivierung des digitalen Produktes werden gesonderte Datensicherungsverträge geschlossen. Ebenso wird hier die Rückgabe der physischen Dokumente oder eine Datenträgervernichtung in Auftrag gegeben.

Bei der Beendigung der Einlagerung hat der Auftragnehmer die Möglichkeit, die Aktenvernichtung von Teilbeständen seiner Einlagerung zu beauftragen. Hierfür erhält er auf Anforderung das Dokument „Freigabebescheinigung“. In diesem Dokument kann explizit festgelegt werden, welche Akten bzw. Ordner nach Jahreszahl aus der Einlagerung entnommen werden und der Aktenvernichtung zugeführt werden sollen. Dies wird durch Unterschrift des Auftraggebers veranlasst und erfolgt ausschließlich auf Weisung des Auftraggebers unter dessen Beachtung der gesetzlichen Aufbewahrungspflichten.

Nach vertraglicher Beendigung der Datenarchivierung erfolgt die Übergabe aller auf Datenträger gespeicherten Daten an den Auftraggeber.

Incident-Response-Management

Im Fall von Datenschutzpannen besteht ein dokumentierter Prozess zur Meldung auch im Hinblick auf die Meldepflicht gegenüber der Aufsichtsbehörde, welcher die Einbeziehung der Betroffenen Abteilung, der IT-Abteilung und des Datenschutzbeauftragten umfasst. Der Prozess umfasst ebenso, in formaler Weise, die Bestimmung der Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen.

Kontrolle der Auftragsverarbeiter

Sofern Auftragsverarbeiter eingesetzt werden, ergreift die Solvere gGmbH Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Es erfolgt ggf. eine sorgfältige Auswahl des Auftragnehmers in Bezug auf Datenschutz und Datensicherheit und die Sichtung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation.

Datenschutzmanagementsystem

Die Solvere gGmbH unterhält ein Kontrollverfahren auf der Grundlage eines risikomanagementbasierten Ansatzes zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Damit wird der Schutz der relevanten Daten gewährleistet. Die Solvere gGmbH ist nach ISO 9001:2015 für den Geltungsbereich Datenschutzgerechte Akten- und Datenträgervernichtung, digitale Archivierung von Kundenakten sowie Büro- und allgemeine Dienstleistungen zertifiziert. Durch das systematische Erfassen und Beseitigen von Schwachstellen werden damit die Schutzmaßnahmen kontinuierlich hinterfragt und verbessert. Die Vorgaben der DIN 66399 werden eingehalten.

Darüber hinaus wird ein Datenschutzmanagementsystem auch durch eine zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter*innen im Betrieb aktiv gelebt. Diese Maßnahmen werden durch die Bestellung des Datenschutzbeauftragten, der Schulung der Mitarbeiter*innen und der Verpflichtung auf Vertraulichkeit sowie das Datengeheimnis gefestigt. Anlassbezogen kommt die Solvere gGmbH ihren Informationspflichten gemäß Art. 13 und 14 DSGVO, dem Widerrufsrecht der Betroffenen, der Pflicht zur Durchführung einer Datenschutz-Folgeabschätzung und der Bearbeitung von Auskunftsanfragen seitens Betroffener nach. Zu diesem Zweck wurden entsprechen Prozesse geschaffen.