Vereinbarung über Auftragsdatenverarbeitung i.S.d. §11 Bundesdatenschutzgesetz (BDSG)

zwischen

INFORM GmbH
Pascalstraße 35
52076 Aachen Im Folgenden „Auftragnehmer“

und

……

……

…… Im Folgenden „Auftraggeber“

Präambel

Diese ADV-Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz im Zusammenhang mit der Auftragsdatenverarbeitung, deren Einzelheiten sich aus dem zwischen den Vertragsparteien geschlossenen Vertrag zur Nutzung der Software „SyncroTESS“ beziehungsweise „SyncroSupply“ *[nicht Zutreffendes bitte streichen]* (im Folgenden „Vertrag“) ergeben.

Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen der Auftragnehmer oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsdatenverarbeitung

(1) Gegenstand und Dauer des Auftrags sowie Umfang und Art der Datenerhebung, -verarbeitung oder -nutzung ergeben sich aus dem Vertrag.

(2) Die Laufzeit dieser ADV-Vereinbarung richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser ADV-Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und ggf. in der Leistungsbeschreibung zum Vertrag konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»verantwortliche Stelle« im Sinne des § 3 Abs. 7 BDSG).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen oder diese ändern, werden vom Auftragnehmer als Antrag auf Leistungsänderung (Change Request) behandelt.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von Betroffenen nur im Rahmen des erteilten Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen des Bundesdatenschutzgesetzes (Anlage zu § 9 BDSG) genügen. Diese Maßnahmen werden wie aus dem Anhang zu dieser ADV-Vereinbarung ersichtlich festgelegt. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG notwendigen Informationen zur Verfügung, sofern er sie sich nicht selbst beschaffen kann.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen per Verpflichtung untersagt ist, die Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis entsprechend § 5 BDSG). Das Datengeheimnis besteht auch nach Beendigung des Auftrages fort.

(5) Unverzüglich nach Kenntniserlangung unterrichtet der Auftragnehmer den Auftraggeber bei schwerwiegenden Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder die im Vertrag getroffenen datenschutzrechtlichen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten nach § 42a BDSG.

(6) Der Auftragnehmer gewährleistet, seinen Pflichten nach §§ 4f, 4g BDSG nachzukommen (§ 11 Abs. 2 Nr. 5 i.V.m. § 11 Abs. 4 BDSG), wie z.B. seiner Pflicht, einen Datenschutzbeauftragen zu bestellen, soweit vom Gesetz vorgeschrieben. Der Auftragnehmer nennt dem Auftraggeber

auf entsprechende Nachfrage seinen betrieblichen Datenschutzbeauftragten bzw. den bei ihm zuständigen Ansprechpartner für die im Rahmen des Vertrages anfallende Datenschutzfragen.

(7) Der Auftragnehmer verwendet die überlassenen Daten – mangels anderslautender Vereinbarung – für keine anderen Zwecke als die der Vertragserfüllung.

(8) Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer auf Grund einer entsprechenden Einzelbeauftragung durch den Auftraggeber.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder an diesen herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben im Zusammenhang mit der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Datenverarbeitungsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Die Pflicht zur Führung des öffentlichen Verfahrensverzeichnisses (JedermannVerzeichnis) gem. § 4g Abs. 2 S. 2 BDSG liegt beim Auftraggeber.

§ 5 Anfragen Betroffener

(1) Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu erteilen, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen. Dies setzt voraus, dass der Auftraggeber den Auftragnehmer hierzu schriftlich oder in Textform aufgefordert hat und der Auftraggeber dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten erstattet.

(2) Der Auftragnehmer wird selbst keine Auskunftsverlangen von Betroffenen beantworten und den Betroffenen insoweit an den Auftraggeber verweisen. Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an den Auftragnehmer, wird der Auftragnehmer den Betroffenen ebenfalls an den Auftraggeber verweisen.

§ 6 Kontrollpflichten

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis.

- Hierfür kann er z. B. Auskünfte und Bestätigungserklärungen des Auftragnehmers einholen,
- sich ein ggf. vorhandenes Testat eines Sachverständigen vorlegen lassen
- oder nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten des Auftragnehmers ohne Störung des Betriebsablaufs die getroffenen Maßnahmen persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser vorab vertraglich zur Geheimhaltung verpflichtet wurde und nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle vernünftigerweise erforderlich sind.

§ 7 Subunternehmer

(1) Die Beauftragung von Subunternehmern durch den Auftragnehmer bedarf grundsätzlich der vorherigen Zustimmung (schriftlich oder in Textform) des Auftraggebers. Der Auftragnehmer wird Subunternehmer nach deren Eignung sorgfältig auswählen.

(2) Zum Zeitpunkt des Abschlusses dieser ADV-Vereinbarung bedient sich der Auftragnehmer der synaix Gesellschaft für angewandte Informations-Technologien mbH („synaix“) als Subunternehmerin. Synaix wird für den Auftragnehmer als externes Rechenzentrum tätig und verarbeitet und/oder nutzt in diesem Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für synaix gilt die Zustimmung des Auftraggebers nach Abs. 1 als erteilt. Dasselbe gilt, sofern der Auftragnehmer im Laufe des Vertragsverhältnisses ein anderes externes Rechenzentrum zusätzlich und/oder alternativ beauftragt. Der Auftragnehmer wird sich dabei nur solcher Anbieter bedienen, deren Server sich innerhalb des Gebietes der EU oder des EWR befinden.

(3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus dieser ADV-Vereinbarung auf den Subunternehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an die Vertraulichkeit, den Datenschutz und die Datensicherheit zwischen den Vertragsparteien. Eine etwaige Prüfung durch den Auftraggeber beim Subunternehmer erfolgt nur in Abstimmung mit dem Auftragnehmer.

Durch schriftliche Aufforderung kann der Auftraggeber vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Subunternehmers verlangen, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen (soweit keine gesetzlichen und/oder vertraglichen Vertraulichkeitspflichten der Einsichtnahme entgegenstehen).

(4) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen oder Wartung. Der Auftragnehmer wird mit solchen Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »verantwortlicher Stelle« im Sinne des Bundesdatenschutzgesetzes liegen.

(2) Änderungen und Ergänzungen dieser ADV-Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser ADV-Vereinbarung zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser ADV-Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der ADV-Vereinbarung im Übrigen nicht.

(4) Es gilt ausschließlich deutsches Recht.

Anhang zur ADV-Vereinbarung:

Beschreibung der technischen und organisatorischen Maßnahmen nach § 9 BDSG

1. Zutrittskontrolle

Ist die Anforderung der Anlage des § 9 BDSG zur Zutrittskontrolle erfüllt?

Gibt es Regelungen zum Gebäudezutritt und zum Betreten des Rechenzentrums bzw. zu den Räumen der Infrastruktur der DV-Einrichtungen?

Erläuterungen / Bemerkungen:

Die räumliche Annäherung an eine Datenverarbeitungsanlage (DVA) ist zu regeln. Es ist zu verhindern, dass unbefugte Personen die Möglichkeit irgendeiner Bedienung der DVA bekommen.

Beispiele:

- Zutrittskontrollsystem, Ausweisleser
- Magnetkarte, Chipkarte zu beachten: § 6c BDSG
- Schlüssel, Schüsselvergabe
- Türsicherung (elektrischer Türöffner usw.)
- Werkschutz, Pförtner
- Überwachungseinrichtung Alarmanlage, Video-/Fernsehmonitor zu beachten: § 6c BDSG

Bei der INFORM GmbH umgesetzte Maßnahmen:

- Festlegung befugter Personen
- Betrieb eines personenbezogenen Zutrittskontrollsystems (Chipkarte)
- Türsicherung (elektronische Schlösser an allen Gebäudeeingängen und Abteilungstüren sowie den Server-, Telefon und Patchräumen mit unterschiedlichen Zutrittsberechtigungen
- Alarmanlage für alle Gebäude mit Aufschaltung auf den Wachdienst, Videoüberwachung mit Speicherung der Alarmbilder für eine beschränkte Zeitspanne
- Pförtner, Sicherheitsdienst (Wachdienst in den Nachtstunden, am Wochenende und an Feiertagen; Authentifizierung beim Wachdienst außerhalb der Bürostunden)

2. Zugangskontrolle

Ist die Anforderung der Anlage des § 9 BDSG zur Zugangskontrolle erfüllt?

Gibt es Regelungen zur Benutzung von DV-Systemen?

Erläuterungen / Bemerkungen:

Jede unbefugte Nutzung von DVA ist zu verhindern, gleichgültig, ob diese mit Hilfe von Datenübertragungseinrichtungen (z. B. auch über das Internet) geschieht oder nicht.

Beispiele:

- Kennwortverfahren (u. a. Sonderzeichen, Mindestlänge, regelmäßige Wechsel des Kennworts)
- Automatische Sperrung (z. B. Kennwort oder Pausenschaltung)
- Einrichtung eines Benutzerstammsatzes pro User
- Verschlüsselung von Datenträgern

Bei der INFORM GmbH umgesetzte Maßnahmen:

- Festlegung befugter Personen
- Definierte Zugangsverfahren für Firmenfremde
- Kennwortverfahren (mit Sonderzeichen, Mindestlänge, regelmäßige Wechsel des Kennworts alle 180 Tage)
- Automatische Sperrung (automatisch startende Screen-Saver mit erneut notwendigen Login)
- Einrichtung eines Benutzerstammsatzes pro User
- Verschlüsselung von notwendigen Datenträgern

3. Zugriffskontrollen

Ist die Anforderung der Anlage des § 9 BDSG zur Zugriffskontrolle erfüllt?

Gibt es Richtlinien zur Einrichtung von Benutzerrechten, zu deren Änderungen und zum Entzug?

Erläuterungen / Bemerkungen:

Es ist sicher zu stellen, dass die Verarbeitung und Nutzung personenbezogener Daten auf das im Rahmen der Aufgabenzuweisung erforderliche beschränkt wird. Eine Regelung zur Vergabe und zum Entzug von Berechtigungen ist zu organisieren und umzusetzen. Dadurch sind personenbezogene Daten in allen Phasen der Erhebung, Verarbeitung und Nutzung und nach der Speicherung so zu schützen, dass Unbefugte sie weder lesen, kopieren, verändern noch entfernen können.

Beispiele:

- differenzierte Berechtigungen (Profile, Rollen, Transaktionen, Objekte)
- Verschlüsselung der Daten

Bei der INFORM GmbH umgesetzte Maßnahmen:

- Zentrale Rechteverwaltung für alle Nutzer
- Abgeschlossenes Rechtesysytem für die gesamte Infrastruktur in und zwischen den Abteilungen
- Differenzierte Berechtigungen für die einzelnen Mitarbeitergruppen
- Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen
- Sonderzugänge (speziell geschützte PCs) für sensitive Daten (projektspezifisch)
- Verschlüsselung und/oder Anonymisierung personenbezogener Daten (projektspezifisch)
- Verschlüsselung mobiler Datenträger in kritischen Bereichen
- Zentrale zugangsgeschützte Datenbank-Server für die Haltung der Kunden-Testdaten
- Nach Ende der Bearbeitung sind die Kundendaten von den Datenbank-Servern zu löschen
- Sicherheitsschränke zur Aufbewahrung von Datenträgern

4. Weitergabekontrolle

Ist die Anforderung der Anlage des § 9 BDSG zur Weitergabekontrolle erfüllt?

Ist die Übermittlung oder Weitergabe von Daten geregelt? Ist der Versand von Datenträgern (auch Papier) geregelt? Bestehen Vorschriften für die Übermittlung von sensiblen oder personenbezogenen Daten (Passwörter, Verschlüsselung etc.)?

Bestehen verfahrensunabhängige Plausiblitäts- und Sicherheitsüberprüfungen beim Dateneingang durch den Auftragnehmer? Findet eine Prüfung der Richtigkeit der Ergebnisse beim Auftraggeber statt?

Erläuterungen / Bemerkungen:

Personenbezogene Daten sind bei der elektronischen Übertragung oder während ihres Transports so zu sichern, dass sie nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (ggf. Verschlüsselung). Es ist zu regeln, dass neben der Überprüf- und Nachvollziehbarkeit der Datenübertragung auch der Zugriff Unbefugter auf dem Übertragungsweg verhindert werden kann. Da dies heute technisch nicht sicher zu stellen ist, ist zu gewährleisten, dass das Verändern oder das Löschen von Daten erkannt werden kann.

Beispiele:

- Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
- Elektronische Signatur
- Protokollierung
- Transportsicherung

Bei der INFORM GmbH umgesetzte Maßnahmen:

- Verschlüsselung / Tunnelverbindung via VPN-Client
- Authentifizierung mit Token
- Kundenspezifische Zertifikate mit Ablaufdatum
- Protokollierung der VPN-Zugänge in Standard Log-Dateien und Online-Überwachung. Es werden alle Einwahlvorgänge protokolliert.
- Das Split-Tunneling ist im VPN-Client deaktiviert
- Verschlüsselung von Datenträgern mittels Truecrypt oder mittels DPM (Hardware abhängig)
- Transport von Datenträgern nur durch autorisierte Personen (projektspezifisch)

5. Eingabekontrolle

Ist die Anforderung der Anlage des § 9 BDSG zur Eingabekontrolle erfüllt?

Werden die Erfassung, Veränderung und Löschung von personenbezogenen Daten protokolliert?

Erläuterungen / Bemerkungen:

Es ist zu gewährleisten (durch Protokollierung), dass nachträglich überprüft und festgestellt werden kann, ob, wen von wem und zu welcher Zeit personenbezogene Daten eingegeben, verändert oder gelöscht wurden.

Beispiele:

- Protokollierungs- und Protokollauswertungssysteme

Bei der INFORM GmbH umgesetzte Maßnahmen:

- Protokollierung in Logfiles wer wann welche Daten geändert hat (projektspezifisch)
- Protokollierte Eingabekontrolle im Produktiv-System (projektspezifisch)
- Dateneingabe/-veränderung nur durch autorisierte Personen (projektspezifisch)
- Alle Datenänderungen und Anmeldevorgänge werden in der jeweiligen Datenbank protokolliert, wer wann welche Daten geändert hat

6. Auftragskontrolle

Ist die Anforderung der Anlage des § 9 BDSG zur Auftragskontrolle erfüllt?

Sind alle Anforderungen des § 11 BDSG (ADV) schriftlich fixiert (Kontrollrechte des Auftraggebers, Rechte der Betroffenen, Weisungen des Auftragnehmers, Unterauftrag, Verpflichtung der MA gemäß § 5 BDSG, Technische und organisatorische Maßnahmen)? Werden die mit der Serviceleistung beauftragten Beschäftigten des Auftragnehmers dem Auftraggeber namentlich gekannt gegeben? Wird beim Personalwechsel der Auftraggeber informiert? Sind Geheimhaltungsverpflichtungen zwischen den Unternehmen geregelt?

Ist eine Weisungsbefugnis hinsichtlich der Verarbeitung der personenbezogenen Daten im Vertrag schriftlich fixiert? Ist vertraglich festgelegt, dass alle personen-bezogenen Daten nur im Rahmen der Weisungen der ADV verwendet werden und ist die Weitergabe an Dritte ohne schriftliche Genehmigung des Auftraggebers ausgeschlossen?

Erläuterungen / Bemerkungen:

Es ist sicher zu stellen, dass die Vorschriften über die ADV (§ 11 BDSG) eingehalten werden.

- Kontrollen durch den Auftraggeber:

Der Auftraggeber wird regelmäßig Kontrollen über die Einhaltung der vertraglichen Regeln beim Auftragnehmer durchführen.

- Rechte der Betroffenen:

Die Rechte des Betroffenen sind gegenüber dem Auftragnehmer geltend zu machen. Es ist zu vereinbaren, dass, wenn Betroffene ihre Rechte unmittelbar beim Auftragnehmer geltend machen, der Auftraggeber hierüber unverzüglich zu benachrichtigen ist.

- Datengeheimnis:

Für die beim Auftragnehmer beschäftigten Personen gilt das Datengeheimnis gemäß § 5 BDSG, sofern sie bei der Erhebung, Verarbeitung bzw. Nutzung der personenbezogenen Daten in einer Phase der Datenverarbeitung (Speicherung, Übermittlung, Veränderung, Löschung oder Sperrung) oder bei der Nutzung tätig sind. Insbesondere die gesetzliche Verpflichtung der sorgfältigen Auswahl des Auftragnehmers erfordert es, diesen Punkt sowie zusätzliche Regelungen über die Wahrung von Geschäftsgeheimnissen im Vertrag zu regeln.

Beispiele:

- eindeutige Vertragsgestaltung
- formalisierte Auftragserteilung (Auftragsformular)
- Kriterien zur Auswahl des Auftragsnehmers
- Kontrolle der Vertragsausführung

Bei der INFORM GmbH umgesetzte Maßnahmen:

- Personenbezogene Daten werden generell nicht zur Verarbeitung an fremde Firmen weiter gegeben, projektspezifisch ist eine Zusammenarbeit mit ausgewählten langjährigen Partnerfirmen notwendig.
- Eindeutige Vertragsgestaltung zwischen INFORM den Partnerfirmen
- Kontrolle der Vertragsausführung
- Vollständige Datenlöschung nach Auftragsbeendigung (inkl. Wartungsbeauftragung)
- Nicht mehr benötigte Kundendaten werden gelöscht

7. Verfügbarkeitskontrolle

Ist die Anforderung der Anlage des § 9 BDSG zur Verfügbarkeitskontrolle umgesetzt?

Existiert beim Auftragnehmer ein Backup-Konzept und wird dieses regelmäßig überprüft? Wird der Katastrophenfall geübt? Ist der Speicher- und Verarbeitungsort genau bezeichnet? Wurde die Aufbewahrungsdauer der Datenbestände und ggf. der Software festgelegt?

Erläuterungen / Bemerkungen:

Die Verfügbarkeit personenbezogener Daten ist zu gewährleisten. Es sind Maßnahmen zu ergreifen, dass DV-Systeme (Hardware und Software) vor zufälliger Zerstörung (K-Fall) geschützt werden.

Beispiele:

- Back up Verfahren
- Spiegeln von Festplatten, z. B. RAID-Verfahren
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte Aufbewahrung
- Virenschutz, Firewall
- Notfallplan

Bei der INFORM GmbH umgesetzte Maßnahmen:

- Back up Verfahren
- Tages-, Wochen, - Monats- und Jahres-Sicherungskopien an unterschiedlichen Aufbewahrungsorten
- RAID Verfahren
- Unterbrechungsfreie Stromversorgung (Notstrom-Anlagen für den Serer-Bereich, Wartungsverträge mit den Herstellern, automatisierte Wartung gemäß Wartungszyklen)
- Virenschutz, Firewall
- Notfallplan

8. Trennungskontrolle

Ist die Anforderung der Anlage des § 9 BDSG zur Gewährleistung der getrennten Verarbeitung (Trennungsgebot) von zu unterschiedlichen Zwecken erhobenen Zwecken erfüllt?

Sind die Systeme mandantenfähig?

Erläuterungen / Bemerkungen:

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden

können. Es besteht keine Notwendigkeit zu einer physischen Trennung. Eine logische Trennung genügt.

Beispiele:

- "interne Mandantenfähigkeit" / Zweckbindung
- Funktionstrennung (Produktion, Test)

Bei der INFORM GmbH umgesetzte Maßnahmen:

- Funktionstrennung (Produktion, Test)
- Trennung der Datenablage und Zugriffsberechtigung je nach Funktion und Mitarbeitergruppe

9. Sonstiges

9.1 Fernwartungs-Zugänge zu Kundensystemen

Es ist sicherzustellen, dass Zugänge zu und von fremden IT-Systemen/-Netzen besonders gesichert und untereinander abgeschottet sind. Weiterhin ist der Personenkreis, der Zugang zu den Systemen hat, zu beschränken.

Beispiele:

- spezielle Fernwartungs-Zugänge
- DMZ, Firewall-Konfigurationen
- VPN-Kanäle

Bei der INFORM GmbH umgesetzte Maßnahmen:

- Individuelle Konfiguration jedes einzelnen Fernwartungszugangs
- Strikte Einhaltung der INFORM-eigenen UND der Kunden-Anforderungen bzgl. Zugang und Sicherheit
- Umsetzung verschiedenster Techniken (LAN-Kopplung, VPN-Systeme, spezielle Fernwartungs-PCs/-VM-Systeme, etc.)

……., den ……. . ……. . ……..
Ort, Datum

……
Name und Unterschrift des Verantwortlichen der INFORM GmbH

……., den ……. . ……. . ……..
Ort, Datum

……
Name und Unterschrift des Verantwortlichen des Auftraggebers