Datenschutzkonzept

der

InterConnect GmbH & Co. KG

Stand: 06.10.2020

Verfasser: Dr. Ralf Schadowski

Inhaltsverzeichnis

1. Vorbemerkung

Die InterConnect GmbH & Co. KG bietet als System- und Softwarehaus mit Sitz in Karlsruhe individuelle IT-Dienstleistungen und internetbasierte Softwarelösungen an.

Im Bereich IT-Dienstleitungen liegt der Schwerpunkt der Kompetenzen auf der kompletten IT-Infrastruktur und der IT-Sicherheit. Die Leistungsangebote beinhalten dabei alle IT-Services von der Beratung, Realisierung, Projektbegleitung bis hin zur Komplettbetreuung der IT-Infrastruktur ihrer Kunden. Der Kundenstamm erstreckt sich zum einen auf kleinere und mittlere Unternehmen, die über keine oder nur eine kleine IT-Abteilung verfügt. Dort werden ein Großteil der erforderlichen Leistungen im Auftrag der Kunden übernommen. Zum anderen werden große Unternehmen als Kunden akquiriert, die Mitarbeiter der InterConnect GmbH & Co. KG in ihre IT-Projekte mit einbeziehen.

Die internetbasierten Softwarelösungen werden speziell für Non-Profit Unternehmen wie Verbände und Vereine entwickelt. Dort beinhaltet das Leistungsportfolio spezielle Online-Verwaltungslösungen beispielsweise für große Sportverbände, aber auch für kleinere Vereine. Darüber hinaus runden die Angebotspalette individuelle Softwareentwicklungen maßgeschneidert auf die Kundenanforderungen ab.

Gegründet wurde das Unternehmen im Jahr 1989 zunächst als GmbH und wurde im Jahr 2004 in eine GmbH & Co. KG umgewandelt. Die Gründer sind auch heute noch als Gesellschafter in der Geschäftsführung tätig.

2. Geltungsbereich

Das Datenschutzkonzept gilt für die

InterConnect GmbH & Co. KG

Am Fächerbad 3

76131 Karlsruhe

Sitz der Gesellschaft: 76131 Karlsruhe

Amtsgericht Mannheim HRA 105138

3. Definitionen und Begrifflichkeiten

Sämtliche Definitionen und Begrifflichkeiten können Anlage 1 entnommen werden.

4. Regelungen der Verantwortlichkeiten im Datenschutz

Der Datenschutz und die Sicherheit informationstechnischer Systeme stellen elementare und unternehmensbezogen umzusetzende Erfordernisse an den täglichen Geschäftsbetrieb. Hierfür sind die Geschäftsleitung sowie deren maßgebenden handelnden Leitungspersonen unmittelbar verantwortlich.

Geschäftsführung und sonstige Personen

(insbesondere berufene Leiter, die mit der Datenverarbeitung betraut sind)

Gert Rudolph, Ben Rudolph

IT-Leiter

(der mit der Datenverarbeitung im Bereich der Servicedienstleistungen beauftragt ist):

Herrn

Peter Rohnacher

peter.rohnacher@interconnect.de

Tel.:+49 (0)721 6656-415

Ansprechpartner für Servicedienstleistungen

Für Kunden stehen als Ansprechpartner für administrative, leistungsbezogene sowie finanzielle Angelegenheiten Mitarbeiter der nachfolgenden Abteilungen zur Verfügung:

- Vertrieb IT-Services Tel.: 0721-6656300 EMAIL: vertrieb@interconnect.de
- Vertrieb IntelliOnline Tel.: 0721-6656300 EMAIL: vertrieb@intellionline.de

Mitarbeiter, die Zugriff auf personenbezogene Daten haben

Den Zugriff auf personenbezogene Daten haben lediglich durch den Datenschutzbeauftragten geschulte Mitarbeiter der jeweiligen Abteilungen entsprechend ihren Aufgaben und den zugehörigen Rollen-/Berechtigungskonzepten. Die Mitarbeiter sind darüber hinaus über eine IT-Benutzerrichtlinie oder mindestens durch eine Vereinbarung zur E-Mail- und Web-Nutzung am Arbeitsplatz (VEWA) über interne Kontrollen zur Einhaltung datenschutzrechtlicher Vorschriften aufgeklärt worden.

Datenschutzbeauftragter

Nach Art. 37 der EU-DSGVO haben öffentliche und nichtöffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen einen Beauftragten für den Datenschutz zu bestellen. Der Datenschutzbeauftragte wirkt auf die Einhaltung des Datenschutzes hin.

Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Grundlage und Maßstab der Aufgabenerfüllung des Datenschutzbeauftragten sind die für die Interconnect einschlägigen Rechtsvorschriften zum Datenschutz. Im Rahmen seiner Aufgabenerfüllung sowie der Anwendung seiner Fachkunde ist der Datenschutzbeauftragte weisungsfrei. Gegenüber der Geschäftsführung der Interconnect hat er ein direktes Vortragsrecht und ist dieser unmittelbar unterstellt.

Zur Beantwortung datenschutzrechtlicher Begehren kann sich der Kunde an den, am 24.05.2018 elektronisch bei der Aufsichtsbehörde gemeldeten, bestellten externen Datenschutzbeauftragten wenden:

Herrn
Dr.rer.nat. Ralf W. Schadowski
c/o ADDAG GmbH&Co.KG
Krefelder Strasse 121
52070 Aachen

Tel.: +49 (0)241 44688 - 0
Fax: +49 (0)241 44688 - 26
E-Mail: Datenschutz@interconnect.de

Qualifikationen zur erforderlichen Fachkunde des Datenschutzbeauftragten:

- Nach ISO/IEC 17024 zertifizierter und überwachter europäischer Datenschutzbeauftragter
- ISO/IEC 27001 zertifizierter Lead Auditor (PECB), anerkannter Auditor IT-Sicherheit
- TÜV cert. sachkundiger Datenschutzbeauftragter
- Fachgruppenleiter für Datenschutz und Vorstand beim Bundesverband der IT-Sachverständigen BISG e.V.
- aktives Mitglied in der Gesellschaft für Datenschutz und Datensicherheit GDD e.V.

Für die Einhaltung der Regelungen zum Betrieb und Sicherheit der informationstechnischen Systeme ist der folgende Ansprechpartner zuständig:

Herrn

Peter Rohnacher

peter.rohnacher@interconnect.de

Tel.:+49 (0)721 6656-415

Datenschutzbericht

Die Interconnect beabsichtigt über die erforderlichen Maßnahmen und Umsetzungen regelmäßige unternehmensinterne Statusberichte zu erstellen. Diese haben mindestens zu enthalten:

- die Durchführung einer Bestandsaufnahme zur Feststellung der Erfüllung gesetzlicher Anforderungen
- Ermittlung, Feststellung und Kontrolle des Handlungs- bzw. Änderungsbedarfs in Bezug auf notwendige Schutzmaßnahmen, sowie Festlegung der Zielstellungen
- Entwicklung / Anpassung von (internen) Richtlinien und Arbeitsanweisungen sowie Formularen zur Realisierung der Anforderungen
- Beurteilung / Bewertung der Angemessenheit der getroffenen technischen und organisatorischen Maßnahmen (vgl. insb. Art. 32 der EU-DSGVO)
- Überwachungsmaßnahmen der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen
- durchgeführte Vorabkontrollen, Schulungen und internen Sicherungsmaßnahmen
- Überblick über aufgetretene Problemfelder und deren Bearbeitung
- Kenntnisnahme des Berichts des Datenschutzbeauftragten

Seit dem 24.05.2018 sind bei der Interconnect GmbH & Co. KG keine Datenschutzverletzungen nach Art. 33, 34 DSGVO bekannt geworden.

Zur Identifikation von meldungspflichtigen Datenschutzverletzungen nach Art. 33, 34 DSGVO, wurden die Data Owner im Unternehmen im Zuge der Umsetzung des sachgerechten Auskunftsverfahrens auf die Risiken und Meldewege beim unsachgemäßen Umgang mit

personenbezogenen Daten besonders hingewiesen und darüber hinaus angewiesen, bei aufgetretenen Verstößen unverzüglich an den Datenschutzbeauftragten zu melden.

5. Umfang und Verwendung personenbezogener Daten / Datenkategorien

Der Umfang und die Verwendung personenbezogener Daten für Interconnect ergeben sich in dem überwiegenden Maß aus den Regelungen der EU-Datenschutz Grundverordnung sowie sonstigen landes- und bundesrechtlichen Datenschutzvorschriften.

Die EU-Datenschutz Grundverordnung geht zur Gewährleistung des informationellen Selbstbestimmungsrechts ebenso wie andere Datenschutznormen von den folgenden Grundregeln aus:

- dem präventiven Verbotsprinzip, das heißt die Zulässigkeit des Umgangs mit personenbezogenen Daten bedarf grundsätzlich der gesetzlichen Erlaubnis oder Einwilligung
- der Zweckbindung / dem Zweckentfremdungsschutz
- der Transparenz (Informationen, Benachrichtigung und Auskunftsanspruch)
- den Grundsätzen der Datenvermeidung und Datensparsamkeit
- des Bestehens von Korrekturrechten (Berichtigung, Sperrung, Löschung und Widerspruch)
- der umfassenden Datensicherung (Schutz vor Verlust, Sabotage, unbefugten Zugriff)
- Durchführung von Kontrollen (intern / extern)

Rechtsgrundlage der Verarbeitung

Im Anwendungsbereich der EU-Datenschutz Grundverordnung richten sich die Zulässigkeit der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nach der zentralen Aussage:

"*Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat*."

Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren das:

- Speichern, Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung
- Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten
- Übermitteln; das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
  - die Daten an den Dritten weitergegeben werden oder
  - der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft
- Sperren: das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken
- Löschen: das Unkenntlich machen gespeicherter personenbezogener Daten
- Nutzen: ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt, vom bloßen Einsicht nehmen durch Mitarbeiter der verantwortlichen Stelle bis zum Gebrauch der Daten

Jedwede Verarbeitung von Kundendaten als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig:

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

Zweckbindung und Berücksichtigung besonderer personenbezogener Daten

Personenbezogene Daten werden ausschließlich zu den vorgenannten Zwecken verarbeitet.

Die Daten des Kunden können an die folgenden Dritten, bei der Vorlage eines rechtlichen Erlaubnistatbestandes weitergegeben werden:

- Öffentliche Stellen, sofern vorrangiger Rechtsvorschriften / bzw. Erlaubnissätze existieren (z.B. Ermittlungsbehörden, Finanzbehörden, Sozialversicherungs-träger usw.)
- Auftragnehmer, insbesondere Auftragsverarbeiter gemäß Art. 28 EU-DSGVO
- sowie externe Stellen und interne Abteilungen zur Erfüllung der Aufgabenstellung

Besondere Arten personenbezogener Daten nach Art. 9 EU-DSGVO, also Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) werden von der Interconnect grundsätzlich nicht automatisiert verarbeitet, es sei dies ist aufgrund zwingender gesetzlicher Regelungen geboten (z.B. zur Beachtung von arbeits- und / oder steuer-rechtlichen Tatbeständen) bzw. es liegt eine gesonderte Einwilligung der Betroffenen nach Art. 7 EU-DSGVO vor, welche offen dargestellt jederzeit widerrufen werden können.

Einhaltung von Datensparsamkeit, Datenvermeidung

Die Interconnect hat sich dem Grundsatz der Datenvermeidung und Datenminimierung nach Art. 5 EU-DSGVO verpflichtet. Die Mitarbeiter sind angewiesen, sofern nicht anders angeordnet, dafür Sorge zu tragen, so wenig personenbezogene Daten wie nötig zu erheben, zu verarbeiten oder zu nutzen. Hierzu wurde allen Mitarbeitern die Datenschutzrichtlinie vorgelegt. In dieser wird den Mitarbeitern u.a. dargestellt, wie bei der Meldung von Datenschutzverletzungen verfahren wird. Darüber hinaus wird den Mitarbeitern das Verständnis zum Risiko beim Umgang mit personenbezogenen Daten vermittelt.

Empfänger von Daten

An die im Folgenden aufgeführten Stellen können zweckgebunden personenbezogene Daten mitgeteilt werden:

- Öffentliche Stellen, sofern vorrangiger Rechtsvorschriften / bzw. Erlaubnissätze existieren (z.B. Ermittlungsbehörden, Finanzbehörden, Sozialversicherungsträger usw.)
- Auftragnehmer, insbesondere Auftragsverarbeiter gemäß Art. 28 EU-DSGVO
- Etwaige gemeinsam Verantwortliche nach Art. 26 DSGVO mit Interconnect

Auftragsverarbeiter werden hierbei auf Grundlage eines geeigneten Risikomodells nach Art. 25 Abs. 1 DSGVO, sowie der Sicherstellung der Rechtsgrundlage zweiter Stufe bei Datentransfers in Drittstaaten ausgewählt. Durch die geschlossenen AV-Verträge als Auftraggeber werden die Dienstleister darauf verpflichtet, bei Datenschutzverletzungen im eigenen Hause den Auftraggeber (Interconnect) zu informieren. Dies schließt ebenfalls ein überzeugendes Konzept zur Erkennung von Datenschutzverletzungen auf Grundlage des sachgerechten Auskunftsverfahrens bei den Auftragsverarbeitern mit ein.

Recht auf Auskunft, Berichtigung, Sperrung, Widerspruch, Schadensersatz

Jedweden betroffenen Personen stehen gesetzliche Rechte auf Auskunft, Berichtigung, Sperrung sowie Widerspruch zu.

In Abstimmung mit dem Datenschutzbeauftragten ist dem Begehren der Betroffenen ausreichend Rechnung zu tragen und unverzüglich nachzukommen. Hierzu wurde das sachgerechte Auskunftsverfahren nach Art. 15 DSGVO in Zusammenarbeit mit dem Datenschutzbeauftragten bei der Interconnect umgesetzt. Es wurden Workflows zu Anfragen Betroffener, Auskunft an die Aufsichtsbehörde, sowie ein Datenschutzeskalationsplan gemeinsam mit den internen Verantwortlichen des Unternehmens erarbeitet. Die zugehörigen Datenspeicherorte von personenbezogenen Daten wurden erkannt und definiert. Um eine fristgerechte Beantwortung von Anfragen Betroffener in Zusammenarbeit mit dem Datenschutzbeauftragten zu garantieren wurden in diesem Zusammenhang Ansprechpartner mit Vertretungen der relevanten Abteilungen im Unternehmen, welche mit personenbezogenen Daten in Berührung kommen, an den Datenschutzbeauftragten übermittelt. Durch die Umsetzung ist ebenfalls die Zusammenarbeit der Abteilungen in Datenschutzfragen sichergestellt.

Vermeidung von Rechtsverletzungen und ihrer Folgen

Sowohl die Mitarbeiter als auch die für die Interconnect tätigen Dienstleister sind, respektive werden auf die Einhaltung der spezifischen datenschutzrechtlichen Regelungen belehrt und auf das Datengeheimnis verpflichtet.

Sofern Rechtsverletzungen bekannt werden und / oder derartige von Dritten glaubhaft gemacht werden, sind der Datenschutzbeauftragte sowie die Geschäftsleitung unverzüglich zu informieren.

Stellt die Interconnect fest, dass bei ihr gespeicherte besondere Arten personenbezogener Daten (Art. 9 EU-DSGVO), personenbezogene Daten, die einem Berufsgeheimnis unterliegen, personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder personenbezogene Daten zu Bank- oder Kreditkartenkonten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, respektive in Zweifelsfällen, teilt sie dies unverzüglich den zuständigen Aufsichtsbehörden sowie den Betroffenen mit (Art. 33 EU-DSGVO).

Löschung von Daten

Die Löschung von Daten erfolgt unverzüglich, sofern ein derartiges Verlangen bei der Interconnect eingeht.

An die Stelle einer Löschung tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

Relevante Aufbewahrungsfristen ergeben sich insbesondere aus den folgenden Regelungen:

- Aufbewahrungsfrist: 6 Jahre (§ 147 Abs. 3 AO, 14 b UStG bzw. § 257 Abs. 4 HGB);
- Aufbewahrungsfrist: 10 Jahre (§ 147 Abs. 3 AO, 14 b UStG bzw. § 257 Abs. 4 HGB);
- Aufbewahrungsfrist: Dauer gemäß vertraglicher Vereinbarung und sonstigen Regelungen (§ 9 GWG);
- Aufbewahrungsfrist: grundsätzlich 3 Jahre (§ 195 BGB).

6. Regelungen zur IT-Sicherheit

Informationsverarbeitung spielt eine Schlüsselrolle für die Aufgabenerfüllung der Interconnect. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch

Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von Systemen muss insgesamt kurzfristig kompensiert werden können.

Alle Mitarbeiter von der Interconnect halten die einschlägigen Gesetze (z. B. Strafgesetzbuch, Betriebsverfassungsgesetz, Handelsgesetzbuch, Sozialgesetzbuch, Gesetze und Regelungen zum Datenschutz) und vertraglichen Regelungen ein. Negative finanzielle und immaterielle Folgen für den Auftraggeber sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden. Alle Mitarbeiter und die Geschäftsführung sind sich ihrer Verantwortung beim Umgang mit den Dienstleistungen bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften.

Zum Schutz, Aufrechterhaltung und Gewährleistung der IT-Sicherheit sowie der Servicequalität hat sich die Interconnect zur Einhaltung der Wahrung einer Prozess-Dokumentation verpflichtet. Eine umfassende Darstellung findet sich im verbundenen IT-Sicherheitskonzept wieder. Hierüber wird ebenfalls sichergestellt, dass die Risiken gegen die Unternehmenswerte minimal gehalten werden im Gegensatz zum Fokus der Rechte und Freiheiten natürlicher Personen im Datenschutz.

Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung (DSFA) ist ein Instrument, um ein Risiko (siehe Anlage 2) zu erkennen und zu bewerten, das für das Individuum in dessen unterschiedlichen Rollen (als Betroffene, Beschäftigte, etc.) durch den Einsatz einer bestimmten Technologie oder eines Systems durch eine Einrichtung/Träger entsteht. Ziel einer DSFA ist es, Kriterien des operationalisierten Grundrechtsschutzes zu definieren, die Folgen von Datenverarbeitungspraktiken möglichst umfassend zu erfassen sowie objektiv und nachvollziehbar mit Blick auf die verschiedenen Rollen und damit verbundenen Interessen so zu bewerten, dass mit adäquaten Gegenmaßnahmen begegnet werden kann.

Die Risikoanalyse erfolgt anhand festgelegter Risiken für Betroffene, Risikoquellen, Schadenshöhen, Eintrittswahrscheinlichkeiten, Risikobewertungen und Risiko-Bewältigung vor und nach Maßnahmen-festlegung. Nach der zweiten Risikoanalyse mit festgelegten, streng umzusetzenden, technisch-organisatorischen Maßnahmen kommt es zum Ergebnis der Risikoanalyse, die im positiven Fall zur Einführung der neuen bzw. zum Weiterbetreiben der vorhandenen Verarbeitungstätigkeit führt. Die negative Risikoanalyse bewirkt im ungünstigsten Fall eine negative DSFA, die zur Einbindung der Aufsichtsbehörde in den Entscheidungsprozess führt. Dieses Modell ist sowohl den Verantwortlichen für den Datenschutz, dem Datenschutzbeauftragten, sowie dem Informationssicherheitsbeauftragten bekannt und wurde von diesen verstanden.

Definitionen für die Schutzbedarfskategorien sind die folgende Eingruppierung[1]:

- Normal: Schadensauswirkungen sind begrenzt und überschaubar und etwaig eingetretene Schäden für Betroffene relativ leicht durch eigene Aktivitäten zu heilen
- Hoch: die Schadensauswirkungen werden für Betroffene als beträchtlich eingeschätzt, z. B. weil der Wegfall einer von einer Organisation zugesagten Leistung die Gestaltung des Alltags nachhaltig veränderte und die Betroffenen nicht aus eigener Kraft handeln können, sondern auf Hilfe angewiesen wären
- Sehr hoch: Die Schadensauswirkungen nehmen ein unmittelbar existenziell bedrohliches, katastrophales Ausmaß für Betroffene an.

Grundsätzlich sollte ein hoher bzw. sehr hoher Schutzbedarf der Daten sichergestellt werden und Risiken minimiert werden.

Allgemeine Risiken

Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Verarbeitung personenbezogener Daten verbundenen Risiken berücksichtigt werden, wie etwa – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnten. Siehe hierzu Anhang 2.

Die Umsetzung der DSFA mit Risikoanalyse erfolgt durch ein eigenes Instrument, bestehend aus der Word-Datei „DSFA-Formular“ und der Excel-Datei „DSFA“.

Eine DSFA ist stets bei Einführung neuer Verarbeitungstätigkeiten durchzuführen. Bei bestehenden Verarbeitungstätigkeiten sollte eine DSFA für die führenden Verfahren durchgeführt werden.

Die Dokumentationen der DSFA erfolgen separat außerhalb dieses Datenschutzkonzeptes.

[1] Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen: Standard-Datenschutzmodell. [Online, zitiert am 2016-02-08]; Verfügbar unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Standard-Datenschutzmodell/SDM-Handbuch_V09a.pdf

7. Technische und Organisatorische Maßnahmen (TOM)

Zur Umsetzung der vorgenannten Anforderungen sind technische und organisatorische Datenschutzmaßnahmen zu implementieren. Gemäß Art. 25, 32 DSGVO werden folgend die technischen und organisatorischen Maßnahmen dargestellt. Die Wirksamkeit nachfolgender Maßnahmen wird mittels des Plan-Do-Check-Act (PDCA) Zyklus nachgehalten. Hierzu wird der Aufbau, die Implementierung, die Überprüfung sowie die Optimierung und Mängelbeseitigung der Maßnahmen zur Sicherheit der Verarbeitung von personenbezogenen Daten auf Grundlage des Datenschutz-Managementsystems (siehe ebenfalls Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung nach Art. 32 DSGVO weiter unten) bei der Interconnect als praktische Umsetzung genutzt.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Bei der Interconnect wurden folgende Maßnahmen getroffen:

- Alarmanlage
- Manuelles Schließsystem
- Videoüberwachung der Zutrittbereiche
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Bei der Interconnect wurden folgende Maßnahmen getroffen:

- Zuordnung von Benutzerrechten
- Passwortvergabe
- Authentifikation mit biometrischen Verfahren
- Authentifikation mit Benutzername / Passwort
- Protokollierung der Besucher
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern
- Einsatz von Hardware-/Software-Firewalls

Zugriffskontrolle

Maßnahmen, die 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.

Bei der Interconnect wurden folgende Maßnahmen getroffen:

- Verwaltung der Benutzerrechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Einsatz von Dienstleistern zur Akten- und Datenvernichtung

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Bei der Interconnect wurden folgende Maßnahmen getroffen:

- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

Pseudonymisierung

Es erfolgt keine Pseudonymisierung.

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

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

Bei der Interconnect wurden folgende Maßnahmen getroffen:

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- E-Mail-Verschlüsselung

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Bei der Interconnect wurden folgende Maßnahmen getroffen:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

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

Verfügbarkeitskontrolle

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

Bei der Interconnect wurden folgende Maßnahmen getroffen:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Maßnahmen, die gewährleisten, dass nach einer Unterbrechung schnellstmöglich der Datenzugriff wiederhergestellt wird.

Bei der Interconnect wurden folgende Maßnahmen getroffen:

- Vorhandenes Backup & Recoverykonzept

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

Datenschutz-Management

Maßnahmen, die gewährleisten, dass die Anforderung der DS-GVO nachprüfbar umgesetzt wurden.

Bei der Interconnect wurden folgende Maßnahmen getroffen:

- DSMS vorhanden
- Regelmäßige Datenschutz Audits

Incident-Response-Management

Maßnahmen, die gewährleisten, dass nach einer Störung der Auftraggeber eine Information über die Störung erhält, sofern dessen Daten betroffen waren.

Bei der Interconnect wurden folgende Maßnahmen getroffen:

- Eskalations-Management vorhanden
- Einbindung des DSB Sicherheitsvorfällen / Datenpannen

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Maßnahmen, die gewährleisten, dass nach einer zeitlichen Vorgabe personenbezogene Daten gelöscht werden:

Bei der Interconnect wurden folgende Maßnahmen getroffen:

- Manuelle Softwareunterstützung
- Automatische Softwareunterstützung
- Eigenentwicklungen

Auftragskontrolle

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

Bei der Interconnect wurden folgende Maßnahmen getroffen:

- Auswahl eines Auftragnehmers unter Sorgfaltsgesichtspunkten
  (insbesondere hinsichtlich Datensicherheit)
- Vorherige Prüfung der und Dokumentation
  der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Schriftliche Weisungen an den Auftragnehmer
  (z.B. durch Auftragsverarbeitungsvertrag) i.S.d. Art. 28 DS-GVO
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

8. Datenschutzerklärung

Verfahren automatisierter Verarbeitungen sind von dem Verantwortlichen der Verarbeitung zu verzeichnen und im Einzelnen in sogenannte Verzeichnisse von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO aufzuführen. Gemäß Art. 13 EU-DSGVO hat der Verantwortliche den Kreis der betroffenen Personen vorab über die Verarbeitung der personenbezogenen Daten zu informieren, ehe eine Einwilligung erfolgt.

Diesem Erfordernis entsprechend hält die Interconnect die Datenschutzerklärung zur Einsicht bereit.

Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegt diese einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO. Eine Datenschutz-Folgenabschätzung ist insbesondere durchzuführen, wenn besondere Arten personenbezogener Daten (Art. 9 EU-DSGVO: Verarbeitung besonderer Kategorien personenbezogener Daten) verarbeitet werden oder die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens, es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Vor der Einführung neuer IT-Systeme bzw. Verfahren automatisierter Verarbeitungen stimmt sich die Interconnect mit dem Datenschutzbeauftragten über die Zulässigkeit als auch die weitere Vorgehensweise ab.

9. Allgemeine Belehrungen zum Thema Datenschutz

Die Interconnect legt Wert darauf, dass ihre Mitarbeiter und / oder die für sie tätigen Dritten im ausreichenden Maß über die datenschutzrelevanten Bestimmungen informiert und in regelmäßigen Abständen hierüber belehrt werden.

Neben den ausdrücklichen in den Arbeitsverträgen enthaltenden datenschutzrechtlichen Regelungen sowie den Bestimmungen zur Wahrung der Vertraulichkeit sind die Mitarbeiter von der Interconnect in ihrer praktischen Arbeit auf die Wahrung des Datenschutzes und der Datensicherheit sensibilisiert. Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Die Interconnect ist zudem bestrebt sämtlichen Mitarbeitern und / oder Dritten, welche die IT-Systeme, respektive die vorhandene Infrastruktur, nutzen, die Wahrung des Datenschutzes und der Datensicherheit zu gewährleisten. Hierfür wurden diverse Richtlinien (insbesondere zur Nutzung von Ressourcen) veröffentlicht.

10. Regelungen zur IT-Nutzung

Die Interconnect ist bestrebt sämtlichen Mitarbeitern und / oder Dritten, welche die IT-Systeme, respektive die vorhandene Infrastruktur, nutzen, die Wahrung des Datenschutzes und der Datensicherheit zu gewährleisten. Hierfür hat die Interconnect diverse interne Richtlinien erstellt. Jeder Nutzer hat die Kenntnis der geltenden Bestimmungen mindestens einmal jährlich zu bestätigen.

Derzeit existieren die nachfolgenden Bestimmungen:

- Notfallkonzept
- IT-Benutzerrichtlinie der Interconnect GmbH & Co. KG

11. Schulungen und Zusammenarbeit

Alle Mitarbeiter werden in regelmäßigen Abständen über die Einhaltung der Grundsätze des Datenschutzes und der Datensicherheit belehrt. Der Inhalt, die Ziele, die Teilnehmer und die Termine werden zwischen dem Datenschutzbeauftragten und der Geschäftsleitung von der Interconnect abgestimmt.

Die Schulungsmaßnahmen werden fortlaufend durchgeführt, mindestens einmal pro Kalenderjahr wird jeder Mitarbeiter einer Schulung zugeführt.

Die Interconnect unterstützt den Datenschutzbeauftragten und stellt insbesondere alle zur Erbringung der Leistungen erforderlichen Informationen, und soweit dies zur Erfüllung der Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung.

Es ist gewährleistet, dass sich Betroffene jederzeit an den Datenschutzbeauftragten wenden können. Alle Mitarbeiter wurden/werden schriftlich im Sinne der EU-DSGVO und dem BDSG zum Datenschutz-Geheimnis verpflichtet und mindestens jährlich persönlich unterwiesen. Die Mitarbeiter melden jede Auffälligkeit im Bereich Datenschutz und IT-Sicherheit an den Datenschutzbeauftragten und/oder die Geschäftsführung.

12. Externe Dienstleister

Die Interconnect bedient sich zu ihrer Aufgabenerfüllung auch externer Dienstleister. Da wesentliche Vorgänge der Datenverarbeitung, der IT-Infrastruktur sowie spezieller kundenspezifischer Anwendungen hiervon betroffen sind, werden mit den Dienstleistern vertragliche Regelungen schriftlich festgehalten.

Die Interconnect verpflichtet alle externen Dienstleistungserbringer zur Wahrung des Datengeheimnisses und der Vertraulichkeit. Im Gegensatz zur Funktionsübertragung werden bei einer Auftragsverarbeitung Datenerhebung, -verarbeitung oder -nutzung für die Erfüllung der Aufgaben und Geschäftszwecke der verantwortlichen Stelle ausgelagert. Der Auftragnehmer hat dementsprechend eine Hilfsfunktion, er leistet dem Auftraggeber in einer oder mehreren Phasen der Datenerhebung, -verarbeitung oder -nutzung sowie eine weisungsgebundene Unterstützung. Er übernimmt keine Aufgabe in ihrer Vollständigkeit, sondern lediglich ihre technische Ausführung. Sofern eine Auftragsverarbeitung vorliegt, schließen die Parteien eine gesonderte Vereinbarung nach Art. 28 EU-DSGVO.

Die Interconnect setzt derzeit im Zusammenhang mit der Datenverarbeitung Dienstleistungsunternehmen ein, die im verbundenen Dokument „Liste der Auftragnehmer“ fortlaufend aktualisiert geführt werden.

13. Vertragliche Mindestanforderungen

Die Interconnect erklärt, dass auch in sonstigen Vertragsverhältnissen mit Dritten, die Zugriff auf personenbezogene Daten ermöglichen können, vertragliche Mindestanforderungen

eingehalten werden. Hierzu werden mit den Dritten entsprechende Geheimhaltungsvereinbarungen vereinbart.

Sofern die Interconnect zudem als Auftragsverarbeiter im Sinne von Art. 28 EU-DSGVO tätig wird, ist eine entsprechende vertragliche Vereinbarung mit der Interconnect abzuschließen.

14. Mitgeltende Unterlagen / verbundene Dokumente

Folgende Dokumente sind ergänzend zu diesem Datenschutzkonzept für die Abbildung datenschutzrechtlicher Anforderungen zu betrachten:

(1) Bestellungsurkunde Datenschutzbeauftragter
(2) Datenschutzerklärung
(3) Verpflichtungserklärung auf den Datenschutz der Mitarbeiter
(4) Vorlage Auftragsverarbeitung nach Art. 28 EU-DSGVO der Dienstleister
(5) „TOM“ = technische und organisatorische Maßnahmen
(6) Liste der Auftragnehmer
(7) IT-Sicherheitskonzept
(8) Notfallkonzept
(9) IT-Benutzerrichtlinie der Interconnect GmbH & Co. KG
(10) Inventarisierung aller Applikationen und Systeme
(11) Verzeichnisse von Verarbeitungstätigkeiten

Hinweis: Nicht alle Dokumente werden aus Sicherheitsgründen zur Verfügung gestellt, können aber auf Anfrage eingesehen werden.

15. Abschließende Anmerkungen

Alle notwendigen Maßnahmen werden getroffen im Rahmen der Angemessenheit der erforderlichen Maßnahme. Sollten Maßnahmen aus dem vorliegenden Dokument nicht oder nicht ausreichend detailliert hervorgehen, möge der Partner des Mandanten bitte schriftlich an diesen herantreten zur Klärung.

Dr. Ralf W. Schadowski
Externer Datenschutzbeauftragter

ISO/IEC 17024 zertifizierter / überwachter europäischer Datenschutzbeauftragter
ISO/IEC 27001 zertifizierter Lead Auditor (PECB), anerkannter Auditor IT-Sicherheit
ISO/IEC 27701 zertifizierter Lead Implementer (PECB), Aufbau Datenschutz-Managementsysteme
Fachgruppenleiter für Datenschutz und Vorstand im Bundesfachverband der IT-Sachverständigen BISG e.V.
Mitglied in der Gesellschaft für Datenschutz und Datensicherheit GDD e.V.

Datenschutzbeauftragter der InterConnect GmbH & Co. KG

Stand: 06.10.2020

16. Kontakt bei Rückfragen zum Datenschutz-Konzept

Der Datenschutzbeauftragte

InterConnect GmbH & Co. KG

Am Fächerbad 3

76131 Karlsruhe

E-MAIL: Datenschutz@interconnect.de

Anlage 1 - Abkürzungsverzeichnis

Abs	Absatz
AIS	Arzt-Informations-System
AMIS	Arzneimittelinformationssystem
AMTS	Arzneimitteltherapiesicherheit
Art	Artikel
Artt	Artikel (Mehrzahl)
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
DB	Datenbank
DBMS	Datenbankmanagementsystem
DIN	Deutsche Institut für Normung e. V.
DMS	Dokumentenmanagementsystem
DSG	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
EDV	Elektronische Datenverarbeitung
EFA	Elektronische Fallakte
EGA	Elektronische Gesundheitsakte
EPA	Elektronische Patientenakte
EU	Europäische Union
GDSG	Gesundheitsdatenschutzgesetz
GG	Grundgesetz
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.
HIS	Hospital Information System
HW	Hardware
IS	Informationssystem

ISO	International Organization for Standardization
IT	Informationstechnik, informationstechnisches…
Kap	Kapitel
KAS	Klinisches Arbeitsplatzsystem
KIS	Krankenhaus-Informationssystem
KMU	Kleines, mittelständisches Unternehmen
LDSG	Landesdatenschutzgesetz
LIS	Labor-Informationssystem
lit	littera (lat. „Buchstabe“)
MBO-Ä	(Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte
NRW	Nordrhein-Westfalen
OH KIS	Orientierungshilfe Krankenhausinformationssysteme
PACS	Picture Archiving and Communication System
PDMS	Patientendatenmanagementsystem
RIS	Radiologisches Informationssystem
RZ	Rechenzentrum
SDM	Standard-Datenschutzmodell
SGB	Sozialgesetzbuch
SW	Software
TK	Telekommunikation(s-)

Anlage 2 - Risiken mit Beispielen

Risiken	Erläuterung	Beispiele
Unbefugte Offenlegung von personenbezogenen Daten	Beabsichtigte/Unbeabsichtigte Veröffentlichung/Offenbarung von personenbezogenen Daten durch Beschäftigte/Auftragsverarbeiter gegenüber unbefugten Dritten	Lesen von Kundendaten oder Mitarbeiterdaten auf PC-Bildschirm durch ungeschützte Technik/offene Akte
Unbefugter Zugang zu personenbezogenen Daten	Beabsichtigte unbefugte Kenntnisnahme personenbezogener Daten durch aktive Benutzung von IT-Systemen oder Papierdateien durch Beschäftigte, Auftragsverarbeiter, unbefugte Dritte	Lesen von Beschäftigtendaten durch aktive Entnahme einer Personalakte oder Einloggen über falsches Passwort im IT-System
Veränderung personenbezogener Daten	Beabsichtigtes/Unbeabsichtigtes Verändern personenbezogener Daten durch Beschäftigte, Auftragsverarbeiter, unbefugte Dritte, IT-Technik	Fehlerhafte Eingabe von Daten beim Abschreiben vom Papierdokument; verbesserndes Fälschen von Zeugnissen zur Übergabe an Arbeitgeber
Verlust personenbezogener Daten	Beabsichtigtes/Unbeabsichtigtes Wegkommen personenbezogener Daten durch Beschäftigte, Auftragsverarbeiter, unbefugte Dritte	Smartphone verlieren, USB-Stick mit personenbezogenen Daten, Papierakten unauffindbar; Diebstahl
Vernichtung personenbezogener Daten	Beabsichtigte/Unbeabsichtigte oder unrechtmäßige Zerstörung personenbezogener Daten durch Beschäftigte, Auftragsverarbeiter, unbefugte Dritte und/oder IT- und technische Probleme, Elementarschäden	Archivbrand mit Zerstörung personenbezogener Daten in Papierdokumenten, Wasserschaden Smartphone
Diskriminierung, Stigmatisierung	Benachteiligung durch vordefinierte Prozessabläufe	durch Algorithmen, intransparentes Zustandekommen von Entscheidungen eines Betroffenen
Identitätsdiebstahl/-betrug	Gefahr, dass persönliche Identitätsinformationen durch Dritte missbraucht werden können	Erschleichen und Benutzen fremder Zugangsdaten zu IT-Systemen

Rufschädigung	Verbreitung vertraulicher Informationen, die den Ruf einer Person nachhaltig beeinträchtigen können	Nichteinhaltung der Vertraulichkeitsverpflichtung
Finanzieller Verlust	Datenmissbrauch führt zu negativen finanziellen Folgen	Daten werden an Auskunftei preisgegeben, die zur Reduzierung der Kreditwürdigkeit der betroffenen Person führen
Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten	Vertrauliche Daten werden durch Übertragungsfehler, fehlerhafter Übermittlung, etc. Dritten zugänglich gemacht	Faxirrläufer, telefonische Weitergabe sensibler Daten (gem. Art. 9 Abs. 1 DSGVO); Nichteinhaltung der Schweigepflicht
Unbefugte Aufhebung Pseudonymisierung	Pseudonymisierung kann eine wirksame Maßnahme darstellen, um dafür zu sorgen, dass ein Zugang zur Identität von Betroffenen nur einem begrenzten Nutzerkreis möglich ist.	Daten Betroffener werden fehlerhaft dechiffriert und Dritten zugänglich gemacht
Anderer erheblicher wirtschaftlicher oder gesellschaftlicher Nachteil	Ansehensverlust mit möglichen finanziellen Folgen	Enttäuschung von Vertraulichkeitserwartungen, Nachfragerückgang nach Imageschaden