Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO als Anlage zu einem oder mehreren von dem Auftraggeber genutztem Vertrag oder Verträgen

Zwischen der Firma

1&1 Internet SE

Elgendorfer Straße 57

56410 Montabaur

Deutschland

– Nachfolgend „**Auftragnehmer**“ genannt –

und

Firma: Diabetes-Schwerpunktpraxis Wiesbaden-Schierstein

Name: Andrea Wenz

Straße, Hausnummer: Heinrich-Zille-Str. 25

Postleitzahl, Ort: 65201 Wiesbaden

Land: DEUTSCHLAND

Kundennummer: 469993860

– Nachfolgend „**Auftraggeber**“ genannt –

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Einzelvertrag (nachstehend „Vertrag“) in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers, oder durch den Auftragnehmer Beauftragte personenbezogene Daten (nachstehend „Daten“) des Auftraggebers verarbeiten.

Diese Anlage ist nur gültig in Verbindung mit einem aktiven Vertrag über die folgenden Produkte:

Server

Cloud Server, Virtual Server Cloud, Managed Cloud Hosting, Dedicated Server (& Managed), Bare Metal Server, Dynamic Cloud Server, Virtual Server (Lin/Win), Container Cluster

Webhosting & Homepage

Webhosting, WordPress Hosting, MyWebsite, E-Shop, ipayment

Office & Online Marketing

Online-Buchhaltung, E-Mail Marketing

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Gegenstand dieser Anlage ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Als Hosting Dienstleister und Administrator von Server-Systemen kann auf Seiten des Auftragnehmers ein Zugriff auf personenbezogene Daten allerdings nicht ausgeschlossen werden.

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ i.S.v. Art. 4 Nr.7 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form, oder in einem elektronischen Format („Textform“) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt, oder ersetzt werden („Einzelweisung“).

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne von Art. 28 Abs. 3 lit.

a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Die Durchführung von rechtswidrigen Weisungen darf der Auftragnehmer ablehnen.

(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 der Datenschutzgrundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

(3) Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen.

(4) Die Beschreibung Technischer und Organisatorischen Maßnahmen gemäß Anhang 1 ist Bestandteil dieser Vereinbarung.

Der Auftragnehmer wird die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit durch Bereitstellung eines Zertifikates zu Datenschutz und Informationssicherheit nachweisen.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

Der Auftragnehmer unterstützt soweit erforderlich den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gemäß Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten.

(5) Der Auftragnehmer stellt sicher, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner stellt der Auftragnehmer sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben, oder einer angemessenen gesetzlichen Schweigepflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrags fort.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

(7) Für alle im Rahmen dieser Anlage anfallenden Datenschutzfragen ist der Ansprechpartner:
1&1 Internet SE
Der Datenschutzbeauftragte
Elgendorfer Str. 57
56410 Montabaur
datenschutz@1und1.de

(8) Der Auftragnehmer stellt sicher, seinen Pflichten nach Art. 32 Abs.1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(9) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Lösung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(10) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

(11) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglich¬keiten zu unterstützen.

§ 4 Pflichten des Auftraggebers

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

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt § 3 Abs. 11 dieser Anlage entsprechend.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung, oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet bei Erfüllung seiner Pflichten nicht dafür, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig, oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

(1) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs nach Anmeldung und unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(2) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 1 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Drittstaatentransfer

(1) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet überwiegend in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Ausnahmen sind der Liste gem. §8 Abs. 2 dieser Anlage zu entnehmen.

§ 8 Subunternehmer (weitere Auftragsverarbeiter)

(1) Mit der Hinzuziehung von verbundenen und fremden Unternehmen zur Wartung, Pflege der Rechenzentrumsstruktur, Telekommunikationsdienstleistungen und Benutzerservice durch den Auftragnehmer ist der Auftraggeber einverstanden.

(2) Eine Liste der aktuell eingesetzten Unterauftragnehmer steht dem Auftraggeber im Kundenportal stets zum Abruf zur Verfügung. Diese Liste wird quartalsweise aktualisiert.

(3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Die volle Verantwortung für die vom Auftragnehmer eingeschalteten Subunternehmer bleibt beim Auftragnehmer.

§ 9 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 drüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der DS-GVO liegen.

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

(3) Es gilt deutsches Recht.

(4) Diese Anlage ersetzt alle vorangegangenen Vereinbarungen dieser Art

§ 10 Haftung und Schadensersatz

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

Dieser Vertrag wird elektronisch geschlossen und ist ohne Unterschrift gültig

Anlagenverzeichnis

Anhang 1: Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen nach Art.32 DSGVO

1. Zutrittskontrolle

Mit der Zutrittskontrolle soll verhindert werden, dass unberechtigte Personen Zutritt zu den informationsverarbeitenden Systemen der 1&1 Internet SE bekommen. Die Rechenzentren der 1&1 Internet SE gewährleisten einen hohen Schutz durch moderne Sicherheitstechnik und umfassende Objekt- und Datenschutzmaßnahmen. Der Zutritt zum Rechenzentrum ist dabei nur einem eingeschränkten Kreis von autorisierten Mitarbeitern möglich.

1.1. Organisatorische Maßnahmen

1.1.1. Empfang- und Ausweispflicht

Der Standort des Rechenzentrumgebäudes wird tagsüber zu den normalen Geschäftszeiten durch einen Pförtner überwacht, außerhalb der Geschäftszeiten durch einen Sicherheitsdienst. Auffälligkeiten werden durch die Einbruchmeldeanlage und Kontrollgänge des Sicherheitsdienstes entdeckt. Am Standort des Rechenzentrums besteht für alle Besucher und externen Mitarbeiter die Pflicht, Ausweise zu tragen. Externe Personen dürfen sich grundsätzlich nur in Begleitung eines internen Mitarbeiters innerhalb der Gebäude aufhalten. Interne Mitarbeiter besitzen durch ihre Zutrittskarten die entsprechende Berechtigung, Zutritt zu den Geschäftsräumen zu erlangen.

Die Ausweis-Richtlinie sieht folgende Anforderungen beim Ausstellen vor:

- Die Ausweise, das Ausweis-Logbuch, sowie alle zugehörigen Dokumente und Unterlagen sind verschlossen aufzubewahren.
- Zugänge zu EDV-gestützten Verwaltungstools sind mit Passwörtern zu versehen, sodass unbefugte keinen Zugriff auf die Arbeitsstationen, über die die Ausweise verwaltet werden, erhalten können.
- Ausweise sind so zu gestalten, dass deren Gültigkeit abläuft.
- Ein Ausweisbuch über Ausgabe und Rücknahme der Ausweise ist in Papierform zu führen.
- Die Einträge des Ausweisbuches sind mindestens 6 Monate aufzubewahren.
- Jeweils ein „Besuch“ soll auf einem Blatt vermerkt werden, sodass verschiedene Besucher, wenn sie nicht an einem Besuch teilgenommen haben, nicht über andere Besucher Kenntnis erlangen können.

1.1.2. Schlüsselvergabe

Durch das installierte Zutrittskontrollsystem können nur Personen in das Rechenzentrum gelangen, die im Vorfeld Berechtigungen im Rahmen ihrer Aufgabenerfüllung (z.B. Systemoperatoren, die Hardware austauschen müssen) erhalten haben. Die Zutrittsberechtigungen werden zentral über ein Zugriffsrechtemanagement, d.h. durch die Einrichtung von Profilen, Vergabe/Sperrung von Berechtigungen eingerichtet. Hierfür existiert ein formaler Genehmigungsprozess. Der Zutritt zum Rechenzentrum erfolgt über eine neutrale

Zutrittskarte, die nach Anforderung und Unterschrift des Empfängers dem Berechtigten ausgehändigt wird. Die Vergabe der Zutrittskarten wird dokumentiert. Bei Verlust der Zutrittskarte wird diese sofort über das installierte Verwaltungssystem gesperrt. Die Berechtigungen können losgelöst von der physischen Verfügbarkeit der Zutrittskarte geändert, gelöscht, oder gesperrt werden.

1.2. Technische Maßnahmen

Das Rechenzentrum wird durch folgende technische Maßnahmen vor unberechtigtem Zutritt geschützt:

- ZK-System (Zutrittskontrollsystem)
- EMA (Einbruchmeldeanlage) mit VdS1- Zulassung
- Videokameras
- Sicherheitstüren
- Bereichswechselkontrolle

Ein wichtiger Bestandteil des Sicherheitskonzeptes ist der Zutritt zum zentralen Rechenzentrum über eine Personalvereinzelungsanlage.

1.2.1. Türsicherung

Eine Sicherheitsschleuse gewährleistet, dass nur einzelne berechtigte Personen das Rechenzentrum betreten können. Um die Sicherheitsschleuse betreten zu können, wird ein elektronischer Schlüssel (so genannter ID-Informationsträger) und eine PIN benötigt, der für den Zugang explizit freigeschaltet sein muss. Nur nach positiver Prüfung der Sicherheitsmerkmale wird der Zutritt zum Rechenzentrum durch die Sicherheitsschleuse gewährt.

1.2.2. Zutrittskontrollsystem und Überwachung

Der Standort des Rechenzentrums verfügt über Zugangsleser an allen Außentüren, sowie Leser an den Schrankenanlagen. Alle Außenzugänge, Etagentüren, sowie Bürobereiche sind mit digitalen Schließzylindern ausgerüstet. Alle Zugänge zum Rechenzentrum sind Videoüberwacht, die durch eine zentrale Videoüberwachungsanlage gesteuert wird. Die Aufzeichnungen werden über einen Zeitraum von 6 Monaten gespeichert. Die Fluchtwegtüren am Standort des Rechenzentrums sind zusätzlich mit einer Fluchttürsteuerung ausgerüstet, die nach Vorgaben des VdS geplant und zertifiziert, sowie regelmäßig gewartet wird.

2. Zugangskontrolle

Mit der Zugangskontrolle soll ein Eindringen unberechtigter Personen in die Informationsverarbeitenden Systeme der 1&1 Internet SE verhindert werden. Hierzu sind technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung implementiert.

2.1. Organisatorische Maßnahmen

2.1.1. Benutzer- und Berechtigungsverfahren

Benutzer, die im Rahmen ihrer Aufgabenerfüllung zu einem System Rechte erlangen sollen, müssen diese Berechtigungen über einen formalen Benutzer- und Berechtigungsprozess beantragen. Die Anforderungen zur Benutzer- und Berechtigungsvergabe sind durch die interne Sicherheitsrichtlinie zum Identity- und Accessmanagement beschrieben und die Berechtigungsvergabe in einer Verfahrensanweisung dokumentiert. Im Benutzer- und Berechtigungs-Verwaltungssystem werden die Benutzerkennungen und Berechtigungen von Benutzern geführt. Technisch erfolgt die Genehmigung für das Erteilen und Löschen von Zugriffsrechten über Ticketsysteme, in denen der Vorgang dokumentiert wird. Im Verwaltungssystem werden Berechtigungen von Benutzern gesperrt, sobald der Benutzer das Unternehmen verlässt, bzw. wenn die Berechtigungen nicht mehr benötigt oder unberechtigt benutzt werden. Auch im Rahmen der Systemdiagnose werden obsolete Zugriffsrechte gelöscht. Technisch ist jeder berechtigte Benutzer auf eine einzelne Benutzer-ID auf dem Zielsystem beschränkt

2.2. Technische Maßnahmen

2.2.1. Authentisierungsverfahren

Zugangsberechtigungen sind so feingranular wie möglich konfiguriert, sodass Personen nur dort Zugang haben, wo sie diesen auf Grund ihrer Funktion und ihrer Aufgabenerfüllung benötigen. Die Zugangskontrollverfahren gelten für alle Mitarbeiter der 1&1 Internet SE. Alle Systeme sind durch zweistufige Authentifizierungsverfahren (z.B. Benutzer-ID und Passwort) geschützt, die unberechtigte Zugriffe unterbinden. Werden im Rahmen des Authentifizierungsverfahrens Passwörter eingesetzt, müssen diese den internen Passwortrichtlinien für Mitarbeiter und Systeme entsprechen. Passwörter, die nach den Richtlinien nicht der Qualität entsprechen, sind nicht erlaubt. Die Systeme werden nach einer bestimmten Zeit der Inaktivität automatisch gesperrt. Zusätzlich werden Accounts automatisch deaktiviert, wenn deren Passwörter nicht geändert werden.

Ein Fernzugriff auf interne Systeme ist nur in authentifizierter Form möglich, bei dem z.B. asymmetrische Authentisierungsverfahren (Public-/Private-Key-Verfahren) eingesetzt werden, die zusätzlich zur Nachweisbarkeit protokolliert werden. Der Zugriff auf interne Systeme wird nur Geräten gewährt, die sich im Besitz der 1&1 Internet SE befinden und administriert werden. Der Zugriff auf interne Systeme über WLAN-Verbindungen kann nur durch einen zusätzlichen VPN-Tunnel erfolgen. Die von der 1&1 Internet SE betriebenen WLAN-Zugangsgeräte erkennen und protokollieren nicht autorisierte Access-Points.

2.2.2. Verschlüsselung

Daten mit hohen Schutzbedarfen werden nach aktuellem Stand der Technik mit verschlüsselten Verfahren analog der internen IT-Sicherheitsrichtlinie zur Kryptographie gesichert. Die eingesetzten Verschlüsselungsverfahren basieren auf Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI). Werden Daten anhand Datenträger ausgetauscht, wird dokumentiert, wer zu welchem Zeitpunkt zu welchem Zweck von wem einen Datenträger erhält. Datenträger, die nicht mehr zum produktiven Einsatz kommen, werden durch sichere

Lösch- und Überschreib-Verfahren nach Empfehlungen des BSI entsorgt. Es gelten hier die Regelungen der internen Sicherheitsrichtlinie zur Entsorgung von Medien.

3. Zugriffskontrolle

Mit der Zugriffskontrolle sollen unerlaubte Handlungen in den informationsverarbeitenden Systemen der 1&1 Internet SE verhindert werden, indem Maßnahmen zur Überwachung und Protokollierung der Zugriffe implementiert werden.

3.1. Berechtigungsvergabe

Die Systeme wurden in der Weise konfiguriert, dass ein regulärer Zugriff mit administrativen Rechten nur für interne, autorisierte Mitarbeiter aus gesicherten Netzsegmenten möglich ist. Hier wurden bedarfsorientierte Berechtigungskonzepte ausgestaltet, die die Zugriffsrechte, sowie deren Überwachung und Protokollierung definieren. Eine Berechtigungsvergabe wird stets nach dem Need-to-know-Prinzip vergeben. Je nach Autorisierung werden differenzierte Berechtigungen, untergliedert nach Rollen und Profilen von Benutzern eingerichtet. Weitere Autorisierungen an Systemen bedürfen der Einrichtung von Berechtigungen nach dem implementierten Benutzer-und Berechtigungsprozess.

3.2. Auswertungen

Zugriffe auf System-IDs und auffällige Zugriffsversuche werden auf einem zentralen Protokollierungsserver protokolliert. Der Zugriff auf die Protokollierungsserver ist nur lesend durch autorisierte Administratoren möglich. Beim auffälligen Zugriffsversuch wird zusätzlich eine Alarmierung (Security Monitoring) an den zuständigen Systemverantwortlichen ausgelöst.

3.3. Veränderungen

Modifikationen an Zugriffsrechten können lediglich von Systemadministratoren des operativen Fachbereichs vorgenommen werden, die die Freigabe des Vorgesetzten erhalten haben. Veränderungen der Zugriffsrechte und Berechtigungen geschehen in der Regel innerhalb eines Arbeitstages, wenn nicht sogar bei Bedarf sofort. Netzwerkgeräte oder Systeme mit voreingestellten Zugriffsmöglichkeiten dürfen nicht im Produktivbereich verwendet werden. Näheres regeln die internen Sicherheitsrichtlinien.

3.4. Löschung

Das Löschen von Benutzerberechtigungen (z.B. Nach dem Austritt eines Mitarbeiters) erfolgt zeitnah, spätestens jedoch innerhalb eines Arbeitstages. Das Löschen von Zugriffsrechten geschieht auch im Rahmen der Systemdiagnose. Hier werden obsolete Zugriffsrechte bereinigt. Im Verwaltungssystem werden Berechtigungen von Benutzern gesperrt, sobald der Benutzer das Unternehmen verlässt bzw. wenn die Berechtigungen nicht mehr benötigt oder unberechtigt benutzt werden. Im Rahmen der Systemdiagnose werden obsolete Zugriffsrechte, die z.B. über einen längeren Zeitraum inaktiv waren, gelöscht.

4. Weitergabekontrolle

Im Rahmen der Weitergabekontrolle werden Maßnahmen beim Transport, der Übertragung und Übermittlung, sowie bei der nachträglichen Überprüfung von personenbezogenen Daten definiert.

4.1. Organisatorische Maßnahmen

4.1.1. Schulungsmaßnahmen

Alle Mitarbeiter der 1&1 Internet SE sind auf das Datengeheimnis gem. § 5 BDSG hin verpflichtet worden. Neue Mitarbeiter erhalten bei Eintritt eine Sicherheitsschulung. Für verschiedene Fachbereiche gibt es speziell abgestimmte Sicherheitssensibilisierungsprogramme.

4.1.2. Klassifizierung der Informationen

Jede Information muss nach ihrem Schutzbedarf eingestuft werden. Handelt es sich um vertrauliche Informationen, müssen diese besonders behandelt werden. Vertrauliche, dienstliche Informationen dürfen nur über sichere Kommunikationswege übertragen werden. Der Umgang mit Informationen wurde in der Richtlinie „Datenklassifikation“ und deren Anhang geregelt. Es sind insbesondere folgende Regeln einzuhalten:

- Es müssen spezielle Verfahren und Regelungen zum Schutz der Informationen und Datenträger beim Transport insbesondere über Unternehmensgrenzen hinweg definiert und dokumentiert werden (z.B. Verfahrensanweisung für den Einsatz von Boten).
- Es müssen so weit wie möglich kryptographische Verfahren (z-B. Verschlüsselung bei der Übertragung vertraulicher Daten) eingesetzt werden. Die Anforderungen aus der IT-Sicherheitsrichtlinie Kryptographie sind zu berücksichtigen.
- Bei der Übergabe an externe Empfänger ist die erfolgte vollständige und sichere Übergabe nachweisbar zu dokumentieren.

4.2. Technische Maßnahmen

4.2.1. Zugriffs-und Transportsicherung

Grundsätzlich können auf die Systeme, die personenbezogene Daten verarbeiten, nur autorisierte Nutzer zugreifen. Die Übertragung von Daten erfolgt ausschließlich durch das System selbst an autorisierte Empfänger, über kryptographisch stark gesicherte Wege, z.B. über VPN mit IPSec nach aktuellem Stand der Technik und Empfehlungen des BSIs. Die Übertragung wird in Logfiles protokolliert.

Um das System vor unberechtigten Zugriffen von Desktop-PCs der Mitarbeiter und somit vor einer unautorisierten Weitergabe von Daten zu schützen, gelten die internen Sicherheitsrichtlinien für Mitarbeiter der 1&1 Internet SE.

Die Integrität von wichtigen Systemdateien wird durch regelmäßige Überprüfung deren kryptografischer Prüfsumme sichergestellt (HIDS).

Der Zugriffsschutz auf Systeme mit sensiblen Informationen wird auf mehreren Ebenen realisiert: Auf Dateisystem-, auf Betriebssystem- und auf Netzwerkebene. Die Schutzmechanismen erlauben nur speziell autorisierten Administratoren den Zugriff auf die jeweilige Ebene. Um Datenverlust vorzubeugen, müssen alle arbeitsrelevanten Daten auf Servern gespeichert werden.

Diese Daten werden regelmäßig gemäß den definierten Backup-Konzepten gesichert, sodass ein Datenverlust dadurch weitestgehend ausgeschlossen ist.

4.2.2. Protokollierung

Der Zugriff und die Aktivitäten der Administratoren werden in speziellen Protokolldateien aufgezeichnet. Die Protokollierung der Zugriffe erfolgt auf einen zentralen, dedizierten Protokollierungsserver, der von den zu protokollierenden Systemen getrennt installiert ist. Der Zugriff auf die Protokolle und auf den zentralen Protokollierungsserver ist geschützt und nur autorisierten Administratoren gestattet. Systemadministratoren dürfen dabei die Protokolle auf den Protokollierungsserver einsehen, aber nicht verändern. Der Transport der Protokollierungsdaten geschieht über eine verschlüsselte Verbindung. Auf den Protokollierungsserver werden verschiedene Verletzungen von Sicherheitskontrollen protokolliert, wie z.B. nicht berechtigte Zugangsversuche oder signifikante Schutzverletzungen. Bei besonders sensiblen Systemen ist der Zugriff nur nach dem 4-Augen-Prinzip möglich.

5. Eingabekontrolle

Um die Nachvollziehbarkeit und Dokumentation der Datenverwaltung und –pflege sicherzustellen, werden Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder gelöscht worden sind, implementiert.

5.1. Protokollierungs- und Protokollauswertung

Durch die Einhaltung der oben aufgeführten Regeln zu Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle wurde die Grundlage für die Eingabekontrolle der Systeme geschaffen, die personenbezogenen Daten verarbeiten. Grundsätzlich wird im Rechte- und Rollen-Konzept zwischen Systemusern, Prozessusern und personalisierten Usern unterschieden.

Angaben zur Protokollierung sind in Kapitel 4.2.2 zu finden.

Protokollauswertungen werden stichprobenartig von den Systemadministratoren vorgenommen, insbesondere jedoch, wenn Auffälligkeiten oder der Verdacht auf eine Kompromittierung (z.B. durch eine Alarmierung / Triggering eines Events) aufgetreten ist. Die Protokollauswertungen sind als Informationen klassifiziert, die nur innerhalb der 1&1 Internet SE im Rahmen der Aufrechterhaltung und Sicherstellung der Systemstabilität und –sicherheit zu verwenden sind.

6. Auftragskontrolle

Alle Weisungen des Auftraggebers zum Umgang mit personenbezogenen Daten werden dokumentiert und an zentraler Stelle für die mit der Datenverarbeitung befassten Mitarbeiter der 1&1 Internet SE hinterlegt.

Die 1&1 Internet SE verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung erfolgt nur nach schriftlicher Einwilligung des Auftraggebers. Der Datenschutzbeauftragte des Auftraggebers hat das jederzeitige Recht, nach Absprache die Umsetzung seiner Weisungen bei

der 1&1 Internet SE zu kontrollieren. Die 1&1 Internet SE wird den Auftraggeber bei der Durchführung von Kontrollen durch den Auftraggeber unterstützen und an der vollständigen Abwicklung der Kontrolle mitwirken.

Die 1&1 Internet SE wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach ihrer Auffassung gegen gesetzliche Regelungen verstößt, sowie dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist. Die 1&1 Internet SE ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne des § 5 BDSG verpflichtet. Sie verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien werden erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet.

7. Verfügbarkeitskontrolle

Alle Dienste der gesamten 1&1 Internet SE und ihrer Tochterunternehmen sind hochsensibel in Bezug auf deren Verfügbarkeit und müssen vor zufälliger Zerstörung oder Verlust geschützt werden. Die Kunden erwarten eine hochverfügbare Bereitstellung aller Netzwerk- und Rechenzentrums-Dienstleistungen. In diesem Zusammenhang werden Maßnahmen zur Datensicherung und –erhaltung umgesetzt.

7.1. Organisatorische Maßnahmen

7.1.1. Notfallhandbücher und Backup-Verfahren

Zur Sicherstellung der Notfallhandbücher und Backup-Verfahren werden in den als für notwendig erachteten Abteilungen Notfallhandbücher erstellt. Die Notfallhandbücher definieren Verantwortlichkeiten (z.B. Notfallverantwortlicher), sowie Eskalations-, Informations- und Alarmierungspfade, legen Wiederanlaufpläne und Verfahren für einen Shutdown für einen Mangelfall fest, regeln Ersatzbeschaffung von Hard- und Software und dokumentieren, wie Daten gesichert und archiviert werden müssen. Die Notfallhandbücher sind damit ein wesentlicher Bestandteil für den Umgang und der Behandlung der Systeme und Daten im Notfall, die insbesondere auf die Backup-Strategien und Backup-Dokumentationen verweisen. Alle Daten werden in regelmäßigen Abständen gesichert, wobei die Sicherung dokumentiert an einem anderen Ort als das zu sichernde System verwahrt wird. Die Backups verlassen jedoch nicht das Rechenzentrum der 1&1 Internet SE. Zum Schutz der Archive und Backups sind die zuvor genannten Zutrittskontrollen implementiert. Der Zugang auf die Backup-Software ist limitiert auf dedizierte Backup-Administratoren. Die Häufigkeit von Datenbackups richtet sich nach der Kritikalität der Informationen und ist individuell anpassbar. Funktionalitätstests von Datenbackups werden stichprobenartig von den zuständigen Systemadministratoren vorgenommen. Die zum Backup benutzten Speichermedien werden nach einem sicheren Lösch- oder Überschreibungsverfahren nach Empfehlung des BSI wiederverwendet.

Im Wiederherstellungsprozess wird beschrieben, wie und in welcher Reihenfolge die Systeme und Daten installiert und wiederhergestellt werden müssen.

Alle Prozesse zur Wiederherstellung der Daten, der Wiederanlaufplan der Systeme, sowie die Notfallsituation müssen in regelmäßigen Abständen in einer Übung durchgeführt und getestet werden. Die Tests und Übungen werden protokolliert und dokumentiert. Die bei Notfällen und Incidents benötigten Eskalationspfade wurden im Praxisbetrieb erprobt.

7.2. Technische Maßnahmen

7.2.1. Firewall und Virenschutz

Die Netze und Systeme der 1&1 Internet SE sind mit einer Firewall gegen Hackerangriffe geschützt, die regelmäßig von autorisierten Systemadministratoren gewartet und aktualisiert werden. Die Firewall- Regeln sind so ausgelegt, dass nur benötigte Dienste erlaubt sind und in der Grundeinstellung jeden Netzwerkverkehr blockieren. Alle Internetverbindungen sind durch mindestens eine Firewall geschützt. Die Kontrolle sicherheitsrelevanter Konfigurationen erfolgt hierbei im Rahmen von Sicherheitsaudits und Penetrationstests, die u.a. von der internen Sicherheitsabteilung durchgeführt wird. Alle Netzwerkkomponenten werden einmal täglich, sowohl intern als auch extern, durch automatische Scanner geprüft.

Das Virenschutzkonzept sieht einen mehrstufigen Schutz vor Schadsoftware über die Netzwerk-Gateways und Systeme der 1&1 Internet SE vor. Der Schutz vor Schadsoftware wird zentral über ein Systemmanagementsystem verwaltet und regelmäßig, mindestens einmal am Tag, aktualisiert. Alle sensiblen und kritischen Systeme sind mit einem fehlertoleranten Festplattenverbund (i.d.R. RAID 5) ausgestattet.

7.2.2. Hochverfügbarkeit und Stromversorgung

Aus der Hochverfügbarkeitsanforderung ergibt sich am Standort Karlsruhe, an dem das System aufgestellt ist, eine grundsätzliche hochredundant ausgelegte Netzwerk-Infrastruktur, die Einzelfehler in fast allen Bereichen und Doppelfehler in vielen Bereichen abfangen kann. Sensible Dienste werden georedundant an verschiedenen Standorten betrieben. Die Stromversorgungen sind mehrfach unabhängig voneinander ausgelegt. Das Rechenzentrum ist mit einer unterbrechungsfreien Stromzufuhr ausgestattet. Die zentrale Elektrotechnik im Hauptrechenzentrum in Karlsruhe ist in vier (3+1) Blöcke aufgeteilt. In jedem Block ist die Technik Mittespannung, Niederspannung, USV und Netzersatzanlage (NEA) enthalten. Ein Betriebsblock dient zur Redundanz.

Die Versorgungsblöcke sind räumlich voneinander getrennt, um eine gegenseitige Beeinflussung im Schadens- oder Störfall zu verhindern. Jeder Block hat einen eigenen mittelspannungsseitigen Abgang. Das Rechenzentrum ist an einem 20 kV Ring der Stadtwerke Karlsruhe angeschlossen, der exklusiv dem Rechenzentrum vorbehalten ist. Um sich vor einem Totalausfall in der Versorgung durch die Stadtwerke zu schützen, ist in zweiter Instanz zwischen Verbraucher und Versorger eine redundant ausgelegte, unterbrechungsfreie Stromversorgung (USV) installiert. Die gesamte Anlage wird über eine zentrale, redundant aufgebaute Netzleittechnik überwacht und gesteuert. Zusätzlich wird permanent die Netzqualität nach DIN EN 50160 von allen Ein- und Ausgängen der USV Anlagen überwacht.

7.2.3. Brandschutz

Eine Argon-Löschanlage schützt die Sicherheitsräume im Brandfall. Das ungiftige Gas bewirkt bei einem Brandfall eine Sauerstoffverdrängung im Raum, wodurch dem Brandherd die

Grundlage Sauerstoff entzogen wird. Die Server werden durch den Löschvorgang nicht beeinträchtigt und können normal weiter betrieben werden.

Um einen Brandfall im Vorfeld zu verhindern ist des Weiteren eine Brandfrüherkennungsanlage installiert, die ständig die Luftpartikel anhand eines vorgegebenen Soll-Kalibrierungszeitraumes überwacht. Ändert sich die Zusammensetzung der Luftpartikel oder steigt die Zahl der für eine Brandentstehung typischen Partikel, schlägt die Früherkennung Alarm. Die Anlage ist direkt auf die Berufsfeuerwehr Karlsruhe aufgeschaltet. Die interne Alarmverfolgung erfolgt über eine Notifikationssteuerung, Email sowie SMS Versand, an das Facility Management der 1&1 Internet SE in Karlsruhe. Die Anlage wurde nach Vorgaben des VdS geplant und zertifiziert. In allen Haustechnik-, Technik-, Lagerräumen, Fluren und Treppenhäusern sind Brandmelder, an allen Zugangsbereichen sind Handmelder installiert. Die Gefahrenmeldeanlage wird nach Vorgaben des VdS regelmäßig gewartet. Zur ersten Bekämpfung von Bränden sind Handfeuerlöscher installiert.

8. Trennungskontrolle

Durch die 1&1 Internet SE getroffenen Maßnahmen zur Trennungskontrolle sind der softwareseitige Ausschluss im Sinne einer Mandantentrennung, die Trennung von Test- und Routineprogrammen, die Trennung durch getroffene Zugriffsregelungen, sowie Dateiseparierung.

Beispielsweise müssen alle Produktivsysteme getrennt von den Entwicklungs- und Testsystemen betrieben werden. Technisch wird das durch eine Segmentierung von Netzen mit einem aktivierten Firewall-Regelwerk realisiert. Produktivdaten dürfen nicht als Kopie für Testzwecke verwendet werden, ebenso dürfen Testdaten nicht in Produktivumgebung eingesetzt werden. Details regeln die internen Sicherheitsrichtlinien zum sicheren Betrieb.