Vereinbarung

(2. Fassung nach Prüfung durch das Landesamt)

zwischen der

Stadt Nürtingen, Marktstraße 7, 72622 Nürtingen

Projekt: Mörikeschule, Frickenhäuser Straße 2, 72622 Nürtingen

- nachstehend Auftraggeber genannt -

und

EDV Service Schaupp GmbH, Gänsäcker 25, 74321 Bietigheim-Bissingen

- nachstehend Auftragnehmer genannt –

gemäß § 11 BDSG zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

1. Gegenstand und Dauer des Auftrags

Es besteht ein Vertrag vom 03.07.2009 zwischen der Stadt Nürtingen und des Auftragnehmers zur Bereitstellung eines Systems zur Abrechnung der Essen in der Mensa der Mörikeschule Nürtingen. In diesem Vertrag ist der Gegenstand und die Dauer des Auftrages sowie die Pflichten des Auftragnehmers und dessen Vergütung im Einzelnen beschrieben.

2. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Aufgaben des Auftragnehmers:

Folgende Daten werden von zukünftigen Teilnehmern der Mensaverpflegung der Mörikeschule Nürtingen durch den Auftraggeber erhoben und erfasst: Name, Vorname, Geburtsdatum, Klasse, Status (Schüler, Lehrer, Sonstige ...), e-Mail.

Der Auftragnehmer weist den Kunden eine persönliche Buchungsnummer zu und errichtet ein virtuelles Konto.

Durch getätigte Überweisungen des o. g. Personenkreises auf das Treuhandkonto des Auftraggebers bei der KSK Esslingen-Nürtingen werden die jeweiligen Bankverbindungen des Kundenstammes dem Auftragnehmer bekannt. Der Auftragnehmer weist sowohl die Bankverbindung als auch die getätigten Überweisungen dem jeweiligen virtuellen Kundenkonto zu.

Dem Auftraggeber ist es ferner möglich, eine Komplettübersicht in das virtuelle Treuhandkonto zu erlangen.

Die Erhebung, Verarbeitung, Nutzung und Speicherung der genannten personenbezogenen Daten dienen dem Zweck, dass Schüler, Lehrer und sonstige Personen an einer bargeldlosen Mensaverköstigung in der Mörikeschule Nürtingen teilnehmen können.

3. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber auf Wunsch zur Prüfung zu übergeben.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen hinsichtlich der Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und der Trennungskontrolle.

Die getroffenen Maßnahmen sind in Anlage I detailliert beschrieben.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG dem Auftraggeber zur Verfügung zu stellen.

Nach § 3a BDSG soll auf den Grundsatz der Datensparsamkeit und Datenvermeidung geachtet werden.

4. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach § 11 Abs. 4 BDSG folgende Pflichten:

- ⇨ Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 4f, 4g BDSG ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- ⇨ Die Wahrung des Datengeheimnisses entsprechend § 5 BDSG. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.
- ⇨ Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage.
- ⇨ Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG beim Auftragnehmer ermittelt.
- ⇨ Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.
- ⇨ Der Auftragnehmer hat im Rahmen der Auftragskontrolle nach Nr. 6 der Anlage zu § 9 Satz 1 BDSG sicher zu stellen, dass personenbezogene Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.
- ⇨ Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

6. Unterauftragsverhältnisse

Soweit bei der Verarbeitung oder Nutzung und Speicherung personenbezogener Daten des Auftraggebers Unterauftragnehmer (aktuell bekannt: 1 & 1, Sitz in 56410 Montabaur und KRZN, Sitz in 47475 Kamp-Lintfort) einbezogen werden sollen, ist der Auftraggeber unverzüglich darüber schriftlich zu informieren. Unterauftragnehmer werden genehmigt, wenn folgende Voraussetzungen vorliegen:

- ⇨ Wenn der Auftragnehmer unter Wahrung seiner unter Punkt 5 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzt.
- ⇨ Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
- ⇨ Dem Auftraggeber werden dem/den Unterauftragnehmer/n gegenüber die gleichen Kontrollrechte (s. Punkt 5 dieser Vereinbarung) wie die dem Auftragnehmer gegenüber eingeräumt.

7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen, durch einen im Einzelfall zu benennenden Prüfer durchführen zu lassen und über alle im Rahmen des Auftragsverhältnisses obliegenden Verpflichtungen durch den Auftragnehmer Auskunft zu erhalten. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

Der Auftraggeber hat das Recht, sich über die Einhaltung der technischen und organisatorischen Maßnahmen gem. § 9 Satz 1 BDSG und der dazu gehörigen Anlage zu überzeugen.

Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und der Anlage nach. Dabei kann der

Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine unverzüglich Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz der im Rahmen dieses Auftrages verarbeiteten personenbezogenen Daten oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

Es ist bekannt, dass nach § 42a BDSG Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang der im Rahmen dieses Auftrages verarbeiteten personenbezogenen Daten. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach § 42a BDSG treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

9. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. § 11 Abs. 3 Satz 1 BDSG). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Nürtingen, 17.12.2012

Häfner, Stadt Nürtingen (Auftraggeber)

Bietigheim-Bissingen, 20.12.2012

Sohnle, ppa. EDV-Service Schaupp (Auftragnehmer)

Anlage I zur

Vereinbarung
zwischen der

Stadt Nürtingen, Marktstraße 7, 72622 Nürtingen

für die Mörikeschule

und

EDV Service Schaupp GmbH,
Gansäcker 25, 74321 Bietigheim-Bissingen

vom 17.12.2012 / 20.12.2012

In der Anlage sind die getroffenen technischen und organisatorischen Maßnahmen hinsichtlich der Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits- und Trennungskontrolle beschrieben. (s. Punkt 3)

Die Anlage I besteht einschließlich dieses Deckblattes aus 8 Seiten.

*Unsere Rechenzentren gewährleisten einen hohen Schutz durch moderne*Sicherheitstechnik und umfassende Objekt und Datenschutzmaßnahmen.

Zutrittskontrolle

Das Rechenzentrum wird durch folgende Maßnahmen vor unberechtigtem Zugang geschützt:
- ZK-System (Zutrittskontrollsystem)
- EMA (Einbruchmeldeanlage) mit VdS-Zulassung
- Video Kameras
- Sicherheitstüren
- Bereichswechselkontrolle

Ein wichtiger Bestandteil des Sicherheitskonzepts ist der Zugang zum Rechenzentrum über eine Personenvereinzelungsanlage.
Durch eine Sicherheitsschleuse wird gewährleistet, dass nur einzelne berechtigte Personen Zutritt zum Rechenzentrum erlangen. Um die Sicherheitsschleuse betreten zu können, wird ein elektronischer Schlüssel
(so genannter ID-Informationsträger) benötigt, der für den Zugang explizit freigeschaltet sein muss.
In der Schleuse werden bestimmte Sicherheitsmerkmale (u.a. Gewicht, Informationsträger, Aussehen der Person) überprüft. Nur nach positiver Prüfung der Sicherheitsmerkmale wird Zugang zum Rechenzentrum durch die Sicherheitsschleuse gewährt.

Zugangskontrolle

Zugangsberechtigungen sind so feingranular wie möglich konfiguriert, so dass Personen nur dort Zugang haben, wo sie diesen auf Grund ihrer Funktion benötigen. Alle Systeme sind mindestens durch Benutzer/Passwort geschützt, so dass auch bei physikalischem Kontakt zur Maschine erkennbare Handlungen unternommen werden müssen, um Zugriff auf das System zu bekommen (z.B. Neustarten des Systems in einen Zustand ohne Passwortschutz; dies würde von der Überwachung jedoch gemeldet bzw. aufgezeichnet werden).
Ein Fernzugriff ist nur in authentifizierter Form möglich, so dass Manipulationen bei einem erfolgreichen Login immer einem Mitarbeiter zugeordnet werden können. Die Mitarbeiter loggen sich durch ihre SSH-Keys oder Passwörter ein. Somit ist grundsätzlich gewährleistet, dass Änderungen zum Mitarbeiter zurück verfolgbar sind.

Zugriffskontrolle

Die Systeme sind so konfiguriert, dass ein regulärer Zugriff mit administrativen Rechten nur für firmeninterne Techniker aus gesicherten Netzsegmenten möglich ist. Der Zugriff geschieht über kryptographisch stark gesicherte (SSH, IPsec per X.509-Authentifizierung) Wege. Der Zugriff und die Aktivitäten der Administratoren werden in Logfiles aufgezeichnet.

Weitergabekontrolle

Vertrauliche dienstliche Informationen dürfen nur über sichere Kommunikationswege übertragen werden.
Grundsätzlich kann auf das System TGP*open* nur durch autorisierte Nutzer zugegriffen werden. Die Übertragung von Daten erfolgt ausschließlich durch das System selbst an autorisierte Empfänger, verschlüsselt und 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 Sicherheitsrichtlinien für Mitarbeiter der EDV der 1&1 Internet AG.
Selbstverständlich sind unsere Mitarbeiter auf das Datengeheimnis gem. § 5 BDSG hin verpflichtet worden.
Um Datenverlust vorzubeugen, müssen alle arbeitsrelevanten Daten auf Servern gespeichert werden. Diese werden regelmäßig gesichert. Ein Datenverlust ist dadurch weitestgehend ausgeschlossen.

Eingabekontrolle

Durch die Einhaltung der oben aufgeführten Regeln zu Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle wurde die Grundlage für die Eingabekontrolle für TGP*open* geschaffen. Regeln, die hierüber hinausgehen, werden in diesem Kapitel dokumentiert.
Grundsätzlich wird im Rechte- und Rollen-Konzept zwischen Systemusern, Prozessusern und personalisierten Usern unterschieden.

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 AG hinterlegt.
Der Datenschutzbeauftragte des Auftraggebers hat das jederzeitige Recht, die Umsetzung seiner Weisungen bei der 1&1 Internet AG zu kontrollieren.

Verfügbarkeitskontrolle

Alle Dienste der gesamten 1&1 und ihrer Töchter sind hochsensibel in Bezug auf deren Verfügbarkeit. Die Kunden erwarten eine hochverfügbare Bereitstellung aller Netzwerk- und RZ-Dienstleistungen.
Zur Sicherstellung dieser werden in den als für notwendig Erachteten Abteilungen Notfallhandbücher erstellt. Aus der Hochverfügbarkeitsanforderung ergibt sich am Standort Karlsruhe, an dem das System aufgestellt ist, eine grundsätzlich hochredundant ausgelegte Netzwerkinfrastruktur, die Einzelfehler in fast allen Bereichen und Doppelfehler in vielen Bereichen abfangen kann.
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 Brandfrüh-erkennungsanlage 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, so schlägt die Früherkennung Alarm.
Zur ersten Bekämpfung von Bränden sind Handfeuerlöscher installiert.
Die Zentrale Elektrotechnik im Hauptrechenzentrum in Karlsruhe ist in vier (3+1) Blöcke aufgeteilt. In jedem Block ist die Technik Mittelspannung, Niederspannung , USV und Netzersatzanlage (NEA) enthalten. Ein Betriebsblock dient als Redundanz. Im 2. Bauabschnitt ist vorgesehen, einen weiteren Betriebsblock (4+1) zu realisieren. 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 ange-schlossen, 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 an allen Ein- und Ausgängen der USV Anlagen überwacht. Unsere Rechenzentren gewährleisten einen hohen Schutz durch moderne Sicherheitstechnik und umfassende Objekt und Datenschutzmaßnahmen.

Zutrittskontrolle

Das Rechenzentrum wird durch folgende Maßnahmen vor unberechtigtem Zugang geschützt:
- ZK-System (Zutrittskontrollsystem)
- EMA (Einbruchmeldeanlage) mit VdS-Zulassung
- Video Kameras
- Sicherheitstüren
- Bereichswechselkontrolle

Ein wichtiger Bestandteil des Sicherheitskonzepts ist der Zugang zum Rechenzentrum über eine Personenvereinzelungsanlage.
Durch eine Sicherheitsschleuse wird gewährleistet, dass nur einzelne berechtigte Personen Zutritt zum Rechenzentrum erlangen. Um die Sicherheitsschleuse betreten zu können, wird ein elektronischer Schlüssel (so genannter ID-Informationsträger) benötigt, der für den Zugang explizit freigeschaltet sein muss.
In der Schleuse werden bestimmte Sicherheitsmerkmale (u.a. Gewicht, Informationsträger, Aussehen der Person) überprüft. Nur nach positiver Prüfung der Sicherheitsmerkmale wird Zugang zum Rechenzentrum durch die Sicherheitsschleuse gewährt.

Zugangskontrolle

Zugangsberechtigungen sind so feingranular wie möglich konfiguriert, so dass Personen nur dort Zugang haben, wo sie diesen auf Grund ihrer Funktion benötigen. Alle Systeme sind mindestens durch Benutzer/Passwort geschützt, so dass auch bei physikalischem Kontakt zur Maschine erkennbare Handlungen unternommen werden müssen, um Zugriff auf das System zu bekommen (z.B. Neustarten des Systems in einen Zustand ohne Passwortschutz; dies würde von der Überwachung jedoch gemeldet bzw. aufgezeichnet werden).
Ein Fernzugriff ist nur in authentifizierter Form möglich, so dass Manipulationen bei einem erfolgreichen Login immer einem Mitarbeiter zugeordnet werden können. Die Mitarbeiter loggen sich durch ihre SSH-Keys oder Passwörter ein. Somit ist grundsätzlich gewährleistet, dass Änderungen zum Mitarbeiter zurückverfolgbar sind.

Zugriffskontrolle

Die Systeme sind so konfiguriert, dass ein regulärer Zugriff mit administrativen Rechten nur für firmeninterne Techniker aus gesicherten Netzsegmenten möglich ist. Der Zugriff geschieht über kryptographisch stark gesicherte (SSH, IPsec per X.509-Authentifizierung) Wege. Der Zugriff und die Aktivitäten der Administratoren werden in Logfiles aufgezeichnet.

Weitergabekontrolle

Vertrauliche dienstliche Informationen dürfen nur über sichere Kommunikationswege übertragen werden.
Grundsätzlich kann auf das System TGP*open* nur durch autorisierte Nutzer zugegriffen werden. Die Übertragung von Daten erfolgt ausschließlich durch das System selbst an autorisierte Empfänger, verschlüsselt und 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 Sicherheitsrichtlinien für Mitarbeiter der EDV der 1&1 Internet AG.
Selbstverständlich sind unsere Mitarbeiter auf das Datengeheimnis gem. § 5 BDSG hin verpflichtet worden.
Um Datenverlust vorzubeugen, müssen alle arbeitsrelevanten Daten auf Servern gespeichert werden. Diese werden regelmäßig gesichert. Ein Datenverlust ist dadurch weitestgehend ausgeschlossen.

Eingabekontrolle

Durch die Einhaltung der oben aufgeführten Regeln zu Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle wurde die Grundlage für die Eingabekontrolle für TGP*open* geschaffen. Regeln, die hierüber hinausgehen, werden in diesem Kapitel dokumentiert.
Grundsätzlich wird im Rechte- und Rollen-Konzept zwischen Systemusern, Prozessusern und personalisierten Usern unterschieden.

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 AG hinterlegt.
Der Datenschutzbeauftragte des Auftraggebers hat das jederzeitige Recht, die Umsetzung seiner Weisungen bei der 1&1 Internet AG zu kontrollieren.

Verfügbarkeitskontrolle

Alle Dienste der gesamten 1&1 und ihrer Töchter sind hochsensibel in Bezug auf deren Verfügbarkeit. Die Kunden erwarten eine hochverfügbare Bereitstellung aller Netzwerk- und RZ-Dienstleistungen.
Zur Sicherstellung dieser werden in den als für notwendig Erachteten Abteilungen Notfallhandbücher erstellt. Aus der Hochverfügbarkeitsanforderung ergibt sich am Standort Karlsruhe, an dem das System aufgestellt ist, eine grundsätzlich hochredundant ausgelegte Netzwerk-Infrastruktur, die Einzelfehler in fast allen Bereichen und Doppelfehler in vielen Bereichen abfangen kann.
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, so schlägt die Früherkennung Alarm.
Zur ersten Bekämpfung von Bränden sind Handfeuerlöscher installiert.
Die Zentrale Elektrotechnik im Hauptrechenzentrum in Karlsruhe ist in vier (3+1) Blöcke aufgeteilt. In jedem Block ist die Technik Mittelspannung, Niederspannung, USV und Netzersatzanlage (NEA) enthalten. Ein Betriebsblock dient als Redundanz. Im 2. Bauabschnitt ist vorgesehen, einen weiteren Betriebsblock (4+1) zu realisieren. 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 an allen Ein- und Ausgängen der USV Anlagen überwacht.

Allgemeine technische und organisatorische Maßnahmen nach § 9 BDSG und Anlage

1. Zutrittskontrolle
Die physikalische Gewährung der Zutrittskontrolle obliegt den Maßnahmen des jeweilig beauftragten Dienstleisters. Diese sind:
|_| 1&1 mit Sitz in Montabaur (siehe Anhang des Providers 1&1)
|_| KRZN mit Sitz in Kamp-Lintfort

2. Zugangskontrolle
Das Eindringen Unbefugter in die DV-Systeme wird verhindert durch:
- Festlegung befugter Personen durch Stammdaten
- Benutzeridentifikation durch Anmeldnamen und Passwort
- Irreversible Verschlüsselung des Passwort
- Mindestlänge und Sonderzeichen des Passworts sind einstellbar
- AES Verschlüsselungsverfahren (Rijndael-Algorithmus)
- Completely Automated Public Turing (CAPTCHA)
- Optionale Sperrung des Zugangs nach 3x Falscheingabe
- Zugang an den Clients erfolgt durch Smartcards

3. Zugriffskontrolle
Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen werden
verhindert durch:
- Einrichtung verschiedener Berechtigungsstufen
1. auf Modulebene
2. auf funktionaler Ebene
- Zentrale Rechteverwaltung durch den Administrator
- Protokollierung der Systemnutzung
- Einrichtung und Auswertung von Zugriffsprotokollen
- Verpflichtung der Mitarbeiter auf Datengeheimnis

4. Weitergabekontrolle
Aspekte der Weitergabe personenbezogener Daten sind geregelt durch:
- Identitätsprüfung jeder Datenanfrage
- Transport der Daten erfolgt durch SSL-Verschlüsselung
- VPN-Verbindungen
- Protokollierung des Daten-Zugriffs

5. Eingabekontrolle
Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege wird gewährleistet durch:
- Protokollierung jeglicher Änderung durch Benutzer in Form
1. betroffener Datensatz
2. Art der Aktivität
3. Zeitpunkt der Aktivität bzw. des Ereignisses
4. ausführende Person (Benutzerkennzeichen)
- Erstellen eines Sicherungsdatensatzes vor der Löschung des Datensatzes durch den Anwender.

6. Auftragskontrolle
Die weisungsgemäße Auftragsdatenverarbeitung wird gewährleistet durch:
- Prüfung der Einhaltung formeller und organisatorischer Maßnahmen zum Datenschutz.
- Dokumentation der Auftragsergebnisse
- Der Auftrag ist schriftlich zu erteilen, wobei **insbesondere im Einzelnen festzulegen sind:**

1. der Gegenstand und die Dauer des Auftrags
2. die Berechtigten zur Erteilung von Aufträgen

7. Verfügbarkeitskontrolle
Die Daten werden gegen zufällige Zerstörung oder Verlust geschützt durch:
- ein tägliches Backup
- Spiegelung der Festplatten durch eine RAID – Implementierung
- eine Absicherung durch USV
- einen Virenscanner (Norman)
- eine Firewall

8. Trennungskontrolle
Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:
- Getrennte Speicherung der Daten
- Zugangs- und Zugriffstrennung der Daten
- Trennung von Test- und Produktiv-Daten