Vertrag zur Auftragsdatenverarbeitung gemäß § 11 BDSG

„Untis MultiUser Hosting“

zwischen dem / der

- nachstehend Auftraggeber genannt -

und dem / der

heinekingmedia GmbH

Hamburger Allee 2-4, 30161 Hannover

- nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand des Auftrags

heinekingmedia GmbH betreibt die Applikation Untis „MultiUser Hosting“. Im Zuge dieses Service ist es notwendig, diejenigen Daten, die vom Auftraggeber in Untis eingegeben oder importiert und dann bearbeitet bzw. verarbeitet werden, zu speichern.

Zu diesen Daten gehören insbesondere Stunden- und Vertretungspläne und abhängig von der eingesetzten Funktionalität unter Umständen auch personenbezogene Daten von Endanwendern (Schülerinnen und Schülern, Studentinnen und Studenten, Lehrpersonal).

Der Auftraggeber erteilt bei Abschluss eines Hosting-Vertrages über die Benutzung von Untis mit heinekingmedia GmbH oder mit einem Vertriebspartner oder Subvertriebspartner von heinekingmedia GmbH auch seine Zustimmung zu dieser Datenbearbeitung bzw. -verarbeitung und Datenspeicherung bzw. holt die entsprechende datenschutzrechtliche Einwilligung – sofern gesetzlich erforderlich – von den Endanwender ein.

1.2 Vertragsdauer

1.2.1.

Sämtliche Verträge, auf deren Basis der Auftraggeber die Applikation Untis sowie jegliche Erweiterungsmodule benutzt und auf welche die gegenständlichen Hosting-Bedingungen Anwendung finden, werden auf unbestimmte Zeit geschlossen.

Nach einer Mindestlaufzeit von 12 Monaten kann der Vertrag von jeder Vertragspartei schriftlich unter Einhaltung einer Frist von mindestens einem Monat zum 30. April eines jeden Jahres gekündigt werden.

1.2.2.

Der Auftraggeber kann den mit heinekingmedia GmbH oder mit einem Vertriebspartner oder Subvertriebspartner von heinekingmedia GmbH geschlossenen Hosting-Vertrag über Untis jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß von heinekingmedia GmbH oder deren Kooperationspartner gegen die Bestimmungen des jeweils als anzuwendend bekannt gegebenen oder aufgrund dieser Bedingungen anzuwendenden Datenschutzgesetzes oder gegen sonstige Bestimmungen dieser Hosting-Bedingungen vorliegt.

1.2.3.

Der Vertrag kann von heinekingmedia GmbH oder deren Vertriebspartner oder Subvertriebspartner, mit dem der Auftraggeber den Vertrag geschlossen hat, jederzeit ohne Einhaltung einer Frist gekündigt werden, wenn der Auftraggeber durch sein Verhalten die Sicherheit des Hosting-Betriebes gefährdet oder wenn ein schwerwiegender Verstoß des Auftraggebers oder der Endanwender gegen die Bestimmungen dieser Hosting-Bedingungen vorliegt.

2. Pflichten des Auftraggebers

2.1.

Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. heinekingmedia GmbH haftet daher nicht für Verstöße des Auftraggebers gegen die nur auf den Auftraggeber, nicht aber auf heinekingmedia GmbH anzuwendenden Datenschutz- und sonstigen rechtlichen Bestimmungen.

Werden vorhersehbare, längere Unterbrechungen des Services von heinekingmedia GmbH dem Auftraggeber rechtzeitig angekündigt, ist der Auftraggeber dafür verantwortlich, dass diese Informationen auch sämtlichen vom Auftraggeber autorisierten Endanwendern bzw. Betroffenen unverzüglich zur Kenntnis gebracht werden, sodass diesen aus der Unterbrechung des Services kein Nachteil entstehen kann.

2.2.

Der Auftraggeber informiert heinekingmedia GmbH unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der über Untis oder über eines der Erweiterungsmodule zu Untis erstellten Auftragsergebnisse feststellt.

2.3.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen von heinekingmedia GmbH und deren Partnern sowie deren Rechtsvorgängern oder jeglichen Rechtsnachfolgern, die in das Vertragsverhältnis eintreten, vertraulich zu behandeln.

2.4.

Der Auftraggeber ist für das Einrichten von Untis sowie dessen Erweiterungsmodule für seine Zwecke zuständig. Dazu gehören insbesondere das Verwalten von Endanwendern und das Vergeben von Zugriffsrechten innerhalb von Untis.

2.5.

Dem Auftraggeber obliegt die eventuell notwendige längerfristige Aufbewahrung der Daten bzw. das Anlegen von Sicherheitskopien, die über die Gewährleistung des täglichen Betriebs hinausgehen. Insbesondere obliegt es dem Auftraggeber, seine Daten rechtzeitig vor Beendigung des Vertragsverhältnisses zu sichern. Für die Sicherung steht dem Auftraggeber eine Backup-Funktionalität zur Verfügung.

2.6

Der Auftraggeber sowie die von ihm angelegten Endanwender werden es insbesondere unterlassen,

a. den Service missbräuchlich zu nutzen oder nutzen zu lassen, insbesondere Informationsangebote mit rechts- oder sittenwidrigen Inhalten zu übermitteln oder auf solche Informationen hinzuweisen, die der Volksverhetzung dienen, zu Straftaten anleiten oder Gewalt verherrlichen oder verharmlosen, sexuell anstößig bzw. pornographisch sind, geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden oder in ihrem Wohl zu beeinträchtigen oder das Ansehen der heinekingmedia GmbH oder deren Partnern schädigen können;

b. beleidigende oder verleumderische Inhalte zu verwenden, einzustellen, zu veröffentlichen oder auf entsprechendes Material auf einer externen Website zu verlinken, unabhängig davon, ob diese Inhalte andere Nutzer, oder andere Personen oder Unternehmen betreffen;

c. unzumutbar (insbesondere durch Spam) zu belästigen, gesetzlich geschützte Inhalte (z. B. durch das Urheber-, Marken-, Patent-, Designrecht oder sonstige Schutzgesetze) oder geistige Eigentumsrechte Dritter verwenden, einzustellen oder zu veröffentlichen, ohne dazu berechtigt zu sein, oder gesetzlich geschützte Waren oder Dienstleistungen zu bewerben, anzubieten oder zu vertreiben sowie wettbewerbswidrige Handlungen vorzunehmen oder zu fördern, einschließlich progressiver Kundenwerbung (z. B. Ketten-, Schneeball- oder Pyramidensysteme);

d. mit anderen Nutzern anzüglich oder sexuell geprägt zu kommunizieren;

e. zu versuchen, selbst oder durch nicht autorisierte Dritte Informationen oder Daten unbefugt abzurufen oder in Programme, die von heinekingmedia GmbH oder deren Partnern betrieben werden einzugreifen oder eingreifen zu lassen oder in Datennetze der heinekingmedia GmbH oder deren Partner unbefugt einzudringen

f. den möglichen Austausch von elektronischen Nachrichten missbräuchlich für den unaufgeforderten Versand von Nachrichten oder Informationen an Dritte zu Werbezwecken (Spamming) zu nutzen.

2.7.

Der Auftraggeber verpflichtet sich ferner,

a. die Endanwender auf die Einhaltung der in dem Punkt 2.6 genannten Pflichten schriftlich zu verpflichten;

b. die heinekingmedia GmbH unverzüglich über festgestellte Verstöße des Auftraggeber oder der Endanwender gegen die Bestimmungen dieser Hosting-Bedingungen (einschließlich der Pflichten in Punkt 2.6) schriftlich oder per E-Mail zu informieren und darauf hinzuwirken, dass die Verstöße unverzüglich abgestellt werden;

c. die heinekingmedia GmbH und deren Partner von Ansprüchen Dritter freistellen, die auf einer rechtswidrigen Verwendung des Service durch ihn oder die Endanwender beruhen oder die sich aus vom Auftraggeber oder Endanwender verursachten datenschutzrechtlichen, urheberrechtlichen oder sonstigen rechtlichen Streitigkeiten ergeben, die mit der Nutzung des Service verbunden sind.

3. Pflichten von heinekingmedia GmbH

3.1.

heinekingmedia GmbH und deren Partner verarbeiten personenbezogene Daten ausschließlich im Rahmen des gegenständlichen Services und entsprechend den Weisungen des Auftraggebers. Sie verwenden die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Um die Daten vor zufälliger Zerstörung oder Verlust zu schützen, werden in regelmäßigen Abständen Replikationen und Backups der Daten hergestellt.

Dem Auftraggeber wird in diesem Zusammenhang zugesichert, täglich Backups (Datensicherungen) bis 1 Monat in die Vergangenheit sowie monatlich (jeweils am Ersten eines jeden Monats) entsprechende Datensicherungen bis 6 Monate in die Vergangenheit vorzunehmen.

Für Erweiterungsmodule, die den persönlichen Dateispeicher des Auftraggebers betreffen, wie Untis Drive, wird ein tägliches Backup vorgenommen. In diesem Zusammenhang wird dem Auftraggeber ein Backup bis 5 Tage in die Vergangenheit zugesichert.

Andere Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

Dem Auftraggeber wird darüber hinaus zugesichert, die im Rahmen des Services bekannt gegebenen personenbezogenen Daten des Auftraggebers bzw. die vom Auftraggeber in Untis oder dessen Erweiterungsmodule eingegebenen personenbezogenen Daten von Schülerinnen und Schülern, Studentinnen und Studenten sowie von Lehrpersonal geheim zu halten.

3.2.

heinekingmedia GmbH sichert das Bemühen zu, den Service möglichst unterbrechungsfrei mit einer garantierten Verfügbarkeit von 98 % (Durchrechnungszeitraum 12 Monate) zu gewährleisten, wobei sich dieser Prozentsatz der Verfügbarkeit gemäß Punkt 5 errechnet, und eventuell auftretende Probleme möglichst rasch zu beheben.

Kurze Serviceunterbrechungen (in der Dauer von weniger als 10 Minuten) sind aus Wartungsgründen möglich und müssen nicht angekündigt werden. Vorhersehbare, längere Unterbrechungen des Services werden von heinekingmedia GmbH dem Auftraggeber jeweils rechtzeitig, d. h., zumindest zwei Wochen vorher, angekündigt.

3.3.

Der Auftraggeber ist jederzeit berechtigt, die Einhaltung der Vorschriften über den Datenschutz entsprechend dem Datenschutzgesetz, dem der Auftraggeber verpflichtet ist und die vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung entsprechender Auskünfte von heinekingmedia GmbH und Einsichtnahme in die gespeicherten Daten.

So lange ein Auftraggeber an heinekingmedia GmbH keine anderen, von ihm einzuhaltenden Datenschutzbestimmungen schriftlich bekannt gibt, halten sich heinekingmedia GmbH und deren Partner an die Regelungen der EU-Datenschutzrichtlinie 95/46/EG in der jeweils geltenden Fassung bzw. ausnahmsweise – soweit es Auftraggeber aus der Bundesrepublik Deutschland betrifft – an die für das jeweilige deutsche Bundesland geltenden Datenschutzbestimmungen.

3.4.

heinekingmedia GmbH und deren Partner setzen für den Service und für die notwendigen Datensicherungsmaßnahmen nur Personal ein, das

- auf das Datengeheimnis nach den jeweils geltenden bzw. vereinbarten Datenschutzbestimmungen verpflichtet wurde,
- über datenschutzrechtliche Vorgaben angemessen und der Aufgabensituation ent- sprechend belehrt und geschult wurde sowie
- über genügend Sachkunde für die ordnungsgemäße Abwicklung der Aufgaben verfügt.

3.5.

Nach Beendigung des Vertragsverhältnisses mit einem Auftraggeber werden sämtliche im Zusammenhang mit Untis und seinen Erweiterungsmodulen bekannt gegebene Daten des Auftraggebers gelöscht. Der Auftraggeber erhält darüber, sofern er dies schriftlich anfordert, eine schriftliche Bestätigung.

3.6.

heinekingmedia GmbH darf von einem Auftraggeber übernommene Aufträge bzw. Aufgaben nur nach vorheriger schriftlicher Genehmigung durch den Auftraggeber an Subunternehmen weiter übertragen. Für sämtliche Subunternehmen und Partner gelten die gleichen Pflichten wie für heinekingmedia GmbH. heinekingmedia GmbH verpflichtet sich, an allfällige Subunternehmen

und Partner die in dieser Hosting-Vereinbarung enthaltenen Pflichten weiter zu überbinden und die Einhaltung dieser Pflichten durch diese regelmäßig zu überprüfen.

3.7.

heinekingmedia GmbH sichert zu, dass bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis gemäß dem jeweils vom Auftraggeber bekannt gegebenen, für ihn geltenden Datenschutzgesetz gewahrt wird. Es wird in diesem Zusammenhang auch zugesichert, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. So lange ein Auftraggeber an heinekingmedia GmbH keine anderen, von ihm einzuhaltenden Datenschutzbestimmungen schriftlich bekannt gibt, sichert heinekingmedia GmbH zu, dass die Regelungen der EU-Datenschutzrichtlinie 95/46/EG in der jeweils geltenden Fassung bzw. ausnahmsweise – soweit es Auftraggeber aus der Bundesrepublik Deutschland betrifft – die für das jeweilige deutsche Bundesland geltenden Datenschutzbestimmungen eingehalten werden.

Auskünfte an Dritte dürfen nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilt werden.

4. Datensicherungsmaßnahmen

4.1.

Folgende technische und organisatorische Maßnahmen zur Datensicherung gelten zwischen sämtlichen Auftraggebern und heinekingmedia GmbH als vereinbart:

a) Zutrittskontrolle (Maßnahmen, um Unbefugten den Zutritt zu den Datenverarbeitungs- anlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden): siehe Anlage 1

b) Zugangskontrolle (Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können): siehe Anlage 1

c) Zugriffskontrolle (Maßnahmen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung entsprechenden Daten zugreifen können und dass diese Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können): siehe Anlage 1

d) Weitergabekontrolle (Maßnahmen, um zu 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): siehe Anlage 1

e) Eingabekontrolle (Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind): siehe Anlage 1

f) Verfügbarkeitskontrolle (Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind): siehe Anlage 1

4.2.

heinekingmedia GmbH sichert dem Auftraggeber im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller schriftlich vereinbarten Datensicherungsmaßnahmen, insbesondere der oben beschriebenen Maßnahmen zu.

4.3.

heinekingmedia GmbH sichert die Beachtung der „Grundsätze ordnungsgemäßer Datenverarbeitung" ausdrücklich zu und gewährleistet die Einhaltung der vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen, die für den Auftraggeber gelten und von diesem an heinekingmedia GmbH schriftlich bekannt gegeben wurden.

4.4.

Die technischen und organisatorischen Maßnahmen zur Datensicherung können im Laufe des Vertragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden.

4.5.

Sollten die für den Betrieb von Untis und seinen Erweiterungsmodulen getroffenen und in diesen Hosting-Bedingungen festgehaltenen Sicherungs- und Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht (mehr) genügen, benachrichtigt der Auftraggeber heinekingmedia GmbH unverzüglich.

Entsprechendes gilt für Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

5. Haftung

5.1.

Sollte die garantierte Verfügbarkeit des Services (gemäß Punkt 3.2.: 96 %) im Beobachtungszeitraum von einem Kalendermonat unterschritten werden, kann der Auftraggeber eine Gutschrift in Höhe von 25 % des Monatsentgelts für den Service von heinekingmedia GmbH verlangen.

Um das Recht auf Erhalt einer Gutschrift zu wahren, hat der Auftraggeber innerhalb von 7 Tagen nach einem die Verfügbarkeit beeinträchtigenden Vorfall diesen an heinekingmedia GmbH schriftlich zu melden.

Nach Ablauf des Beobachtungszeitraums wird von heinekingmedia GmbH festgestellt, ob die garantierte Verfügbarkeit tatsächlich unterschritten wurde und wird in diesem Fall dann dem Auftraggeber seitens heinekingmedia GmbH die Gutschrift auf die nächste Rechnung gutgeschrieben. Die Berechnung der Verfügbarkeit des Services wird auf Basis von Stunden nach der nachstehenden Formel durchgeführt:

Verfügbarkeit in Prozent = (Beobachtungszeitraum – angekündigte Ausfallszeiten – Ausfalls- zeit des Service) / (Beobachtungszeitraum – angekündigte Ausfallszeiten) x 100

Der Erhalt von Gutschriften stellt die einzige und ausschließliche Entschädigung für den Auftraggeber im Falle eines Serviceausfalls dar. Der Auftraggeber verzichtet ausdrücklich darauf, darüber hinausgehende Ansprüche welcher Art auch immer zu erheben.

5.2.

Für den Ersatz von Schäden, die ein vom Auftraggeber autorisierter Endanwender bzw. Betroffener wegen einer nach den anzuwendenden Datenschutzbestimmungen unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber diesem verantwortlich. Soweit der NUTZER zum Schadenersatz verpflichtet ist, bleibt ihm der Rückgriff gegenüber heinekingmedia GmbH in jenen Fällen vorbehalten, in welchen UNTIS GMBH oder deren Partner am Schadenseintritt ein Verschulden sowie ein Grad an Fahrlässigkeit, der über leichte Fahrlässigkeit hinausgeht, zur Last liegt.

6. Sonstige Bestimmungen

6.1.

heinekingmedia GmbH verpflichtet sich, sämtliche ihr aus den gegenständlichen Hosting- Bedingungen zukommenden Verpflichtungen auch an jeweilige Partner zu überbinden.

6.2.

Sollte eine Bestimmung dieser Hosting-Bedingungen ganz oder teilweise rechtsunwirksam oder undurchführbar sein oder werden, so berührt dies nicht die Rechtswirksamkeit oder Durchführbarkeit aller anderen Bestimmungen dieser Hosting-Bedingungen. Die Vertragsparteien werden die rechtsunwirksame oder undurchführbare Bestimmung durch eine wirksame und durchführbare Bestimmung ersetzen, die gemäß Inhalt und (wirtschaftlichem) Zweck der rechtsunwirksamen oder undurchführbaren Bestimmung möglichst nahe kommt.

6.3.

Sämtliche Änderungen und Ergänzungen eines Vertrages, auf dessen Basis ein Auftraggeber die Applikation Untis oder dessen Erweiterungsmodule benutzt und auf welchen die gegenständlichen Hosting-Bedingungen Anwendung finden, bedürfen der Schriftform, ebenso jeweiligen Änderungen dieser Hosting-Bedingungen, wobei solche nur in Ausnahmefällen in Betracht kommen und mit heinekingmedia GmbH gesondert ausgehandelt und ausdrücklich schriftlich vereinbart werden müssten. Dies gilt auch für jeweilige Nebenabreden und auch für ein Abgehen von diesem Schriftformerfordernis.

6.4.

Aus einer Handlung oder Unterlassung einer Vertragspartei oder Ihrer Partner oder vom Auftraggeber autorisierter Endanwender bzw. Betroffener kann kein Verzicht auf Rechte aus dieser Hosting-Vereinbarung abgeleitet werden, wenn ein solcher nicht ausdrücklich schriftlich von heinekingmedia GmbH oder dem Auftraggeber erklärt wird.

6.5.

Zur Entscheidung aller aus einem Vertrag, auf dessen Basis ein Auftraggeber die Applikation Untis oder dessen Erweiterungsmodule benutzt und auf welche die gegenständlichen Hosting-Bedingungen Anwendung finden, entstehenden Streitigkeiten (einschließlich der Interpretation der Bestimmungen dieser Hosting-Vereinbarung) wird die ausschließliche Zuständigkeit des jeweils sachlich zuständigen Gerichts vereinbart, in dessen örtlichem Zuständigkeitsbereich der registrierte Firmensitz von heinekingmedia GmbH gelegen ist.

6.6.

Auf einen Vertrag, auf dessen Basis ein Auftraggeber die Applikation Untis benutzt und auf welchen die gegenständlichen Hosting-Bedingungen Anwendung finden, bzw. auf diese Hosting-Bedingungen selbst; dies unter Ausschluss des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf („UN-Kaufrecht“).

Unterschrift heinekingmedia	Unterschrift Auftraggeber

Anlage 1: Vereinbarung zur Auftragsdatenverarbeitung gemäß § 11 BDSG:

Allgemeine technische und organisatorische Maßnahmen nach § 9 BDSG und Anlage

1. Zutrittskontrolle

Maßnahmen, die verhindern, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen erhalten, mit welchen personenbezogene Daten verarbeitet werden:

- Umzäunung der Gebäude
- Alarmanlage mit mehrstufigen Alarmbereichen
- Mehrstufige Sicherheitszonen
- Zutritt zu Sicherheitszonen nur nach Need-to-Prinzip
- Automatisches Zugangskontrollsystem mit Protokollierung der Zugänge
- Verwaltung und Wartung der Zutrittssysteme ist geregelt
- Türsicherungen durch Chipkarten-/Transpondersystem
- Schlüsselregelung (Schlüsselausgabe etc.) und Dokumentation der Schlüsselvergabe
- Protokollierung und Authentifizierung der Besucher
- Besucher-Zugang nur in ständiger Begleitung von Mitarbeitern
- Videoüberwachung von Sicherheitsbereichen auf dem Gelände
- Videoüberwachung von Sicherheitsbereichen innerhalb des Gebäudes
- Kontrollen durch Sicherheitsdienst außerhalb der Arbeitszeiten
- Sicherung von Fenstern der Geschäftsräume
- DataCenter-Räume verfügen nicht über Fenster

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können:

- Personenbezogene Authentifizierung von Benutzern mit Passwort im net.DE Netzwerk
- Automatisierte Passwortrichtlinien
- Differenzierte Vergabe von Berechtigungen
- Zertifikatsbasierte Zugangsberechtigungen für Administratoren
- Verschlüsselter Zugriff auf Systeme durch Administratoren
- Benutzerrechtevergabe nach Need-to-Know-Prinzip
- Firewalling
- Begrenzung der Administrationszugänge ausgehend von definierten Netzwerksegmenten
- Administratoren-Zugang von außerhalb nur via IPSecVPN
- BIOS-Passwörter und Verschlüsselung von mobilen Geräten zur Administration
- WLAN-Zugriff nur in einem separaten Firewall-Segment auf öffentliche Bereiche

3. Zugriffskontrolle, Speicherkontrolle

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:

- Passwortrichtlinien
- Protokollierung von Zugriffen
- Verschlüsselter Zugriff auf Systeme durch Administratoren
- Zusätzliche Protokollierung von bestimmten Anwendungen
- Sperren von Zugriffen nach einer bestimmten Anzahl erfolgloser Logins für bestimmte Systeme
- Sperren von Zugriffen bei Verdacht auf Verletzungen der Informationssicherheit
- Zugriff auf Systeme, die personenbezogene Daten der net.DE-Kunden gespeichert haben könnten, erfolgt nur durch Administratoren
- Reduktion der zugriffsberechtigten Personen auf das benötigte Minimum
- Elektronische Dokumentation sämtlicher Passwörter und Verschlüsselung dieser Dokumentation zum Schutz vor unbefugtem Zugriff

4. Weitergabekontrolle, Übermittlungskontrolle, Transportkontrolle

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:

- Verschlüsselung durch dem aktuellen Stand der Technik entsprechende Verschlüsselungsverfahren
- VPN
- Fax-Protokollierung
- Transport durch Mitarbeiter und net.DE-Fahrzeuge oder sorgfältig ausgewählte Subunternehmen
- Zugriff auf optische Laufwerke, USB etc. in der Probezeit von Mitarbeitern nicht möglich

5. Eingabekontrolle

Eine nicht-anfechtbare Eingabekontrolle kann für Systemadministratoren mit Super-User-Rechten auf einem System nur bedingt erfüllt werden. Super-User-Zugänge werden darum nur falls notwendig vergeben. Für alle übrigen Administratoren- und User-Zugänge gelten diese Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Protokollierung der Tätigkeiten von Usern
- Nachvollziehbarkeit der Eingabe, Änderung von Löschung von Daten durch User
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

6. Auftragskontrolle

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

- Bestellung eines Datenschutzbeauftragten
- Vertraulichkeitsvereinbarung mit Dritten (NDA)

- Revisionssichere Protokollierung von Weisungsbefugnissen
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen als Bestandteil aller Mitarbeiter-Arbeitsverträge
- Schulung der Mitarbeiter (Datenschutz und Sicherheitsbewusstsein)

7. Verfügbarkeitskontrolle

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

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlagen
- Dieselbetriebene Netzersatzanlange zur Notstromversorgung (NEA)
- Brandmeldezentrale (BMZ) mit Feuer und Brandmeldeanlangen
- Mehrzonen-Feuerlöschanlange (Argon oder Stickstoff)
- Mehrere, geschlossene Brandabschnitte
- Regelmäßige Tests von USV, Klimaanlage, NEA und BMA durch net.DE
- Zusätzlich Wartungsverträge für USV, Klimaanlagen, NEA und BMA
- Alarmmeldungen bei unbefugtem Zutritt über Fluchtwege
- Ständige Überwachung von Temperatur und Luftfeuchtigkeit im DC
- Notfallplan
- Erreichbarkeit des technischen Personals 24/7
- Backup der Systeme gemäß Backup-Plan
- Archivierung von Backups in getrennten Brandabschnitten
- Virenschutz
- Festplattenspiegelung
-

8. Datentrennungsgebot

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

- Logische Mandantentrennung
- Physikalisch getrennte Speicherung auf gesonderten Systemen
- Logische Trennung von Produktiv- und Test-Systemen
- Getrennte Ordnerstrukturen

Unterschrift heinekingmedia

Unterschrift Auftraggeber