Vertrag über die Verarbeitung von Daten im Auftrag

zwischen

Wiesmann GmbH
Markus Wiesmann
Auf der Dinkel 65
59379 Selm
Deutschland

– Auftraggeber –

und

united-domains AG
Gautinger Straße 10
82319 Starnberg

– Auftragnehmer –

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder »Verarbeitung« (von Daten) benutzt wird, wird die Definition der »Verarbeitung« im Sinne von Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen auf Grundlage des bestehenden Domain-Hostingvertrages und gegebenenfalls gesondert abgeschlossenen E-Mail- und/oder Webspace-Hostingvertrages:

– Der Auftragnehmer stellt dem Auftraggeber Domain-Hosting zur Verfügung, bei dem bei dem für kurze Zeit aus sicherheitstechnischen Gründen IP-Logs von Besuchern der Kunden-Domains gespeichert werden.

– Der Auftragnehmer stellt dem Auftraggeber E-Mail- und/oder Webspace-Services (Shared Hosting, nicht zur exklusiven Nutzung) zur Verfügung, auf denen Kundenkommunikation (E-Mails) und Kundendaten gelagert werden, die über vom Auftraggeber eingerichtete E-Mail-Konten ein- und ausgehen und/oder auf dem Webspace gespeichert werden.

– Der Auftragnehmer erbringt im Fall von technischen Schwierigkeiten hinsichtlich der vorbenannten Services Supportleistungen durch die eigenen Mitarbeiter.

Die zu verarbeitenden Daten sind diejenigen, die sich aufgrund von Besuchen der Kunden-Domain(s), der Kundenkommunikation per elektronischer Post (E-Mail) in den E-Mail-Accounts des Auftraggebers und durch gespeicherte Daten auf dem Webspace ergeben; sie umfassen Nutzungs- und Bestandsdaten, die sich aus E-Mails, IP-Logs und anderen gespeicherten Daten ergeben.

Zum Kreis der Betroffenen zählen Kunden der Auftraggeberin, sowie die Auftraggeberin, Ihre Mitarbeiter und Dritte.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Auftraggeber. Dem

Auftragnehmer darf den Auftraggeber auf seiner Meinung nach rechtlich unzulässige Datenverarbeitungen hinweisen.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer informiert den Auftraggeber, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber kann ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen. Die bei einverständlicher Umsetzung der Weisungen entstehende Vergütung bei Mehraufwänden richtet sich nach Ziffer 10 (2) dieses Vertrages.

(4) Der Auftraggeber kann weisungsberechtigte Personen in schriftlich oder in Textform benennen. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich oder in Textform mitteilen.

(5) Der Auftraggeber informiert den Auftragnehmer, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(6) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten auf Grundlage der bestehenden gesonderten Domain-, E-Mail und Webspace-Hostingverträge im Rahmen der getroffenen Vereinbarungen. Zweck, Art und Umfang der Datenverarbeitung richten sich nach diesem Vertrag.

(2) Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet

werden, vorbehaltlich gerichtlicher oder behördlicher Weisungen und gesetzlicher Bestimmungen, die dieser Bestimmung vorgreifen.

(3) Der Auftragnehmer bestätigt, dass er einen betrieblichen Datenschutzbeauftragten i.S.d. § 4f BDSG bestellt bzw. nach Art. 37 DSGVO benannt hat.

Zum Zeitpunkt des Vertragsschlusses ist

> Rechtsanwalt Daniel Dingeldey, Cosimaplatz 2, 12159 Berlin,
> datenschutzbeauftragter@united-domains.de, Telefon 08151-36867-0

als betrieblicher Datenschutzbeauftragter bestellt.

(4) Der Auftragnehmer sorgt im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten für die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen.

(5) Der Auftragnehmer gestaltet sein Unternehmen und seine Betriebsabläufe so, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(6) Der Auftragnehmer informiert den Auftraggeber, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

(7) Der Auftragnehmer informiert den Auftraggeber – soweit notwendig – über Verstösse gegen datenschutzrechtliche Vorschriften oder gegen die hier getroffenen vertraglichen Vereinbarungen, die im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt und zur Kenntnis gelangt sind.

(8) Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete

- besondere Arten personenbezogener Daten (Art. 9 DSGVO) oder

- personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder (auch i.S.v. Art. 10 DSGVO)
- personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, informiert der Auftragnehmer den Auftraggeber über Zeitpunkt, Art und Umfang des Vorfalls in Schrift- oder Textform (Fax/E-Mail). Die Information umfasst soweit möglich eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und eine Darlegung möglicher nachteiliger Folgen sowie darüber, welche Maßnahmen getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei entsprechenden Meldepflichten unterstützen.

(9) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32—36 DSGVO genannten Pflichten.

(10) An der Erstellung der Verzeichnisse von Verarbeitungen (Verfahrensverzeichnisse) durch den Auftraggeber wirkt der Auftragnehmer mit, indem er gegebenenfalls dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitteilt.

(11) Der Auftragnehmer benennt dem Auftraggeber die Personen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind.

Weisungsempfangsberechtigte Personen des Auftragnehmers sind:

Der Justiziar: zum Zeitpunkt des Vertragsschlusses Herr Steffen Hamann

Der CIO: zum Zeitpunkt des Vertragsschlusses Herr Tobias Sattler

5. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren. Hierfür kann er Selbstauskünfte des Auftragnehmers einholen.

(2) Der Auftragnehmer gibt dem Auftraggeber auf dessen schriftliche Anforderung die Auskünfte, die zur Durchführung einer Kontrolle erforderlich sind.

(3) Der erforderliche Umfang erstreckt sich angesichts der vertraglich vereinbarten Leistung des Auftragnehmers auf eine Selbstauskunft hinsichtlich der vom Auftragnehmer für den Auftraggeber verarbeiteten Daten nicht aber über die verwendeten Datenverarbeitungssysteme und -programme.

(4) Der Auftragnehmer erteilt, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber im Sinne des Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber und ermöglicht der jeweils zuständigen Aufsichtsbehörde eine Kontrolle.

(5) 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 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. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(6) Der Auftraggeber stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftragnehmer zu, sofern der Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt.

(7) Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen; sie ist in Ziffer 10 geregelt. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

6. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, die in den TOMs genannten Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Auftragnehmer darf – nach sorgfältiger Auswahl – Subunternehmen beauftragen, bzw. ersetzen, wobei er regelmäßig auf die Einhaltung der Datenschutzbestimmungen durch diese zu achten hat. Der Auftragnehmer stellt vertraglich sicher, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. Der Auftragnehmer informiert den Auftraggeber rechtzeitig über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer. Damit erhält der Auftraggeber die Möglichkeit, gegen eine solche Änderungen Einspruch zu erheben.

(2) Nicht als Unterauftragsverhältnisse verstehen sich Dienstleistungen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, Telekommunikationsleistungen, Bewachungs- und Wartungsdienste, Reinigungskräfte und Entsorgung von Datenträgern. Der Auftragnehmer vereinbart mit Dienstleistern, die Nebenleistungen für ihn erbringen, angemessene und gesetzteskonforme vertragliche Vereinbarungen und ergreift Kontrollmaßnahmen, um den Schutz und die Sicherheit der Daten des Auftraggebers gewährleisten zu können.

7. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer vor Vertragsschluss etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer bestätigt, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer bestätigt hiermit, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese zur Vertraulichkeit verpflichtet werden. Sofern der Auftragnehmer im Zusammenhang mit Leistungen für den Auftraggeber an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, verpflichtet er die hieran beteiligten Beschäftigten schriftlich auf das Fernmeldegeheimnis i.S.d. § 88 TKG.

(3) Der Auftragnehmer wird alle Beschäftigten, die Leistungen im Zusammenhang mit dem Auftrag des Auftraggebers erbringen, verpflichten, alle Daten des Auftraggebers, insbesondere die für den Auftraggeber verarbeiteten personenbezogenen Daten vertraulich zu behandeln.

8. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung – durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

9. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden, auch über das Ende des Vertragsverhältnisses hinaus. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen, es sei denn, es läge eine gerichtliche Entscheidung oder eine rechtmäßige Anfrage der Strafverfolgungsbehörden vor oder es besteht aufgrund gesetzlicher Regelung eine Auskunftspflicht.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

10. Vergütung

(1) Der Auftraggeber hat dem Auftragnehmer dessen Aufwände für Tätigkeiten, die neben dem Domain-, Webspace- und E-Mail-Hostingvertrag und im Zusammenhang mit seinen und den Kontrollbefugnissen der Aufsichtsbehörden entstehen, zu ersetzen, sofern diese durch den Auftraggeber mittel- und unmittelbar veranlasst sind und über eine bloße, einfach gelagerte Auskunftserteilung, Berichtigung, Löschung oder vergleichbare Leistung hinausgehen.

(2) Für diese Aufwände berechnet die Auftragnehmerin einen Betrag von € 1.200,00 pro Manntag (8 Arbeitszeitstunden), wobei die kleinste Abrechnungseinheit 15 Minuten beträgt. Im Falle von Reisekosten werden diese zusätzlich abgerechnet und zwar für Bahnfahrten in der 2. Klasse, Flugreisen in der Economy Class und bei Reisen mit Kraftfahrzeugen nach den gesetzlichen Bestimmungen. Die hier genannten Entgelte sind Nettopreise und verstehen sich zuzüglich der gesetzlichen Umsatzsteuer.

11. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

12. Dauer des Auftrags

(1) Der Vertrag wird auf unbestimmte Zeit geschlossen.

(2) Er ist mit einer Frist von einem Monat kündbar.

(3) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

(4) Der Vertrag endet automatisch, wenn kein gesonderter Dienstleistungsvertrag über Domain-, E-Mail- und/oder Webspace-Hosting mehr besteht.

(5) Das Recht auf außerordentliche Kündigung bleibt unberührt.

13. Beendigung

(1) Nach Beendigung des Vertrages löscht der Auftragnehmer auf Anforderung des Auftraggebers und unter Einhaltung gesetzlicher Vorgaben die angefallenen Daten auf Datenträgern. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer.

(2) Im Falle von E-Mail- und Webspace-Hosting werden mit Beendigung des jeweiligen Vertrages die Daten unmittelbar automatisiert gelöscht. Etwaige Datensicherungen beim Auftragnehmer werden in der Regel binnen spätestens vierzehn Tage nach Beendigung des Vertrages, bzw. nach Löschung der Ursprungsdaten ebenfalls automatisiert gelöscht.

14. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache,

dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Die Geltendmachung eines Zurückbehaltungsrechtes i.S.d. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten ausgeschlossen

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlagen:

Anlage 1 – Unterauftragnehmer
Anlage 2 – technische und organisatorische Maßnahmen

Anlage 1 – Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten (»Unterauftragnehmer«).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

QSC AG
Am Tower 5
90475 Nürnberg
T +49 911 309 50 50
F +49 911 309 50 049
datacenter-support@qsc.de
http://www.qsc.de

Bei der QSC AG liegen eigene Server des Auftragnehmers, auf denen Webspace und E-Mails der Kunden gespeichert werden.

1&1 IONOS SE
Elgendorfer Straße 57
56410 Montabaur
T +49 (0) 721 96 00
info@1und1.de
https://1und1.de

Über die 1&1 Internet SE betreibt der Auftragnehmer Webspace-Server und Webseiten-Baukästen.

Open-Xchange GmbH
Olper Hütte 5f
57462 Olpe
T +49 2761 75252 00
https://open-xchange.com

Über die Open-Xchange GmbH betreibt der Auftragnehmer teilweise E-Mail-Dienstleistungen

STRATO AG
Pascalstraße 10
10587 Berlin
T: +49 (0) 30-300 146 0
http://strato.de

Über die Strato AG bezieht united-domains seinen Online-Speicher.

Anlage 2

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

Der Auftragnehmer trifft nachfolgende technische und
organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Die Büroräume der united-domains AG befinden sich in einem Bürohaus in Starnberg.

Die Büroräume sowie der Kellerraum sind durch eine Schließanlage mit Sicherheitsschlössern gesichert. Die Ablageräume sind zusätzlich durch ein PinPad gesichert. Es gibt zwei Serverräume, deren einer durch eine Schließanlage und der andere durch eine Schließanlage und ein PinPad gesichert ist.

Die Schlüsselvergabe an Mitarbeiter und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende

eines Arbeitsverhältnisses die Übergabe und den Entzug von Schlüsseln und Zutrittsberechtigungen für die Büro- und andere Räume regelt.

Zutrittsberechtigungen zu den Serverräumen und der Ablage werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Besucher melden sich beim Empfang und erhalten durch diese Zutritt zu Büroräumen. Der Empfang kann die Eingangstür zum Büro einsehen und trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet.

united-domains nutzt für die unterschiedlichen Dienstleistungen, die sie erbringt, unterschiedliche Dienstleister und Rechenzentren.

Datenzentren:

QSC AG in Nürnberg und München

Die Rechenzentren der QSC AG befinden sich auf eingezäuntem Gelände. Die Gebäude oder Gebäudeteile sind videoüberwacht und zum Teil mit Bewegungsmeldern und einer Einbruchsmeldeanlage überwacht.

Die Maßnahmen zur Zutrittssicherheit sind abhängig vom Einsatzzweck der Räumlichkeiten und dem Schutzbedarf der Systeme, die sich in ihnen befinden. Sensible Datenverarbeitungsanlagen befinden sich immer in entsprechend geschützten Räumlichkeiten des Anbieters.

Es existieren technische und organisatorische Maßnahmen zur Beschränkung des Zutritts zu geschützten Bereichen für interne und externe Personen. Für den Zutritt zu den Rechenzentren existiert ein Rechtesystem.

Die Zutrittssteuerung an den Rechenzentren erfolgt über ein Zutrittskontrollsystem. Das System regelt und kontrolliert den Zutritt zum Grundstück und zu den Gebäuden. Es besteht ein Protokoll geführtes Schlüsselmanagement.

Die Rechenzentren werden rund um die Uhr (24X7) von einem Wachdienst überwacht. Es bestehen zudem technische Überwachungssysteme.

Open-Xchange GmbH in Olpe

Der Dienstleister ist nach ISO/IEC 27001:2013 zertifiziert. Das Rechenzentrum erlaubt den Zutritt nur für Mitarbeiter. Es besteht ein Protokoll geführtes Schlüsselmanagement. Darüber hinaus ist der Zutritt über elektronische und biometrische Kontrollen gesichert. Serverräume sind nochmals gesondert geschützt. Es gibt besondere zutrittsbegrenzte Bereiche.

1&1 Internet SE

Das Rechenzentrum wird tagsüber von einem Pförtner überwacht und außerhalb der Geschäftszeiten von einem Sicherheitsdienst, der regelmäßige Kontrollgänge macht. Es gibt eine Einbruchmeldeanlage. Mitarbeiter haben die Pflicht, Ausweise zu tragen. Besucher werden innerhalb der Gebäude von autorisierten Mitarbeitern begleitet. Es gibt eine Ausweisrichtlinie, ein Ausweisbuch und eine nur per Passwörtern von Autorisierten nutzbare Verwaltungssoftware. Darüber hinaus gibt es ein Zutrittskontrollsystem und Schlüsselvergaberichtlinien, die unter anderem die Protokollierung von vergebenen Zutrittskarten vorsieht. Es gibt ein Videoüberwachungssystem, Sicherheitstüren und eine Bereichswechselkontrolle. Die Türen sind mit Sicherheitsschleusen versehen, die einen elektronischem Schlüssel zusammen mit PIN-Eingabe benötigen. Sämtliche Türen sind mit digitalen Schließzylindern versehen. Die Zugänge zum Rechenzentrum sind videoüberwacht.

Strato AG

Unbefugten ist der Zutritt zu Räumen, in denen Datenverarbeitungsanlagen untergebracht sind, verwehrt. Der Zutritt zu den Datenverarbeitungsanlagen wird protokolliert. Die Berechtigung zum Zutritt ist auf bestimmte Personen festgelegt. Die personengebundenen Zutrittsberechtigungen wird verwaltet. Fremdpersonal erhalten Zutritt nur in Begleitung. Die Räumlichkeiten werden überwacht.

1.2 Zugangskontrolle

Für die Zugangskontrolle sind nachfolgende Maßnahmen von united-domains AG getroffen worden:

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren oder zur Vergabe von Zugangsdaten Berechtigte vergeben, je nachdem auf welche Systeme Zugriff notwendig ist. Je nach System und Notwendigkeit findet eine Protokollierung der Erteilung von Berechtigungen statt. Darüber hinaus wird bei einigen Systemen protokolliert, wer die letzte Rechteänderung pro Tool und Mitarbeiter durchgeführt hat. Bei sensiblen Systemen wird die Berechtigung mehrmals im Jahr überprüft.

Der Benutzer erhält in der Regel einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Es gibt eine Passwortrichtlinie. Das Werkzeug, das Mitarbeitern zur Erstellung von Passwörtern zur Verfügung steht, zeigt zudem anschaulich die Qualität des gewählten Passworts und lässt nur solche mit hoher Qualität überhaupt zu. Es enthält eine Anleitung zur Erstellung sicherer Passwörter.

Bei besonders sensiblen Systemen erfolgt die Zugriffsrechtevergabe über Administratoren. Bei weniger kritischen Systemen erfolgt die Vergabe von Zugriffsrechten über Abteilungs- oder Teamleiter. Die Rechtevergabe erfolgt auf Anfrage eines Mitarbeiters gegenüber seinem direkten Vorgesetzten, wenn er Zugriffe benötigt. Dieser entscheidet ob der Zugriff notwendig ist und unterscheidet nach Lese- und Schreibrecht. Die Rechte werden granular vergeben und können auf Tool- und Flag-Ebene eingeschränkt vergeben werden.

Der Zugriff auf Datenbanken unterliegt besonderen Regeln und wird nur stufenweise nach Überprüfung der Notwendigkeit und nach bestimmten zeitlichen Abläufen durch den jeweiligen Teamleiter freigegeben.

Fernzugriffe auf IT-Systeme der united-domains erfolgen ausschließlich über verschlüsselte Verbindungen und von Administratoren freigeschaltete Geräte.

Datenzentren:

QSC AG in Nürnberg und München

Zum Zugang zu Systemen muss sich der Nutzer grundsätzlich mittels eines Verfahrens auf dem aktuellen Stand der Technik authentifizieren. Bei Systemen mit besonders hohem Schutzbedarf bzw. kritischen Zugriffswegen sind zusätzliche Verfahren, wie z. B. eine Zwei-Faktor-Authentifizierung, etabliert.

Der Zugang zu Applikationen und zu Informationen erfolgt auf Basis von Rollen und dem konkreten geschäftlichen Bedarf der Benutzer. Es gilt das "Need To Know"-Prinzip.

Das Passwortverfahren ist in einer Passwortrichtlinie dokumentiert, in der hohe Anforderungen an die Erstellung von Passworten gestellt wird und über die nur sehr sichere Passworte zugelassen werden.

Fehlerhafte Anmeldungen werden soweit sinnvoll und technisch machbar protokolliert und bei Bedarf ausgewertet.

Unsichere Netze werden durch Security Gateways separiert und überwacht.

Der Zugang über mobile Geräte bzw. deren Einsatz wird über eine Richtlinie und über die "Regeln für mobile Devices" reglementiert und gesteuert.

Open-Xchange GmbH in Olpe:

Der Dienstleister ist nach ISO/IEC 27001:2013 zertifiziert. Der Zugang zu Systemen und Netzwerk ist benutzer- und passwortgeschützt. Es besteht eine Passwortregelung, die die Anforderungen für die Komplexität für Passwörter und deren regelmäßige Erneuerung beschreibt. Sensible Systeme sind nur über gezielte zusätzliche Freigaben benutzbar. Benutzer werden nach mehreren Zugriffsfehlversuchen automatisch blockiert. Systeme

sperren sich automatisiert nach einem definierten Zeitablauf ohne Aktivität des Nutzers (Bildschirmschonersperre).

1&1 Internet SE

Der Zugriff auf Systeme erfolgt nach einem formalen Benutzer- und Berechtigungsprozess gemäß der internen Sicherheitsrichtlinie. Die Berechtigungsvergabe wird dokumentiert. Jeder berechtigte Benutzer ist auf eine eigene Benutzer-ID auf dem Zielsystem beschränkt. Die Zugangsberechtigungen sind feingranular konfigurierbar. Alle Systeme sind durch ein zweistufiges Identifizierungsverfahren geschützt. Fernzugriffe sind nur in authentifizierter Form über VPN möglich und werden protokolliert. Es können nur authorisierte Geräte auf die Systeme zugreifen. Daten mit hohem Schutzbedarf werden nur nach BSI-Standards verschlüsselt gespeichert.

Strato AG

Ziel ist es zu verhindern, das die Datenverarbeitungssysteme von Unbefugten genutzt werden. Dazu ist der Schutzbedarf festgelegt. Es gibt einen Zugangsschutz, sichere Zugangsverfahren mit verschlüsselter und starker Authentisierung, Protkollierung und Überwachung von Zugriffen und Berechtigung sowie Verwaltung und Dokumentation der Vorgänge.

1.3 Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen der united-domains AG werden von Administratoren und bestimmten Mitarbeitern eingerichtet.

Berechtigungen werden grundsätzlich nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind. Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten.

Es gibt für bestimmte Systeme ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.

Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet.

Alle Mitarbeiter der united-domains AG sind angewiesen, Informationen mit personenbezogenen Daten in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen. In den unterschiedlichen Büros gibt es, je nach Datensensibilität Aktenvernichter (Schredder) mit unterschiedlichen Sicherheitsstufen. Papiere mit personenbezogenen Daten werden ausschließlich in Schreddern mit der höchsten Sicherheitsstufe vernichtet.

Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

Datenzentren:

QSC AG in Nürnberg und München

Zum Zweck der Zugriffskontrolle erfolgt die Autorisierung von Benutzern über ein Rechte- bzw. Berechtigungssystem. Besondere Zugriffsberechtigungen bedürfen der Genehmigung durch Beauftragte. Vergabe und Entzug von Zugriffsberechtigungen werden durch einen elektronischen Workflow unterstützt und dokumentiert. Der Berechtigungsprozess beinhaltet den Entzug von Zugriffsberechtigungen. Eine Kontrolle der Berechtigungsvergaben erfolgt anlassbezogen und regelmäßig im Rahmen interner und externer Audits.

Die kontrollierte Vernichtung von Daten und Ausdrucken erfolgt durch spezialisierte, zertifizierte Dienstleister.

Open-Xchange GmbH in Olpe

Der Dienstleister ist nach ISO/IEC 27001:2013 zertifiziert. Die Zugriffsrechte werden ausschließlich von Administratoren vergeben. Die Berechtigung ist granular und wird nach Notwendigkeit vergeben. Die Berechtigungsvergabe wird protokolliert, die Berechtigungen mehrmals im Jahr überprüft. Zugriffe auf die Systeme werden beim Login protokolliert.

1&1 Internet SE

Aufgrund der Systemkonfiguration sind reguläre Zugriffe nur mit administrativen Rechten für autorisierte Mitarbeiter nach dem Need-to-Know Prinzip möglich. Zugriffe auf System-IDs und auffällige Zugriffsversuche werden protokolliert. Bei auffälligen Zugriffen findet eine Alarmierung der autorisierten Administratoren statt. Weiteres ist in einer Sicherheitsrichtlinie geregelt.

Strato AG

Es kann nur auf die Daten zugegriffen werden, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

1.4 Trennung

Alle von der united-domains AG und deren Dienstleistern für Kunden eingesetzten IT-Systeme sind jeweils getrennt, je nach Verarbeitungszweck, aufgesetzt. Die Trennung von Daten von verschiedenen Kunden innerhalb der einzelnen Systeme ist stets gewährleistet.

Testsysteme und Livesystem der united-domains AG sind hart getrennt: Zugriffe untereinander sind aufgrund physischer Trennung ausgeschlossen. Darüber hinaus bestehen Firewall-Regeln.

1.5 Pseudonymisierung & Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt bei der united-domains AG wie auch bei deren Dienstleistern grundsätzlich über verschlüsselte Verbindungen. Die Kommunikation zwischen sensiblen Systemen erfolgt immer verschlüsselt. Passwörter von Kunden werden im gesamten System verschlüsselt gespeichert.

Zugriffe von Kunden auf Systeme (z.B. Webspace) erfolgen verschlüsselt. Logs werden teilweise pseudonymisiert (IP verkürzt) oder nach 7 Tagen gelöscht.

Darüber hinaus werden Daten auf mobilen Geräten (Notebooks) und externen Datenträgern verschlüsselt gespeichert. Es besteht eine entsprechende Handlungsrichtlinie.

2. Integrität

2.1 Eingabekontrolle

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die von der united-domains AG im Auftrag verarbeitet werden, unterliegt alleine den Auftraggebern. Nur nach gesonderter Beauftragung durch den jeweiligen Auftraggeber nehmen Mitarbeiter der united-domains AG Einblick in Daten (Webspace, E-Mail) der Auftraggeber.

Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden. Die Zugriffe über bestimmte Tools werden in einem User-Log vermerkt, inklusive eindeutigem Identifizierungsmerkmals des eingeloggten Mitarbeiters. Die Protokolle bestehen solange die zweckgebundene Notwendigkeit gegeben ist. Der Zugriff auf diese Protokolle unterliegt der jeweiligen Berechtigung des Mitarbeiters.

2.2 Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden von der united-domains AG erfolgt, darf jeweils nur in dem Umfang, erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.

Alle Mitarbeiter der united-domains AG werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.

Alle Mitarbeiter der united-domains AG werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

3. Verfügbarkeit und Belastbarkeit

Daten auf den Systemen von united-domains AG werden mindestens täglich gesichert. Die Sicherungen werden verschlüsselt an physisch getrennten Orten gespeichert. Es gibt ein Backupprozedere.

Das Einspielen von Backups wird regelmäßig getestet.

Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. In den Serverräumen befinden sich Brandmeldeanlagen. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

Die Daten werden auf ihre Integrität hin überprüft, um sie vor Schäden bei Fehlfunktionen von System zu schützen. Der Zugriff darauf unterliegt einer Freigabe für bestimmte Mitarbeiter.

Es gibt bei der united-domains AG einen Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

Datenzentren:

QSC AG in Nürnberg und München

Gesetzliche Vorgaben zum Brand- und Wasserschutz werden in allen Gebäuden eingehalten. Die Rechenzentren sind ISO27001 und nach weiteren TÜV Standards zertifiziert und entsprechen hohen Anforderungen an Brand- und Wasserschutz.

Die Rechenzentren des Anbieters sind durch getrennte USV-Anlagen mit Batteriepufferung und Dieselgeneratoren gegen Stromausfälle gesichert. Die Hauseinführungen sind redundant implementiert.

Notfallplan und entsprechende Handbücher zur Aufrechterhaltung der Kernprozesse im Notfall und zur möglichst raschen Wiederherstellung des Normalbetriebs sind vorhanden und etabliert. Die für die Erfüllung des Notfallplans notwendigen Übungen und Tests sind definiert, werden durchgeführt und die Durchführung sowie Verbesserungsmaßnahmen werden dokumentiert.

Open-Xchange GmbH in Olpe

Es bestehen Backupregeln. Server und Festplatten werden gespiegelt. Es bestehen unterbrechungsfreie Stromversorgungen. Backups werden an physisch getrennte Orte verbracht. Es gibt Notfallpläne. Die Serverräume verfügen über Klimanalagen.

1&1 Internet SE

Es bestehen Notfallhandbücher mit Wiederanlaufverfahren und ein Backup-Verfahren. Daten werden in regelmäßigen Abständen in einem sicheren Ort innerhalb des Rechenzentrums gesichert. Es werden Funktionstests von Backups vorgenommen. Die Systeme sind über Firewalls geschützt und werden täglich durch autorisierte Systemadministratoren gewartet und aktualisiert. Es besteht ein zentrales Systemmanagementsystem. Das Rechenzentrum ist mit einer unterbrechungsfreien

Stromzufuhr ausgestattet und an ein gesondertes Netz angeschlossen. Darüber hinaus gibt es eine Brandschutzfrüherkenungsanlage sowie eine Feuerlöschanlage.

Strato AG

Es besteht ein Notfallplan und Datensicherungskonzept. Brandschutz ist gewährleistet, Primärtechnik, Stromversorgung und Kommunikationsverbindungen sind redundant. Die Systeme werden überwacht und die Notfalleinrichtungen regelmäßig überprüft.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die united-domains AG hat ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.

Es sind ein Datenschutzbeauftragter und ein Informationssicherheitsbeauftragter benannt. Diese ergreifen in Abstimmung Maßnahmen im Bereich von Datenschutz und Datensicherheit, die im Wege eines Datenschutzmanagementsystems umgesetzt werden.

In regelmässigen Abständen finden Datenschutzschulungen durch den Datenschutzbeauftragten statt. Es wird erfasst, wer an der Schulung teilgenommen hat. Die Schulungsunterlagen stehen allen Mitarbeitern zur Einsicht zur Verfügung. Bei Beginn des Arbeitsverhältnisses und unter anderem im Rahmen der Datenschutzschulungen werden die Mitarbeiter der united-domains AG zur Verschwiegenheit und Vertraulichkeit verpflichtet.

Es ist unter anderem über Schulungen sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich gemeldet und untersucht werden. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese über Art und Umfang des Vorfalls informiert werden.

Bei der Verarbeitung von Daten für eigene Zwecke erfolgt im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde.

Es existiert ein Verzeichnis der Verarbeitungstätigkeiten.

4.1 Auftragskontrolle

Die Verarbeitung der im Auftrag verarbeiteten Daten erfolgt ausschließlich in der Europäischen Union.

Die united-domains AG hat einen betrieblicher Datenschutzbeauftragter benannt.

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag nach zuvor durchgeführter Prüfung durch den Datenschutzbeauftragten abgeschlossen.

4.2 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Die Mitarbeiter von united-domains AG tragen bei der Planung und Entwicklung der Software und Systeme Sorge dafür, dass dem Grundsatz der Erforderlichkeit Rechnung getragen wird. Kritische Fragen werden mit dem Datenschutzbeauftragten abgestimmt.

Berechtigungen auf Daten oder Applikationen können flexibel und granular gesetzt werden.