Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

zwischen

_____
(Firma)

_____
(Straße)

_____
(PLZ Ort)

– nachfolgend „Auftraggeber“ genannt –

und

netracom GmbH
Weidenstraße 20
45772 Marl

– nachfolgend „Auftragnehmer“ genannt –

besteht / bestehen unter

Kundennummer: _____

ein / mehrere von dem Auftraggeber genutzte(r) Vertrag / Verträge (nachfolgend „Hauptvertrag“ genannt).

1. Vertragsgegenstand

Im Rahmen der Leistungserbringung in der Geschäftsbeziehung zwischen Auftraggeber und Auftragnehmer ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

2. Umfang der Beauftragung

2.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.
2.2 Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie in Anlage 1 zu diesem Vertrag spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.
2.3 Dem Auftragnehmer bleibt es vorbehalten, die Auftraggeber-Daten zu anonymisieren oder zu aggregieren, so dass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, und in dieser Form zum Zweck der bedarfsgerechten Gestaltung, der Weiterentwicklung und der Optimierung sowie der Erbringung des nach Maßgabe des Hauptvertrags vereinbarten Dienstes zu verwenden. Die Parteien stimmen darin überein, dass anonymisierte bzw. nach obiger Maßgabe aggregierte Auftraggeber-Daten nicht mehr als Auftraggeber-Daten im Sinne dieses Vertrags gelten.
2.4 Der Auftragnehmer darf die Auftraggeber-Daten im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke auf eigene Verantwortung verarbeiten und nutzen, wenn eine gesetzliche Erlaubnisvorschrift oder eine Einwilligungserklärung des Betroffenen das gestattet. Auf solche Datenverarbeitungen findet dieser Vertrag keine Anwendung.
2.5 Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44 - 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

3. Weisungsbefugnisse des Auftraggebers

3.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
3.2 Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers

und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens, in dem die Weisung zu dokumentieren und die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber zu regeln ist.

3.3 Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeber-Daten beim Auftraggeber liegt.

4. Verantwortlichkeit des Auftraggebers

4.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4.2 Dem Auftraggeber obliegt es, dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeber-Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4.3 Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

4.4 Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

5. Anforderungen an Personal

Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten

6. Sicherheit der Verarbeitung

6.1 Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten. Die vom Auftragnehmer umgesetzten, erforderlichen technischen und organisatorischen Maßnahmen, werden Grundlage des Auftrags. Die Dokumentation der technischen und organisatorischen Maßnahmen wird dem Auftraggeber übergeben.

6.2 Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen.

7. Inanspruchnahme weiterer Auftragsverarbeiter

7.1 Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus Anlage 2. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.
7.2 Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.
7.3 Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.
7.4 Unter Einhaltung der Anforderungen der Ziffer 2.5 dieses Vertrags gelten die Regelungen in dieser Ziffer 7 auch, wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird. Der Auftraggeber bevollmächtigt den Auftragnehmer hiermit, in Vertretung des Auftraggebers mit einem weiteren Auftragsverarbeiter einen Vertrag unter Einbeziehung der EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern vom 5.2.2010 zu schließen. Der Auftraggeber erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Art. 49 DSGVO im erforderlichen Maße mitzuwirken.

8. Rechte der betroffenen Personen

8.1 Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.
8.2 Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.
8.3 Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Auftraggeber-Daten, die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und

den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.
8.4 Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten, Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.
8.5 Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Art. 20 DSGVO besitzt, wird der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Bereitstellung der Auftraggeber-Daten in einem gängigen und maschinenlesbaren Format unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

9. Mitteilungs- und Unterstützungspflichten des Auftragnehmers

9.1 Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber zeitnah über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten unterstützen.
9.2 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

10. Datenlöschung

10.1 Der Auftragnehmer wird die Auftraggeber-Daten nach Beendigung dieses Vertrages löschen, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.
10.2 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

11. Nachweise und Überprüfungen

11.1 Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.
11.2 Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.
11.3 Zur Durchführung von Inspektionen nach Ziffer 11.2 ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 9 bis 17 Uhr) nach rechtzeitiger Vorankündigung gemäß Ziffer 11.5 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von

Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeber-Daten verarbeitet werden.

11.4 Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

11.5 Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.

11.6 Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 11 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

11.7 Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrage anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

12. Vertragsdauer und Kündigung

12.1 Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

13. Haftung

13.1 Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.
13.2 Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

14. Schlussbestimmungen

14.1 Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.
14.2 Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

x

_____

(Ort, Datum, Unterschrift Auftraggeber)

Marl, 12. September 2022

_____

(Ort, Datum, Unterschrift Auftragnehmer)

netracom
Weidenstraße 20 · 45772 Marl
Tel.: 02365 297350-0
Fax: 02365 297350-9
E-Mail: info@netracom.de
Web: www.netracom.de

Anlagen:

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Anlage 2: Weitere Auftragsverarbeiter

Anlage 3: technische und organisatorische Maßnahmen

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Zweck der Datenverarbeitung	Hosting, Webdesign, SEO, Onlineshops, Impressum, Datenschutzerklärung, SSL Zertifikate, Warenwirtschaft
Art und Umfang der Datenverarbeitung	Speicherung, Weitergabe (z.B. SSL-Zertifikate, Datenschutzerklärung, Impressum), Bearbeitung, Einfügen von Inhalten in Websites, Bearbeiten bei Onlineshops
Art der Daten	Vertragsdaten Zahlungsdaten Mitarbeiterdaten
Kategorien betroffener Personen	Kundendaten des Auftraggebers Mitarbeiterdaten

Anlage 2: Weitere Auftragsverarbeiter

Firma, Anschrift	Art der Verarbeitung	Zweck	Art der Daten	Kategorien der betroffenen Personen
Host Europe GmbH Hansestr. 111 51149 Köln	Speicherung, Bearbeitung	Hosting	Mitarbeiterdaten, Unternehmensdaten	Mitarbeiter
icertificate GmbH Nordstraße 73a 53111 Bonn	Speicherung, Bearbeitung	SSL-Zertifikate	Mitarbeiterdaten, Unternehmensdaten	Mitarbeiter
eRecht24 GmbH & Co.KG Lietzenburger Str. 94 10719 Berlin	Speicherung, Bearbeitung	Datenschutzerklärung Impressum	Mitarbeiterdaten, Unternehmensdaten	Mitarbeiter

Anlage 3: Technisch-organisatorische Maßnahmen

Organisation:

netracom GmbH
Weidenstraße 20
45772 Marl
- nachfolgend netracom genannt -

vertreten durch den Geschäftsführer: Martin König

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

Zutrittskontrolle

Der Zugang zum Haupteingang der netracom sowie sämtlicher Nebeneingänge ist durch einen Zaun physikalisch beschränkt. Die Türen und Tore durch den Zaun sind verschlossen und können nur mit Transpondern von Mitarbeitern der netracom Vorort geöffnet werden. Darüber hinaus können das Haupttor sowie der Haupteingang des Zauns via Klingel und daran gekoppelte manuelle Öffnungsfunktion durch netracom-Mitarbeiter geöffnet werden.

a. Zutrittskontrolle des Gebäudes Tag/Nacht

1. Haupteingang

   Die Zugänge zum Gebäude sind stets verschlossen und können von außen nur mit Sicherheitsschlüsseln geöffnet werden. Der Zugang zum Gebäude wird durch qualifizierte Mitarbeiter am zentralen Empfang überwacht und jeder Mitarbeiter, Kunde oder Lieferant muss sich am Empfang anmelden. Besucher müssen entweder angemeldet sein oder über die Berechtigungen zu einer Eigenanmeldung verfügen. Besucher werden von einer Mitarbeiterin oder einem Mitarbeiter persönlich am Empfang abgeholt. Organisatorisch ist geregelt, dass Fremde sich im Gebäude niemals allein aufhalten oder frei bewegen dürfen.

2. Weitere Zugänge

   Der Nebeneingang zum Gebäude ist ebenfalls stets verschlossen und kann nur mit Sicherheitsschlüsseln geöffnet werden. Der Zugang zum Gebäude wird durch qualifizierte Mitarbeiter am zentralen Empfang überwacht und jeder Mitarbeiter, Kunde oder Lieferant muss sich am Empfang anmelden. Besucher müssen entweder angemeldet sein oder über die Berechtigungen zu einer Eigenanmeldung verfügen. Besucher werden von einer Mitarbeiterin oder einem Mitarbeiter persönlich am Empfang abgeholt. Organisatorisch ist geregelt, dass Fremde sich im Gebäude niemals allein aufhalten oder frei bewegen dürfen.

b. Zutrittskontrolle für den Serverraum (falls im Haus betrieben)

1. Unbefugten wird der Zutritt zu Datenverarbeitungssystemen nicht gewährt.

Zugangskontrolle

a. Zugang zu Datenverarbeitungsstationen und Systemen

2. Der Zugang über Außenschnittstellen zu unseren EDV-Systemen ist durch eine Firewall geschützt. Öffentlich erreichbare Systeme, wie E-Mail oder Internetzugang werden über entsprechende Trennungen von anderen Diensten isoliert. Sämtliche Systeme sind passwortgeschützt und verfügen über benutzerspezifische Zugänge. Gruppenzugänge werden nicht genutzt.

b. Allgemeine Passwortrichtlinie

1. Der Einsatz starker Passwörter ist Basis unserer internen Passwortrichtlinie. Die Passwort-Richtlinie der netracom definiert eine hohe Passwortkomplexität, sowie den Verbot der Wiederverwendung eines Passwortes. Gemäß der internen Richtlinien der netracom erfolgen je nach Systemart und Einstufung unterschiedliche Reaktionen auf Fehlversuche bei der Anmeldung. Neben der zeitweisen Sperrung, dem dynamischen Hinzufügen von Netzwerk-Sperren, oder der vollständigen Sperrung eines Zugangs erfolgt auch eine Protokollierung und Alarmierung.

c. Zugriffskontrolle

1. Im Falle einer externen Einwahl in die internen Netzwerke der netracom erhält der Mitarbeiter lediglich Zugriff auf für ihn relevante Netzbereiche. Die Allgemeine netracom Richtlinie: Zugriff nur gemäß den weisungsgemäßen Befugnisse.

d. Berechtigungskonzept Laufwerk

1. Der Zugriff auf Netzwerkverzeichnisse oder Systeme, in denen personenbezogene Daten gespeichert werden, ist auf die jeweiligen Personen beschränkt, die mit den Aufträgen beschäftigt sind, für die solche Daten verwendet werden sollen. Dabei muss jeder Benutzer sich mit personenspezifischen Zugangsdaten authentifizieren. Die initiale Zugriffsmöglichkeit ist, wo immer dies aufgrund der Funktion des Systems und den Vorgaben des Kunden realisiert werden kann, immer auf das interne Netzwerk der netracom beschränkt.

e. Berechtigungskonzept ERP

1. Der Zugriff auf ERP Systeme, in denen personenbezogene Daten gespeichert werden, ist auf die jeweiligen Personen beschränkt, die mit den Aufträgen beschäftigt sind, für die solche Daten verwendet werden sollen. Dabei muss jeder Benutzer sich mit personenspezifischen Zugangsdaten authentifizieren.

f. Berechtigungskonzept CRM

1. Der Zugriff auf CRM Systeme, in denen personenbezogene Daten gespeichert werden, ist auf die jeweiligen Personen beschränkt, die mit den Aufträgen beschäftigt sind, für die solche Daten verwendet werden sollen. Dabei muss jeder Benutzer sich mit personenspezifischen Zugangsdaten authentifizieren.

g. Organisatorische Regelungen zum Speichern von Daten

1. Mitarbeiter der netracom erhalten dabei auf Basis definierter Berechtigungen je Anwendung / System nur die notwendigen Berechtigungen. Der Zugriff in denen personenbezogene Daten gespeichert werden, ist auf die jeweiligen Personen beschränkt, die mit den Aufträgen beschäftigt sind, für die solche Daten verwendet werden sollen. Dabei muss jeder Benutzer sich mit personenspezifischen Zugangsdaten authentifizieren.

h. Zugriff auf und aus dem Wifi Netzwerk

1. Der Zugriff auf Netzwerkverzeichnisse oder Systeme, in denen personenbezogene Daten gespeichert werden, ist auf die jeweiligen Personen beschränkt, die mit den Aufträgen beschäftigt sind, für die solche Daten verwendet werden sollen. Dabei muss jeder Benutzer sich mit personenspezifischen Zugangsdaten authentifizieren. Die initiale Zugriffsmöglichkeit ist, wo immer dies aufgrund der Funktion des Systems und den Vorgaben des Kunden realisiert werden kann, immer auf das interne Netzwerk der netracom beschränkt.

Trennungskontrolle

1. netracom verarbeitet eigene personenbezogene Daten immer nur innerhalb der für die konkrete Aufgabe notwendigen Systeme und Prozesse. Im Rahmen der eigenen Verarbeitung von personenbezogenen Daten trennt netracom Test-Umgebungen von Produktiv-Umgebungen. Je nach erbrachter Leistung isoliert netracom Kundendaten entweder physisch (separate Hardware-Systeme, bspw. „Hosting dedizierter Server“) oder logisch. Eine logische Isolierung kann hier je nach erbrachter Leistung unterschiedlich realisiert werden („Virtuelle Server“, „Mandantenfähige Software“). Eine darüberhinausgehende Trennungskontrolle für die Speicherung und Verarbeitung von personenbezogenen Daten im Rahmen der Auftragsverarbeitung obliegt dem Auftraggeber.

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

Weitergabekontrolle

1. Personenbezogene Daten oder anderweitig vertrauliche Daten werden bei der Übertragung mindestens mittels einer Transportverschlüsselung verschlüsselt.

   Darüber hinaus empfiehlt netracom bei der Übertragung von personenbezogenen Daten im Kundenkontakt zusätzlich eine dateibasierte Verschlüsselung zu verwenden. So wird auch eine temporäre Ablage der Daten auf netracom oder Kundenseite abgesichert. Dies setzt jedoch die technische Fähigkeit des Kunden zur Annahme oder Übermittlung einer entsprechend verschlüsselten Datei voraus. Soweit netracom diese Möglichkeit mit dem Kunden feststellt, wird netracom eine solche mit dem Kunden abgestimmte Methode zur dateibasierten Verschlüsselung verwenden.

   Der Versand personenbezogener Daten erfolgt ausschließlich im gesetzlich vorgesehenen Rahmen. Mobile Datenträger mit personenbezogenen Daten werden nur in gesicherten Räumen gehalten, bei Nichtverwendung im Tresor. Daten, die für eine Auftragsdurchführung nicht mehr benötigt werden, wie z.B. gesperrte Daten, werden in einem separierten zugriffsgeschützten Speicherbereich abgelegt. Datenträger oder Hardware werden nur durch entsprechend verpflichtete und zertifizierte Unternehmen repariert oder entsorgt. Gleiches gilt für die Entsorgung von Daten auf Papier.

Eingabekontrolle

1. Nur ausgewählte Mitarbeiter können in einem Kundenprojekt auf die Systeme und Daten des Kunden zugreifen. Dabei werden nur Mitarbeiter ausgewählt, die auch für die Erbringung der vertraglich zugesicherten Leistung direkt notwendig sind. Die Legitimation der Mitarbeiter ergibt sich aus der Zuordnung zur Gruppe der für diesen Kunden zuständigen Mitarbeiter. Alle Mitarbeiter sind dabei auf die Vertraulichkeit und Einhaltung der gesetzlichen sowie internen Regelungen verpflichtet.

   Arbeiten an den Kundensystemen werden protokolliert. Wo technisch möglich erfolgt eine automatische Protokollierung aller Veränderungen und Aktionen. Darüber hinaus erfolgt eine manuelle Protokollierung der Mitarbeiter. Dies wird regelmäßig Stichprobenhaft überprüft.

   Die Standard-Arbeitsanweisung an Mitarbeiter ist keine personenbezogenen Daten der Kunden zu verändern oder zu manipulieren. Dies darf nur auf explizite Weisung des Kunden erfolgen. Davon ausgenommen sind Regelprozesse zur Verwaltung von Daten (Datensicherung, Löschung von Protokolldaten nach vertraglich festgelegter Aufbewahrungszeit etc.), die im Rahmen des Betriebes der Kundeninstan-

zen in Standard-Logdateien der eingesetzten Serversoftware anfallen und ebenfalls personenbezogene Daten enthalten können.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

1. netracom nutzt physisch voneinander unabhängige und räumlich getrennte Rechenzentren. Die Sicherstellung der Verfügbarkeit kundenspezifischer Daten erfolgt im Rahmen der vertraglich definierten Anforderungen. Für IT-Systeme und Daten der netracom, die zum Betrieb des Rechenzentrums und somit zur Sicherstellung der Verfügbarkeit von Kundensystemen und –daten ebenfalls notwendig sind, erfolgt eine tägliche Sicherung mit zusätzlicher Sicherung aller geänderten Daten nachdem Arbeiten an den netracom-Systemen durchgeführt wurden. Darüber hinaus werden die Storage-Systeme, auf denen Kundensysteme betrieben werden, standardmäßig mit fehlertoleranten RAID-Systeme vor Datenverlust geschützt. Hier kann es je nach vertraglicher Individualkonfiguration bei Kunden jedoch Abweichungen geben. Für vom Auftraggeber von Dritten gemietete EDV-Systeme oder vom Auftraggeber eingestellte EDV-Systeme ist der Auftraggeber verantwortlich.

   netracom überwacht die Verfügbarkeit jeglicher Systeme zum Betrieb der Rechenzentren. Darüber hinaus überwacht netracom im Standard auch die Verfügbarkeit von Kundensystemen. Der Umfang dieses Monitorings wird dabei im Rahmen der Vertragsgestaltung / Angebotsphase durch den Kunden festgelegt und kann auch in einer bestehenden Vertragsbeziehung jederzeit angepasst werden. Neben einer zeitnahen Alarmierung bei Ausfall oder Störung entsprechender Systeme oder Anwendungen kann netracom so auch die Verfügbarkeit eines Systems oder einer Anwendung nachweisen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und

Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

1. Im Rahmen des Datenschutz-Managements dokumentiert netracom jegliche Verfahren und Prozesse mit Verarbeitung von personenbezogenen Daten in unternehmensinternen Verfahrensverzeichnissen.

   Im Rahmen des Datenschutz-Managements nimmt netracom bei identifizierten Bedarf Datenschutz-

Folgenabschätzungen vor.

Darüber hinaus hat netracom alle Mitarbeiter zur Einhaltung der Vertraulichkeit und der Datenschutzgesetze schriftlich verpflichtet und erneuert diese Verpflichtung jährlich. Ebenso ist ein regelmäßiger Sensibilisierungs- und Schulungsprozess aller Mitarbeiter etabliert.

Incident-Response-Management

1. netracom betreibt einen dokumentierten Prozess zum Incident-Response-Management. Neben Eskalations- und Meldewegen beinhaltet dieser Prozess die Nachbetrachtung und Analyse und anschließende Optimierung auf Basis gewonnener Erkenntnisse.

   Zur Erkennung von Incidents setzt netracom sowohl gerätebasierte als auch netzwerkbasierte Lösungen ein (Intrusion-Detection, Virus- und Malware-Erkennung, Anti-Spam-Filter sowie Anomalie-Detektionen). Darüber hinaus überwacht netracom die Infrastruktur und Kundensysteme mit einer Monitoring-Lösung auf Störungen und Anomalien.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

1. netracom verfolgt das Prinzip der Datenminimierung. So werden nur Daten die für den jeweiligen Prozess / Kontext notwendig sind verarbeitet und gespeichert. Die Angemessenheit wird regelmäßig geprüft. Alle Berechtigungen werden nach einem „Need-to-have“-Prinzip vergeben und müssen begründet werden. Die Vergabe von Berechtigungen wird regelmäßig im internen Revisionsprozess überprüft und hinterfragt.

   Speicher- und Löschfristen werden aktiv definiert. Deren Einhaltung wird geprüft.

Auftragskontrolle (Outsourcing an Dritte)

1. netracom prüft (Unter-) Auftragnehmer im Rahmen des Auswahlprozesses sowie in der kontinuierlichen Zusammenarbeit auf angemessene Datenschutz- und IT-Sicherheitsprozesse. Hierzu nimmt netracom eine Sorgfaltsprüfung im Auswahlprozess eines (Unter-) Auftragnehmers vor.

   netracom verpflichtet jegliche (Unter-) Auftragnehmer vertraglich sowohl auf die geltenden Vertraulichkeitsverpflichtungen als auch auf die Einhaltung des Datenschutzes. Entsprechend wird für alle (Unter-) Auftragnehmer mit Bezug zu personenbezogenen Daten eine Auftragsvereinbarung geschlossen.