Datenschutzerklärung

INHALT

- Geltungsbereich der unterschiedlichen Datenschutzgesetze
- Erhebung, Verarbeitung und Nutzung von Bestandsdaten sowie Verkehrsdaten
- Weitergabe und die Sicherheit der personenbezogenen Daten
- Sicherheitsmaßnahmen nach §9 BDSG
- Personenbezogene Daten von Kunden unserer Kunden
- Weitere Informationen
- Änderung der Datenschutzhinweise
- Verantwortlichkeiten

UNTERNEHMENSVORSTELLUNG

Die netplace Telematic GmbH wurde 1997 gegründet und bietet als Internet Service Provider ein umfangreiches Produktportfolio an qualitativ hochwertigen Internet Dienstleistungen für Geschäftskunden.
Sicherheit und Qualität unter Einhaltung allgemein anerkannter technischer Standards und gesetzlichen Regelungen sind die wichtigsten Eckpfeiler unserer Arbeit, beginnend ab der Projektierung eines Services bis zum geregelten Betrieb.

Die wichtigsten Ziele unserer Qualitäts- und Sicherheitspolitik sind der Schutz von Informationen vor Bedrohungen bzgl. Vertraulichkeit, Integrität und Verfügbarkeit, die Minimierung von Geschäftsrisiken und die Ausfallsicherheit der von uns betreuten Systeme. Die konsequente Umsetzung der hierzu erforderlichen Maßnahmen bildet die Grundlage für Kundenzufriedenheit und sichert unseren geschäftlichen Erfolg.

netplace

Marsstr. 26, 80335 München **Tel.: (089) 55 18 05 10** **Fax: (089) 55 18 05 23** **WWW.NETPLACE.COM**

Datenschutzerklärung

Die Datenschutzerklärung gilt für die Firma **netplace Telematic GmbH**, nachfolgend kurz **netplace** genannt. Als Anbieter umfassender Internetdienstleistungen wissen wir, wie wichtig das Thema Datenschutz ist. Wir möchten Ihnen daher versichern, dass wir den Schutz Ihrer persönlichen Daten sehr ernst nehmen und auf die Einhaltung der gesetzlichen Vorschriften des Datenschutzes achten. Die rechtlichen Grundlagen finden sich im Bundesdatenschutzgesetz (BDSG), dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG).

Geltungsbereich der unterschiedlichen Datenschutzgesetze

- TRANSPORTDIENSTE

  Sind Dienste auf der reinen Transportebene (etwa E-Mail oder Hosting Transport und Internetzugänge z.B. DSL). Zu den hierfür maßgeblichen Vorschriften gehört insbesondere das Telekommunikationsgesetz TKG.
- TELEDIENSTE

  Dienste, die für eine individuelle Nutzung durch einen einzelnen Kunden bestimmt sind. Beispiele sind etwa die Bereitstellung von Serversystemen für Internetanwendungen oder Nutzung von Applikationskomponenten z.B. Datenbanken ohne redaktionelle Bearbeitung. Für diese Dienste richtet sich der Datenschutz vornehmlich nach dem Telemediengesetz TMG.
- OFFLINE-EBENE

  Die "Offline-Ebene" unterfällt dem Bundesdatenschutzgesetz, BDSG, oder den entsprechenden Landesdatenschutzgesetze. Ein Beispiel hierfür ist die Erfassung und Verarbeitung von personenbezogenen Daten zur Rechnungslegung.

Erhebung, Verarbeitung und Nutzung von Bestandsdaten

Im Rahmen der gesetzlichen Bestimmungen gemäß § 33 Abs. Bundesdatenschutzgesetz (BDSG) und § 13 Telemediengesetz (TMG) verarbeitet netplace die bei Vertragsschluss und während der Vertragslaufzeit erhobenen Daten, die zur gegenseitigen, ordnungsgemäßen Vertragserfüllung erforderlich sind. Zu diesen gehören:

- Vor- und Nachname
- der vollständigen IP-Adresse
- Anschrift, Straße und Ort
- Geburtsdatum
- Telefonnummern und/bzw. Email-Adressen
- Daten über die Zahlungsabwicklung (Bankverbindungen)
- Daten zu den beauftragten Dienstleistungen
- Kundennummer

Im Falle der Beendigung des Vertragsverhältnisses werden Ihre Bestandsdaten zum Ende des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres gelöscht. Die Löschung erfolgt nicht, wenn gesetzliche Vorschriften die Aufbewahrung der Daten verlangen oder ihre Einwilligung vorliegt. Freiwillig gemachte Angaben werden nach Beendigung des Zwecks, spätestens aber mit der Löschung aller Bestandsdaten, sowie bei Widerruf der Einwilligung gelöscht.

Wir weisen Sie darauf hin, dass zu einer Domain-Registrierung die Übermittlung bestimmter personenbezogener Daten, in der Regel Name und Anschrift, an die entsprechenden nationalen oder internationalen Registrierungsstellen und die Veröffentlichung in den von jedermann abrufbaren Whois-Datenbanken erforderlich ist.

Für die Registrierung einer ".de-Domain" zum Beispiel werden derzeit Namen und Anschriften des Domain-Inhabers, des administrativen und technischen Ansprechpartners sowie des Zonen-Verwalters und darüber hinaus Telefon- und Telefaxnummer sowie E-Mail-Adresse des technischen Ansprechpartners und des Zonenverwalters an die DENIC eG, Frankfurt/Main, übermittelt und in der DENIC-Datenbank unter http://www.denic.de im Internet veröffentlicht.

Erhebung, Verarbeitung und Nutzung von Verkehrsdaten

Verkehrsdaten sind die Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Bei Internetzugängen sind dies z.B. Anschluss und Benutzerkennung, Zugangskennwörter, Beginn und Ende der Verbindung, die IP-Adressen, Übertragungsprotokolle und das übertragene Datenvolumen.

Soweit die Verkehrsdaten für Abrechnungszwecke erforderlich sind (Abrechnungsdaten), werden sie längstens bis zu sechs Monate nach Versendung der Rechnung gespeichert, darüber hinaus nur, wenn und solange der Nutzer Einwendungen gegen die Rechnung erhebt oder die Rechnung trotz Zahlungsaufforderung nicht bezahlt. Werden die Daten zur Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen benötigt, sperren wir die Daten.

Soweit dies erforderlich ist, erheben und verwenden wir Ihre Bestands- und Verkehrsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an unseren Telekommunikationsanlagen und, soweit Anhaltspunkte bestehen, zum Aufdecken sowie Unterbinden von Missbrauch und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und –dienste.

Sofern auf das Internetportal der netplace Telematic GmbH zugegriffen wird, erfolgt die Speicherung eines Datensatzes auf dem Web-Server.

Der Datensatz besteht aus:

- der vollständigen IP-Adresse
- dem Zeitpunkt des Aufrufs
- der Methode des Aufrufs
- der aufgerufenen URL
- der verwendeten Version des HTTP-Protokolls
- dem Ergebniswert des Aufrufs
- der Größe des Aufrufs in KByte
- der Seite, die vor dem Aufruf dieser Seite aufgerufen wurde
- der verwendeten Programme (Browser und Betriebssystem)

Die IP-Adresse wird gemäß Telemediengesetz (TMG) anonymisiert und damit der Personenbezug gelöscht. Die Erstellung von personenbezogenen Nutzerprofilen ist damit ausgeschlossen.

Die aus den oben genannten Daten bestehenden, anonymisierten Datensätze werden ausschließlich zu statistischen Zwecken ausgewertet.

Weitergabe von Daten

Nach Maßgabe der hierfür geltenden Bestimmungen sind wir berechtigt, Auskunft an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfolgung zu erteilen.

Sicherheit der personenbezogenen Daten

Es liegt im Bestreben von netplace, alle erforderlichen Maßnahmen zu ergreifen, um die von Ihnen übermittelten personenbezogenen Daten zu schützen. netplace verwendet zum Schutz aller von Ihnen bereitgestellten personenbezogenen Daten branchenübliche physische und logische Zugriffskontrollmechanismen, die in Abhängigkeit von veränderten behördlichen Bestimmungen und dem Risikoumfeld angepasst werden.

Dies schließt Internet-Firewalls, Erkennung von unberechtigtem Eindringen, Virenschutz, Netzwerküberwachung und gegebenenfalls Secure Socket Layer-Verschlüsselung (SSL-Verschlüsselung) oder in ähnlicher Weise verschlüsselte Browser ein.

Beide Vertragsparteien werden Passwörter geheim halten und diese ändern, sobald die Vermutung besteht, dass unberechtigte Dritte Kenntnis von dem Passwort erhalten haben. Der Kunde wird netplace sofort unterrichten, wenn ein entsprechender Verdacht besteht. Gleiches gilt umgekehrt für netplace, wenn Änderungen an Passwörtern vorgenommen werden, die für den Kunden und dessen Tätigkeiten von Bedeutung sind. Die Übermittlung der neuen Passwörter erfolgt gemäß Absprache zwischen den Vertragsparteien ausschließlich an dazu besonders autorisierte Personen des jeweiligen Vertragspartners.

Vorkehrungen und Maßnahmen zum Schutz personenbezogener Daten

Zum Schutz personenbezogener Daten vor Missbrauch und Verlust hat netplace die unter dem Punkt „Sicherheitsmaßnahmen“ genannten technischen und organisatorischen Vorkehrungen getroffen. Diese Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Beabsichtigte wesentliche Änderungen (z.B. wesentliche Änderung von Verschlüsselungsverfahren oder Anmeldeprozeduren) werden dokumentieren und den Kunden mitgeteilt.

netplace bestätigt, dass die für die Durchführung des Auftrags eingesetzten Personen gemäß § 5 BDSG (Datengeheimnis) schriftlich verpflichtet und in die Schutzbestimmungen des BDSG sowie weiterer maßgeblicher Bestimmungen zum Datenschutz (z.B. § 88 TKG sowie §§ 203, 206 StGB) eingewiesen worden sind.

netplace vergibt Zugriffsberechtigungen nur an Personen, die mit der Durchführung des Auftrags befasst sind. Die Berechtigungen sind in dem für die Erfüllung der jeweiligen Aufgaben erforderlichen Umfang zu vergeben.

Während der Entwicklung von Software werden grundsätzlich keine personenbezogenen Daten, sondern lediglich anonymisierte Original- oder fiktive Testdaten verwendet.

netplace wird personenbezogene Daten nach Abschluss der Arbeiten vollständig datenschutzgerecht löschen (einschließlich der verfahrens- oder sicherheitstechnisch notwendigen Kopien) oder an den Kunden zurückgeben. Das gleiche gilt auch für Test- und Ausschussmaterial, das bis zur Löschung oder Rückgabe unter datenschutzgerechtem Verschluss gehalten wird. Gesetzliche Aufbewahrungspflichten insbesondere nach AO und HGB bleiben hiervon unberührt. Vertragsbezogene Daten (z.B. Ansprechpartner), die zur Sicherung von Beweisinteressen erforderlich sind, werden bis zum Ablauf der regelmäßigen Verjährungsfrist aufbewahrt. Die Löschung wird auf Anforderung schriftlich bestätigt.

Sicherheitsmaßnahmen nach § 9 BDSG

Zutrittskontrolle

Die Betriebsräume der netplace gliedern sich in Büro- und Technikbereiche, wobei die Datacenter besondere Schutzzonen sind, für die spezielle Zutrittsregelungen gelten. Diese Regelungen und verschiedene technische Maßnahmen haben das Ziel, Unbefugten den Zutritt zu den Systemen in den Datacentern zu verwehren und den Zugang zu Informationen und Dokumenten zu kontrollieren.

Der Zugang zu den Bereichen ist durch ein elektronisches Zutrittskontrollsystem geschützt, um sicherzustellen, dass nur autorisierten Mitarbeitern Zutritt

gewährt wird. Innerhalb der Geschäftszeiten ist eine Authentifizierung mit der persönlichen Chipkarte erforderlich. Jeder versuchte Zutritt wird vom Kontrollsystem protokolliert. Die Zutrittsprotokolle werden vom Sicherheitsbeauftragten auf Anfrage generiert und dem ISMT (Informationssicherheits-Managementteam) zur Prüfung bereitgestellt.

Alle Regelungen und Verfahren der Zutrittskontrolle sind im ISMS der netplace (Informationssicherheits-Managementsystem) definiert und vom TÜV-Nord nach ISO-27001 zertifiziert. Neben den internen Audits finden jährliche Überwachungsaudits durch die Zertifizierungsstelle statt.

Zugangskontrolle

Der Zugang zu Informationen und Geschäftsprozessen wird auf der Basis von Geschäfts- und Sicherheitsanforderungen kontrolliert. Dabei sind spezifische Regelungen für die Informationsverbreitung und Zugriffsberechtigung berücksichtigt. Geschäftsanforderungen an die Zugangskontrolle sind definiert und dokumentiert. Regeln und Rechte der Zugangskontrolle für jeden Benutzer oder jede Gruppe von Benutzern (Rollen) sind in einer Erklärung der Zugangspolitik unmissverständlich aufgeführt. Als Grundprinzip der Zugangskontrolle und Rechtevergabe gilt, dass der Zugang zu allen Systemen, Diensten und Informationen verboten ist, solange er nicht einzelnen Benutzern oder Benutzergruppen ausdrücklich erlaubt wird.

Die Regelungen und Verfahren der Zutrittskontrolle sind ebenfalls im ISMS dokumentiert und sind Bestandteil interner Audits und der jährlichen Überwachungsaudits durch die Zertifizierungsstelle.

Zugriffskontrolle

Im Rahmen der Zugriffskontrolle ist ein Rechtemanagement installiert, dass Pflichten, Berechtigungen und Verantwortungsbereiche regelt, um die Möglichkeit einer unbefugten oder vorsätzlichen Veränderung oder eines Missbrauchs von Systemen und Daten zu reduzieren.
Das Berechtigungskonzept umfasst unterschiedliche Ebenen der Informationssicherheit, wie Benutzer, Rollen und Berechtigungen für den Zugriff auf Dokumente, Knowledge Base, Prozesse und Systeme.

Im Prinzip gilt der Grundsatz, dass Berechtigungen ausschließlich für Rollen und so restriktiv wie möglich konfiguriert werden (Need-to-know-Prinzip).

Die Zugriffskontrolle ist ebenfalls Bestandteil des ISMS und unterliegt somit den internen Audits durch das ISMT und der Zertifizierungsstelle.

Weitergabekontrolle

Im Rahmen der ISMS sind Regelungen und Verfahren für den Umgang mit sensiblen und klassifizierten Informationen festgelegt.

Dies umfasst u.a.

- Umgang mit klassifizierter Information
- Verfahren und Regeln zum Schutz von Informationen, die zwischen Geschäftsanwendungen übertragen werden
- Transport physischer Medien, Entsorgung, Vernichtung und Weiterverwendung
- Messaging und Kryptographie

Eingabekontrolle

Ziel der Verfahren zur Eingabekontrolle ist es, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind. Die im ISMS festgelegten Richtlinien definieren die Verfahren zur:

- Überprüfung und Kontrolle von Ein-/Ausgabedaten
- Kontrolle der internen Verarbeitung
- Integrität von Daten inkl. Protokollierung von Veränderungen
- Gesetzeskonforme Einhaltung von Aufbewahrungsfristen

Auftragskontrolle

Die in der ISMS Richtlinie „Dienstleistungen von Dritten“ regelt, ob und wie personenbezogene Daten im Auftrag verarbeitet werden dürfen. Die Einhaltung der Regelungen wird in internen Audits und den jährlichen Überwachungsaudits geprüft.

Verfügbarkeitskontrolle

Als Maßgabe für die Verfügbarkeit der IT-Infrastruktur gilt die Verfügbarkeitsklasse VK3 gemäß Klassifizierung des Bundesamts für Sicherheit in der Informationstechnik BSI. Die Maßnahmen zum Schutz gegen zufällige Zerstörung oder Verlust von Daten sind in folgenden ISMS Richtlinien festgelegt:

- Platzierung und Schutz von Betriebsmitteln in speziellen Sicherheitszonen
- Anforderungen und Regelungen für unterstützende Versorgungseinrichtungen, wie Klimaanlagen, USV und Stromersatzanlage (Dieselgenerator)
- Anforderungen an zentrale Infrastruktur-Komponenten
- Regelungen und Vorgaben bzgl. Redundanz und Sicherheit
- Richtlinien und Verfahren zur Netzwerk und Host Security
- Backup und Wiederherstellungsprozeduren.
- Business Continuity Framework und Desaster Recovery Prozeduren

Trennungskontrolle

Im Rahmen der Trennungskontrolle sind folgende ISMS Richtlinien definiert:

- Vorgaben an die Systementwicklung und –beschaffung
- Richtlinie zur Segmentierung er IT-Infrastruktur
- Abnahme- und Freigabeverfahren
- Richtlinie für die Geschäftsinformationssysteme, u.a. Mandantenfähigkeit

Vorabkontrolle

Vor dem Einsatz oder der wesentlichen Änderung eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten führt netplace eine Vorabkontrolle nach § 7 Abs. 6 HDSG durch. Um zu untersuchen, ob durch die beabsichtigte automatisierte Datenverarbeitung das in § 1 Abs. 1 Nr. 1 HDSG beschriebene Recht der informationellen Selbstbestimmung gefährdet wird. Zusätzlich werden Fälle getrennt betrachtet, die von diesem Schema voraussichtlich abweichen. Dies sind z.B.

- Telefonanlage (welche Daten sind dort und wozu gespeichert)
- Entwicklung eigener Softwarekomponenten für die Verarbeitung personenbezogener Daten

Personenbezogene Daten von Kunden unserer Kunden

Wenn wir unseren Kunden Dienstleistungen zur Verfügung stellen, verarbeiten wir in manchen Fällen personenbezogene Daten ihrer Kunden („Kundendaten“) in deren Auftrag. In diesen Fällen liegt die Entscheidung über den Zweck der Verarbeitung der Kundendaten weniger bei uns als bei unseren Kunden.

Weitere Informationen über die Verwendung und den Schutz sowie die Zugangs- und Änderungsmöglichkeiten der Kundendaten finden Sie in der Datenschutzerklärung des Kunden von netplace, dem Sie Ihre personenbezogenen Daten übermittelt haben.

Unter Umständen verpflichten entsprechende Gesetze Kunden dazu, von uns die Einhaltung derselben Sicherheitsrichtlinien zu verlangen, denen sie durch diese Gesetze unterliegen.

Weitere Informationen

netplace verpflichtet sich, dem Kunden auf Verlangen jederzeit über den gespeicherten Datenbestand, soweit er ihn betrifft, vollständig Auskunft zu erteilen. netplace wird weder diese Daten noch den Inhalt privater Nachrichten des Kunden ohne dessen Einverständnis an Dritte weiterleiten. Dies gilt nur insoweit nicht, als netplace gesetzlich verpflichtet ist, Dritten, insbesondere staatlichen Stellen, solche Daten zu offenbaren oder soweit international anerkannte technische Normen dies vorsehen und der Kunde nicht widerspricht.

netplace weist den Kunden ausdrücklich darauf hin, dass der Datenschutz für Datenübertragungen in offenen Netzen, wie dem Internet, nach dem derzeitigen Stand der Technik nicht umfassend gewährleistet werden kann. Der Kunde weiß, dass netplace das auf einem Webserver gespeicherte Seitenangebot und unter Umständen auch weitere dort abgelegte Daten des Kunden aus technischer Sicht jederzeit einsehen kann. Auch andere Teilnehmer am Internet sind unter Umständen technisch in der Lage, unbefugt in die Netzsicherheit einzugreifen und den Nachrichtenverkehr zu kontrollieren. Für die Sicherheit der von ihm ins Internet übermittelten Daten trägt der Kunde daher selbst Sorge.

Beide Vertragspartner stehen dafür ein, dass das jeweils mit der Vertragsabwicklung befasste Personal die Datenschutzbestimmungen kennt und beachtet.

Änderung der Datenschutzhinweise

Bitte beachten Sie, dass diese Datenschutzhinweise jederzeit unter Beachtung der geltenden Datenschutz Vorschriften geändert werden können. Es gilt immer die zum Zeitpunkt Ihres Besuchs abrufbare Fassung.

Letzte Änderung: 13.02.2014

Verantwortlichkeiten

Rolle	Kontakt
Geschäftsführer	Maximilian Fruth max.fruth@netplace.com
Beauftragter für Informationssicherheit	Maximilian Fruth
Information Security Officer	Tobias Maier tobias.maier@netplace.com
Beauftragter für Datenschutz	Robert Grube robert.grube@netplace.com

Postalischer Kontakt

netplace Telematic GmbH
Datenschutzbeauftragter
Marsstraße 26
80335 München