INHALTSVERZEICHNIS

1. GRUNDSÄTZE

Die Mitarbeiter und Mitarbeiterinnen der InterNetX GmbH und ihrer Tochterunternehmen erachten Informationen und Daten, insbesondere wenn sie personenbezogen sind, als kritische Werte für die Unternehmensgruppe. Die unternehmens- und personenbezogenen Daten sowie die Systeme, die diese Informationen und Daten verarbeiten, sind vor Verlust, Zerstörung, Nicht-Verfügbarkeit, Diebstahl, unberechtigten Veränderungen, Informationsabfluss, Verfälschung beweiserheblicher Daten und unberechtigten Zugriff zu schützen.

Die Mitarbeiter sind hinsichtlich Datenschutz und ihrer Pflichten zum ordnungsgemäßen Umgang mit Daten und DV-Technik informiert und entsprechend verpflichtet (Datengeheimnis, Betriebs- und Geschäftsgeheimnisse). Sie werden regelmäßig über die strafrechtlichen Bestimmungen informiert, die für den unrechten Umgang mit Daten gelten.

2. MAßNAHMEN NACH ART. 32 DSGVO

Folgende Maßnahmen werden ergriffen, um ein dem Risiko angemessenes Schutzniveau i.S.d. Art. 32 DSGVO zu gewährleisten:

2.1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1.1 Zutrittskontrolle

Datacenter München
Die Räumlichkeiten des Rechenzentrums in München sind hochgesichert. Bevor Zutritt gestattet wird, haben sich Besucher des Rechenzentrums, die sich vorher anzumelden haben, einer Personenkontrolle unter Vorlage eines gültigen Personalausweises zu unterziehen. Neue Mitarbeiter haben sich unter Vorlage einer entsprechenden Autorisierung des Rechenzentrumleiters schriftlich zu registrieren.

Jeder Besucher wird von mindestens einem Mitarbeiter begleitet. Alle Rechenzentrumstüren sind biometrisch gesichert und können daher nur von registrierten Mitarbeitern per Fingerabdruck geöffnet werden. Des Weiteren werden alle Türen und Gänge im technischen Bereich sowie die Serverräume videoüberwacht. Das Rechenzentrum ist an 365 Tagen im Jahr rund um die Uhr besetzt. Zudem ist das gesamte Rechenzentrum gem. ISO 27001 zertifiziert.

Headquarter Regensburg
Die Zugänge zu den Büroräumen der Firmenzentrale in Regensburg sind ebenfalls durch ein Zutrittssystem gesichert. Die Zutrittskontrolle erfolgt über Transponder, die nur an zutrittsberechtigte Mitarbeiter vergeben werden. Die Vergabe der Transponder wird protokolliert. Scheidet ein Mitarbeiter aus, ist der Transponder am letzten Arbeitstag zurückzugeben. Erfolgt die Rückgabe nicht rechtzeitig, wird der Transponder deaktiviert, so dass mit diesem kein Zutrittt mehr möglich ist. Die Zutrittskontrolle wird über verschiedene Berechtigungsstufen kontrolliert und überwacht; die Mitarbeiter haben generell nur an den regulären Arbeitstagen und während der Geschäftszeiten Zutritt in die für sie freigegebenen Räumlichkeiten. Änderungen von Berechtigungsstufen für einzelne Mitarbeiter können nur durch die jeweils besonders autorisierten Personen im Vier-Augen-Prinzip beantragt werden. Änderungen und Neuvergaben bzgl. der Zutrittsberechtigungen werden protokolliert und regelmäßig überprüft.

Besucher erhalten ausschließlich beim ausgeschilderten Empfang Zutritt, nachdem sie sich an der Gegensprechanlage (mit Videokamera) zu erkennen gaben. Besucher erhalten grundsätzlich keinen eigenen Transponder. Um in die verschiedenen Abteilungen zu gelangen, ist daher die persönliche Begleitung durch einen Mitarbeiter mit entsprechender Zutrittsberechtigung erforderlich.

Die Eingänge zu den jeweiligen Abteilungen sowie wichtige Räumlichkeiten der Infrastruktur, wie z.B. Serverräume, werden zusätzlich mit Kameras überwacht, deren Aufnahmen über einen Bewegungssensor gestartet und räumlich getrennt gespeichert werden.

2.1.2 Zugangskontrolle
Um eine unbefugte Systembenutzung auszuschließen, wird der Zugang zu Datenverarbeitungssystemen durch verschiedene Vorkehrungen eingeschränkt und ist somit nur autorisierten Mitarbeitern möglich. Obligatorisch ist ein voreingestellter Passwortschutz an Servern, Workstations, Notebooks, mobilen Endgeräten und Applikations-Software. Als weitere Vorkehrung sind alle Server und Workstations mittels Portsecurity an den Switch-Port angeschlossen, wodurch ein unberechtigter Zugriff durch ein fremdes, nicht freigegebenes Endgerät auf das Firmennetzwerk unterbunden wird.

Die mobilen Endgeräte wie Notebooks und Smartphones verfügen zusätzlich zum Passwortschutz über weitere Vorkehrungen wie z.B. automatisches Sperren, Fernzugriff und Lokalisierung im Falle eines Diebstahls. Durch den Fernzugriff ist es möglich, die kompletten Daten zu löschen. Die Datenträger der Notebooks sind zusätzlich mit einer Verschlüsselung nach aktuellen Sicherheitsstandards verschlüsselt, um einen unberechtigten Zugriff auf die Daten zu verhindern.

Die Passwortnutzung, Anmeldung und der VPN-Zugriff werden zusätzlich protokolliert. Die Datenträgerarchive werden in einem Schutzbereich (teilweise außer Haus) betrieben und sind nur autorisiertem Personal zugänglich. Vor unberechtigten System- bzw. Datenzugriff schützen Anti-Virensoftware und Firewalls, welche ständig aktualisiert werden.

Es wird jedoch darauf hingewiesen, dass für den Zugangsschutz datenverarbeitender Systeme, welche Kunden / Auftraggeber von InterNetX mieten, grundsätzlich der jeweilige Kunde / Auftraggeber selbst zuständig ist. Es liegt in seiner Verantwortung, diese vor unbefugtem Zugriff Dritter zu schützen, Passwörter geheim zu halten etc.

2.1.3 Zugriffskontrolle

Die Zugriffskontrolle wird durch ein entsprechendes Berechtigungskonzept für sämtliche Server-Systeme der InterNetX GmbH gewährleistet. Hierbei werden mitarbeiterindividuell die Benutzerberechtigungen festgelegt, durch die Geschäftsleitung freigegeben und systemseitig hinterlegt. Die Rechtevergabe erfolgt nur im jeweils erforderlichen Rahmen. Bei Austritt eines Mitarbeiters werden unverzüglich dessen Zugangsberechtigungen entzogen bzw. gelöscht.

2.1.4 Trennungskontrolle

Personenbezogene Daten werden getrennt geführt und bereit gestellt. Im Web-Frontend werden nur relevante Daten dargestellt. So werden in Anwendungen, die Kunden / Auftraggebern zugänglich sind, nur diejenigen Informationen bereitgestellt, welche für die konkreten Prozesse zweckdienlich sind. Abrechnungsrelevante Daten sind nur im Backend verfügbar, dies auf getrennten Systemen in unterschiedlichen Segmenten.

Gesonderte Testumgebungen arbeiten mit fingierten Datensätzen und sind von produktiven Umgebungen getrennt. Zudem sind sämtliche unternehmenseigenen Systeme mandantenfähig konzipiert.

2.1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Wo möglich und technisch sinnvoll, werden personenbezogene Daten pseudonymisiert. So werden beispielsweise Kontaktdatensätze, die ein Kunde / Auftraggeber zur Nutzung für in seinem Account befindliche Domains hinterlegt, in sog. Handle-IDs umgewandelt. Hierdurch können die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden. Die zusätzlichen Informationen, um die Datensätze wieder identifizierbar zu machen, werden getrennt gespeichert.

Weiterhin werden im Rahmen eines Privacy Service bei Domainregistrierungen Pseudonymisierungsdienste angeboten, die der Auftraggeber für sich und seine Kunden nutzen kann.

2.2. Integrität

2.2.1 Weitergabekontrolle

Eine Weitergabe der verarbeiteten Daten ist an die in den Verfahrensbeschreibungen angegebenen Stellen vorgesehen. Diese Übertragung findet automatisiert, aber auch manuell und nur im Rahmen des jeweiligen Auftrages statt.

Zu vernichtende Drucke werden einer datenschutzgerechten Vernichtung zugeführt. Zur Vernichtung einzelner Dokumente ist ein Aktenvernichter installiert. Elektronische Datenträger werden durch mehrfaches Überschreiben gelöscht und konform zur DIN 66399-2 vernichtet, sodass keine Daten rekonstruiert werden können.

Datentransfers erfolgen nur im Rahmen der gesetzlichen Regelungen. Insbesondere findet jedwede elektronische Kommunikation ausschließlich auf verschlüsseltem und gesichertem Wege nach aktuellem Stand der Technik statt.

2.2.2 Eingabekontrolle

Änderungen personenbezogener Daten werden zentral protokolliert und können nachträglich abgerufen werden. Zudem werden Änderungen an Anwendungen und Systemen lokal und remote protokolliert. Dabei ist der Zugriff auf das zentrale Protokollierungssystem stark restriktiv. Bezüglich sämtlicher Anwendungen und Systeme findet ein Monitoring statt, bei etwaigen Störungen und Veränderungen werden Benachrichtigungen an Mitarbeiter mit Sicherheitsfreigabe verschickt.

2.3. Verfügbarkeit und Belastbarkeit/Resilienz (Art. 32 Abs. 1 lit. b DSGVO)

Zum Schutz vor Datenverlust sind alle Server-Systeme mit einer unterbrechungsfreien Stromversorgung (USV) ausgerüstet, die bei länger andauernden Stromausfällen das System automatisch und kontrolliert herunterfährt. Des Weiteren sind die Festplatten aller Workstations verschlüsselt und zum Schutz vor Diebstahl mit Kensington-Lock gesichert.

Jedes System wird mit einer Firewall betrieben, welche ausschließlich legitime Verbindungen zulässt. Zentrale Firewalls im Netzwerk sorgen für zusätzlichen Schutz vor Viren, Trojanern und weiterer Schadsoftware. Durch die Kombination von zentralen und dezentralen Firewalls als auch AntiViren Software wird ein Höchstmaß an Sicherheit erzielt.

Storages und zentrale Datenspeicher verfügen ebenfalls über AntiViren Software und unterliegen strengen internen Vorgaben bzgl. Nutzung und Sicherung. Alle Storages, Server und Systeme werden mindestens täglich gesichert. Zusätzliche standortübergreifende Backups werden in verschlüsselter Form dezentral (off-site) gespeichert. Durch den Einsatz von Snapshots können strategisch wichtige Systeme und Anwendungen innerhalb kürzester Zeit auch im Worst-Case-Szenario (disaster recovery) wiederhergestellt werden.

Für regelmäßige Backups seiner Server ist der jeweilige Kunde selbst verantwortlich, wenn er nicht ausdrücklich Backup-Leistungen in Auftrag gegeben oder einen Managed Server gebucht hat, der diese Leistungen beinhaltet.

2.4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

2.4.1 Datenschutzmanagement

Das Datenschutz-Management (DSMS) hat das Ziel, die Eintrittswahrscheinlichkeit für Datenpannen oder Datenschutzverstöße zu verringern und im Falle eines Eintritts den Schaden und das Risiko für die betroffenen Personen zu begrenzen. Dazu ist ein Datenschutz-Management bzw. Incident Management, konform der ISO/IEC 27001:2013, etabliert, welches nach dem PDCA-Prinzip arbeitet. Es finden in regelmäßigen Abständen Reviews statt, wobei Risikobewertungen durchgeführt und Gefährdungs-Trends abgeleitet werden, um entsprechende Maßnahmen zu ergreifen und eine ständige Weiterentwicklung des Systems zu gewährleisten.

2.4.2 Datenschutzfreundliche Voreinstellungen

Nach internen Vorgaben werden bei der Entwicklung eines jeden neuen Produkts oder Änderung eines bestehenden darauf geachtet, dass ausschließlich diejenigen Daten erhoben werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Gleiches gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. In regelmäßigen Abständen werden bestehende Verarbeitungen hinsichtlich Datenminimierung überdacht und ggf. optimiert.

2.4.3 Auftragskontrolle

Eine Auftragskontrolle beim Auftragnehmer erfolgt, soweit dies für die Auftragsdurchführung erforderlich ist. Auftragsverarbeitungen i.S.d. Art. 28 DSGVO sind jedoch nicht die vertraglichen Hauptleistungspflichten. Insbesondere hat InterNetX grundsätzlich weder Kenntnis noch Einfluss darauf, ob personenbezogene oder sonstige sensible Daten auf den Kundensystemen gespeichert werden. Sofern InterNetX jedoch beispielsweise im Rahmen von Supportleistungen oder Wartungen eine Zugriffsmöglichkeit auf bestimmte Kundensysteme erhält, wird dies automatisch protokolliert.