Vertrag

über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Auftrag gemäß § 11 Bundesdatenschutzgesetz

§ 1 Vertragsgegenstand

Die Parteien haben einen Vertrag geschlossen, nach dem IdentPro dem „Kunden“ Speicherkapazitäten und weitere einzeln bezeichnete Hosting-Leistungen gegen Entgelt zur Verfügung stellt (nachfolgend „Nutzervereinbarung“ genannt). Im Rahmen der „Nutzervereinbarung“ ist es erforderlich, dass IdentPro mit personenbezogenen Daten umgeht, für die der „Kunde“ als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „Kunden-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit „Kunden-Daten“ zur Durchführung der „Nutzervereinbarung“.

§ 2 Art, Umfang, Zweck und Laufzeit der Auftragsdatenverarbeitung

1) IdentPro erhebt, verarbeitet und nutzt die „Kunden-Daten“ im Auftrag und nach Weisung des „Kunden“ i.S.v. § 11 BDSG (Auftragsdatenverarbeitung). Der „Kunde“ bleibt im datenschutzrechtlichen Sinn verantwortliche Stelle („Herr der Daten“).
2) Die Erhebung, Verarbeitung und Nutzung der „Kunden-Daten“ im Rahmen der Auftragsdatenverarbeitung erfolgt entsprechend den in **Anlage 1** zu diesem Vertrag enthaltenen Festlegungen zu Art, Umfang und Zweck der Datenverarbeitung. Sie bezieht sich auf die in **Anlage 1** festgelegte Art der „Kunden-Daten“ und den dort bestimmten Kreis der Betroffenen.
3) IdentPro darf die „Kunden-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. In jedem Fall darf IdentPro die „Kunden-Daten“ anonymisieren und in anonymisierter Form für eigene Zwecke verarbeiten und nutzen.
4) Die Erhebung, Verarbeitung und Nutzung der „Kunden-Daten“ findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. „Kunden-Daten“ werden, wenn nicht am Sitz der IdentPro selbst, insbesondere in einem in den Niederlanden belegenen Rechenzentrum sowie in einem Backup-Rechenzentrum in der Republik Irland statt.
5) Unabhängig davon, dass eine Erhebung, Verarbeitung oder Nutzung von „Kunden-Daten“ außerhalb des EWR möglicherweise nicht der Privilegierung des § 11 BDSG unterfällt, ist es IdentPro gestattet, „Kunden-Daten“ unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den „Kunde“ vorab über den Ort der Datenverarbeitung informiert und ihm die Einhaltung der Sicherheitsmaßnahmen gemäß § 6 dieses Vertrags in geeigneter Form nachweist.
6) Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung der „Nutzervereinbarung“. Eine Kündigung der „Nutzervereinbarung“ bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

§ 3 Weisungsbefugnisse des „Kunden“

1) IdentPro verwendet die „Kunden-Daten“ ausschließlich in Übereinstimmung mit den Weisungen des „Kunden“, wie sie abschließend in den Bestimmungen dieses Vertrags Ausdruck finden. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des in der „Nutzervereinbarung“ festgelegten Änderungsverfahrens, in dem auch die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den „Kunden“ zu regeln ist.
2) Ist IdentPro der Ansicht, dass eine zulässige Einzelweisung gegen geltendes Datenschutzrecht verstößt, wird sie den „Kunden“ möglichst zeitnah darauf hinweisen. Außerdem ist IdentPro berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den „Kunden“ auszusetzen.

§ 4 Pflichten des „Kunden“

1) Der „Kunde“ ist für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der „Kunden-Daten“ sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Sollten Dritte gegen IdentPro aufgrund der Erhebung, Verarbeitung oder Nutzung von

„Kunden-Daten“ Ansprüche geltend machen, wird der „Kunde“ IdentPro von allen solchen Ansprüchen auf erstes Anfordern freistellen.

2) Der „Kunde“ ist Eigentümer der „Kunden-Daten“ und Inhaber aller etwaigen Rechte, die die „Kunden-Daten“ betreffen.
3) Dem „Kunden“ obliegt es, IdentPro die „Kunden-Daten“ rechtzeitig zur Leistungserbringung nach der „Nutzervereinbarung“ zur Verfügung zu stellen, und er ist verantwortlich für die Qualität der „Kunden-Daten“. Der „Kunde“ hat IdentPro unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse der IdentPro Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

§ 5 Pflichten der IdentPro

1) IdentPro stellt sicher und kontrolliert regelmäßig, dass die Datenverarbeitung und -nutzung im Rahmen der Leistungserbringung nach der „Nutzervereinbarung“ in ihrem Verantwortungsbereich, der Unterauftragnehmer nach § 9 dieses Vertrags einschließt, in Übereinstimmung mit den Bestimmungen dieses Vertrags erfolgt.
2) IdentPro darf ohne vorherige Zustimmung durch den „Kunden“ im Rahmen der Auftragsdatenverarbeitung keine Kopien oder Duplikate der „Kunden-Daten“ anfertigen. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß der „Nutzervereinbarung“ (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
3) IdentPro unterstützt den „Kunden“ bei Kontrollen durch die Aufsichtsbehörde im Rahmen des Zumutbaren und Erforderlichen, soweit diese Kontrollen die Datenverarbeitung durch IdentPro betreffen.
4) IdentPro hat dem „Kunden“ auf Anforderung eine Übersicht über die in § 4e Satz 1 BDSG genannten Angaben sowie über die zugriffsberechtigten Personen zur Verfügung zu stellen (§ 4g Abs. 2 Satz 1 BDSG)
5) IdentPro hat die bei der Verarbeitung von „Kunden-Daten“ beschäftigten Personen gemäß § 5 BDSG schriftlich auf das Datengeheimnis zu verpflichten.
6) IdentPro ist verpflichtet, einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten nach § 4f BDSG zu bestellen, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind.
7) IdentPro unterliegt der behördlichen Aufsicht nach § 38 BDSG sowie den Bußgeld- und Strafvorschriften in § 43 Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 BDSG sowie in § 44 BDSG.

§ 6 Technische und organisatorische Maßnahmen

1) IdentPro hat vor Beginn der Verarbeitung der „Kunden-Daten“ die in **Anlage 2** dieses Vertrags aufgelisteten technischen und organisatorischen Maßnahmen zu implementieren und während des Vertrags aufrechtzuerhalten.
2) Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, ist es IdentPro gestattet, alternative und adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in **Anlage 2** festgelegten Maßnahmen nicht unterschritten wird. IdentPro wird solche Änderungen dokumentieren. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen schriftlichen Zustimmung des „Kunden“ und sind von IdentPro zu dokumentieren und dem „Kunde“ auf Anforderung zur Verfügung zu stellen.

§ 7 Mitzuteilende Verstöße der IdentPro

1) IdentPro informiert den „Kunden“ zeitnah, wenn sie feststellt, dass sie oder ein Mitarbeiter bei der Verarbeitung von „Kunden-Daten“ gegen datenschutzrechtliche Vorschriften oder gegen Festlegungen aus diesem Vertrag verstoßen haben, sofern deshalb die Gefahr besteht, dass „Kunden-Daten“ unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.
2) Soweit den „Kunden“ aufgrund eines Vorkommnisses nach § 7 Abs. 1 gesetzliche Informationspflichten wegen einer unrechtmäßigen Kenntniserlangung von „Kunden-Daten“ (insbesondere nach § 42a BDSG) treffen, hat IdentPro den „Kunden“ bei der Erfüllung der Informationspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der IdentPro hierdurch entstehenden, nachzuweisenden Aufwände und Kosten zu unterstützen.

§ 8 Kontrollrechte des „Kunden“

1) Der „Kunde“ ist berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 8:00 bis 17:00 Uhr) auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen der IdentPro deren Geschäftsräume, in denen „Kunden-Daten“ verarbeitet werden, zu betreten, um sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** zu diesem Vertrag zu überzeugen. Der „Kunde“ erkennt an, dass wegen der besonderen Sensibilität des von der IdentPro im Rahmen eines Unterauftragsverhältnisses nach § 9 genutzten Rechenzentren ein Betretungsrecht bezüglich dieser Rechenzentren ausgeschlossen ist. Der „Kunde“ hat allerdings das Recht, von IdentPro eine Bestätigung über die ordnungsgemäße Datenverarbeitung und die Einhaltung der technischen und organisatorischen Maßnahmen durch deren Unterauftragnehmer zu verlangen (z.B. durch aktuelle Zertifizierungen, Auditierungsergebnisse o.ä.); Einzelheiten hierzu sind in § 8 Abs. 7 geregelt.
2) IdentPro gewährt dem „Kunden“ die zur Durchführung der Kontrollen nach § 8 Abs. 1 erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte. § 8 Abs. 1 Satz 2 gilt entsprechend.

3) IdentPro ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des „Kunden", Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte der IdentPro sind oder wenn IdentPro durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der „Kunde" ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden der IdentPro, zu Informationen hinsichtlich Kosten – es sei denn, dass diese die Basis des erstattungsfähigen oder durchlaufenden Aufwandes darstellen – zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten der IdentPro, die nicht unmittelbar relevant für die vereinbarten Kontrollzwecke sind, zu erhalten.
4) Der „Kunde" hat IdentPro rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der „Kunde" darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des „Kunden", weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.
5) IdentPro erhält vom „Kunden" eine aufwandsbezogene Entschädigung für ihren im Rahmen dieser Kontrollen anfallenden Aufwand gemäß den jeweils gültigen Stunden- und Tagessätzen der IdentPro.
6) Beauftragt der „Kunde" einen Dritten mit der Durchführung der Kontrolle, hat der „Kunde" den Dritten schriftlich ebenso zu verpflichten, wie auch der „Kunde" aufgrund von dieser § 8 dieses Vertrags gegenüber der IdentPro verpflichtet ist. Zudem hat der „Kunde" den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen der IdentPro hat der „Kunde" dieser die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der „Kunde" darf keinen Konkurrenten der IdentPro mit der Kontrolle beauftragen.
7) Nach Wahl der IdentPro kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsberichts") erbracht werden, wenn der Prüfungsbericht es dem „Kunden" in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** zu diesem Vertrag zu überzeugen.

§ 9 Unterauftragsverhältnisse

1) IdentPro darf Unterauftragsverhältnisse hinsichtlich der Verarbeitung oder Nutzung von „Kunden-Daten" nur nach vorheriger schriftlicher Zustimmung des „Kunden" begründen. Der „Kunde" erklärt sich damit einverstanden, dass IdentPro für die Erbringung der Leistungen aus der Nutzervereinbarung ein Unterauftragsverhältnis mit der Microsoft Inc. geschlossen hat. Die „Kunden-Daten" werden demgemäß direkt in einem von der Microsoft Inc. betriebenen Rechenzentrum in den Niederlangen und einem Backup-Rechenzentrum in der Republik Irland gespeichert. Dieses Unterauftragsverhältnis schließt die datenschutzrechtliche Unterbeauftragung ein. Eine solche vorherige Zustimmung darf vom „Kunde" nur aus wichtigem, der IdentPro nachzuweisenden Grund verweigert werden. Im Fall der Einschaltung eines nach §§ 15 ff. AktG mit der IdentPro verbundenen Unternehmens als Unterauftragnehmer erteilt der „Kunde" hiermit ausdrücklich seine Zustimmung. IdentPro wird dem „Kunden" auf Anforderung eine aktuelle Übersicht über die eingeschalteten Unterauftragnehmer übergeben.
2) Keiner Zustimmung bedarf die Einschaltung von Subunternehmern, bei denen der Subunternehmer lediglich eine Nebenleistung zur Unterstützung bei der Leistungserbringung nach der „Nutzervereinbarung" in Anspruch nimmt, auch wenn dabei ein Zugriff auf die „Kunden-Daten" nicht ausgeschlossen werden kann; dazu zählen insbesondere Transportleistungen von Post- oder Kurierdiensten sowie Geldtransportdienstleistungen, Telekommunikationsdienste, Bewachungsdienste und Reinigungsdienste, nicht aber Prüfungs- und Wartungsleistungen i.S.v. § 11 Abs. 5 BDSG. IdentPro wird mit solchen Subunternehmern branchenübliche Geheimhaltungsvereinbarungen treffen.
3) Zur Prüfung einer nach § 9 Abs. 1 erforderlichen Zustimmung hat IdentPro dem „Kunden" eine Kopie der Vereinbarung zur Unterauftragsdatenverarbeitung zur Verfügung zu stellen. Der Unterauftragsdatenverarbeitungsvertrag muss ein adäquates Schutzniveau aufweisen, welches demjenigen dieses Vertrags vergleichbar ist. Dem „Kunden" sind in dem Unterauftragsdatenverarbeitungsvertrag gegenüber dem Unterauftragnehmer eigene Kontrollrechte nach § 8 dieses Vertrags einzuräumen.
4) Die Regelungen in diesem § 9 gelten auch, wenn ein Unterauftragnehmer in einem Drittstaat eingeschaltet wird – ungeachtet des Umstands, dass Datenweitergaben an einen solchen Unterauftragnehmer nicht den Privilegierungen des § 11 BDSG unterliegen. Der „Kunde" bevollmächtigt IdentPro hiermit, in Vertretung des „Kunden" mit einem Unterauftragnehmer, der „Kunden-Daten" außerhalb des EWR verarbeitet oder nutzt, einen Vertrag unter Einbeziehung der EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern vom 5.2.2010 zu schließen. Der „Kunde" erklärt sich bereit, an der Erfüllung der Voraussetzungen nach § 4c BDSG im erforderlichen Maße mitzuwirken.

§ 10 Rechte der Betroffenen

1) Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem „Kunden" geltend zu machen.
2) Soweit ein Betroffener sich unmittelbar an IdentPro zwecks Auskunft, Berichtigung, Löschung oder Sperrung der ihn betreffenden Daten wenden sollte, wird IdentPro dieses Ersuchen zeitnah an den „Kunden" weiterleiten.
3) Für den Fall, dass eine betroffene Person ihre Rechte auf Berichtigung, Löschung oder Sperrung von „Kunden-Daten" oder auf Auskunft über die gespeicherten „Kunden-Daten", den Zweck der Speicherung und die Personen und Orte, an die „Kunden-Daten" regelmäßig übermittelt werden, geltend macht, hat IdentPro den „Kunden" bei der Erfüllung dieser Ansprüche in angemessenem und für den „Kunden" erforderlichen Umfang zu unterstützen, sofern der „Kunde" die Ansprüche nicht ohne

4) Mitwirkung der IdentPro erfüllen kann. IdentPro erhält vom „Kunden“ eine Entschädigung für ihren im Rahmen der Mitwirkung anfallenden Aufwand gemäß den jeweils gültigen Stunden- und Tagessätzen der IdentPro.
5) IdentPro wird es dem „Kunden“ ermöglichen, „Kunden-Daten“ zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des „Kunden“ die Berichtigung, Sperrung oder Löschung selbst vornehmen, wenn und soweit das dem „Kunden“ selbst unmöglich ist.

§ 11 Rückgabe und Löschung überlassener Daten und Datenträger

1) IdentPro hat sämtliche „Kunden-Daten“ nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung der „Nutzervereinbarung“) zu löschen und von dem „Kunden“ erhaltene Datenträger, die zu diesem Zeitpunkt noch „Kunden-Daten“ enthalten, an den „Kunden“ zurückzugeben.
2) Über eine Löschung bzw. Vernichtung von „Kunden-Daten“ hat IdentPro ein Protokoll zu erstellen, das dem „Kunden“ auf Anforderung vorzulegen ist.
3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind durch IdentPro entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 12 Verhältnis zur „Nutzervereinbarung“

Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen der „Nutzervereinbarung“. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus der „Nutzervereinbarung“, gehen die Regelungen aus diesem Vertrag vor.

Sankt Augustin, den 25-02-2014

_____	_____
(Ort, Datum)	(Ort, Datum)
	
_____	_____
(„Kunde“)	(IdentPro GmbH)

Anlagen:

Anlage 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kreis der Betroffenen
Diese Anlage 1 ist vom Kunden zu erstellen und der IdentPro zur Verfügung zu stellen.

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 2: Technische und organisatorische Maßnahmen

Übersicht über die technischen und organisatorischen Sicherheitsfunktionen

Dieses Dokument bietet einen Überblick über einige der technischen und organisatorischen Maßnahmen, mit denen die Sicherheit von der Microsoft Windows Azure Platform gewährleistet wird, die die Basis der finderbox Applikation bildet.

Sicherheit für die Hostumgebung

Die Windows Azure Platform-Umgebung besteht aus Computern, Betriebssystemen, Anwendungen und Diensten, Netzwerken, Geräten für Betrieb und Überwachung und spezialisierter Hardware, dazu kommt noch Verwaltungs- und Betriebspersonal, das für die Ausführung und Wartung der Dienste unentbehrlich sind. Ein weiterer Bestandteil der Umgebung sind die physischen Betriebszentren, in denen die Dienste untergebracht sind. Diese müssen wiederum sowohl vor absichtlichen Beschädigungen als auch vor zufälligen Schäden geschützt werden.

Schlüsselpunkte im Entwurf der Architektur

Windows Azure Platform ist mit umfassenden Verteidigungsebenen entworfen; somit wird das Risiko minimiert, dass der Ausfall eines einzelnen Sicherheitsmechanismus die Sicherheit der gesamten Umgebung beeinträchtigt. Zu den Verteidigungsebenen gehören:

- **Filterungsrouter:** Filterungsrouter blockieren Kommunikationsversuche zwischen Adressen und Ports, für die keine Kommunikationserlaubnis konfiguriert ist. Dies trägt zum Schutz vor häufig vorkommenden Angriffen bei, bei denen sogenannte "Dronen" oder "Zombies" verwendet werden, um nach anfälligen Servern zu suchen. Obwohl solche Angriffe relativ einfach geblockt werden können, zählen sie zu den beliebtesten Methoden, die Angreifer verwenden, um nach Schwachstellen zu suchen. Filterungsrouter unterstützen auch die Konfiguration von Back-End-Diensten, damit der Zugriff auf diese nur vom zugehörigen Front-End aus erfolgen kann.

- **Firewalls:** Firewalls beschränken die Datenkommunikation zu (und von) bekannten und autorisierten Ports, Protokollen und Ziel- und Quell-IP-Adressen.

- **Kryptografischer Schutz für Nachrichten:** Für den Schutz von Steuerungsnachrichten, die zwischen Windows Azure-Datencentern und zwischen Clustern innerhalb eines bestimmten Datencenters ausgetauscht werden, wird TLS mit kryptografischen Schlüsseln mit mindestens 128 Bit verwendet.

- **Verwaltung von Sicherheitspatches für Software:** Die Verwaltung von Sicherheitspatches leistet einen wichtigen Beitrag zum Schutz von Systemen vor bekannten Sicherheitsrisiken. Windows Azure Platform verwendet integrierte Bereitstellungssysteme zur Verwaltung der Verteilung und Installation von Sicherheitspatches für Microsoft-Software.

- **Überwachung:** Zur Sicherheitsüberwachung werden zentralisierte Überwachungs-, Korrelations- und Analysesysteme verwendet, die die große Menge der von den Geräten innerhalb der Umgebung erzeugten Informationen verwalten und zeitnahe und relevante Überwachungs- und Warnfunktionen bieten.

- **Netzwerksegmentierung:** Microsoft verwendet eine Reihe von Technologien, um an strategischen Punkten und innerhalb der Datencenter Barrieren für unerlaubten Datenverkehr einzurichten. Dazu zählen Firewalls, Netzwerkadressübersetzungs-komponenten (Lastenausgleichskomponenten) und Filterungsrouter. Das Back-End-Netzwerk besteht aus partitionierten lokalen Netzwerken für Web- und Anwendungsserver, für die Datenspeicherung und für die zentralisierte Verwaltung. Diese Server sind in private Adresssegmente gruppiert, die durch Filterungsrouter geschützt werden.

Physische Sicherheit

Die physische Sicherheit geht mit den softwarebasierten Sicherheitsmaßnahmen einher, und für beide gelten ähnliche Risikobewertungs- und -abwehrmaßnahmen.

Windows Azure Platform-Dienste werden den Kunden über ein Netzwerk von Datencentern bereitgestellt, von denen jedes für einen ununterbrochenen Betrieb ausgelegt ist und über verschiedene Betriebsschutzmaßnahmen gegen Stromausfälle, physisches Eindringen und Netzwerkausfälle verfügt. Diese Datencenter halten anwendbare Industriestandards bezüglich der physischen Sicherheit und Zuverlässigkeit ein. Sie werden von Microsoft-Betriebspersonal verwaltet, überwacht und betreut und sind geografisch voneinander getrennt.

Microsoft verwendet Hochsicherheits-Zutrittsmechanismen, und der Zutritt ist nur einer kleinen Zahl von Betriebsmitarbeitern erlaubt, die ihre Administratorzugangspasswörter regelmäßig ändern müssen. Der Zugang zu den Datencentern und die Erlaubnis zum Öffnen von Tickets für den Zugang zu den Datencentern wird vom Netzwerkbetriebsleiter im Einklang mit vor Ort geltenden Sicherheitsverfahren für die Datencenter überwacht.

Betriebs- und Personalsicherheit

Windows Azure Platform ist so entwickelt, dass während des Betriebs routinemäßig kein Zugriff auf Kundendaten durch Microsoft-Mitarbeiter erfolgt.

Reaktionen auf Zwischenfälle

Es stehen rund um die Uhr Betriebsmitarbeiter für Windows Azure Platform-Dienste bereit. Tritt ein Vorfall auf, der ein Sicherheitsrisiko darstellt, werden von den Betriebsmitarbeitern die dokumentierten Verfahren für das Auftreten eines solchen Vorfalls angewendet. Des Weiteren ist ein vollständiger Kommunikationsplan vorhanden, der ebenfalls beim Auftreten eines Vorfalls, der ein Sicherheitsrisiko darstellt, angewendet wird.

Überprüfung

Die Verwaltungsvorgänge von Microsoft werden überprüft. Der Audit-Trail kann angezeigt werden, um den Verlauf der Änderungen nachzuverfolgen.

Sicherheit auf Anwendungsebene

Zusätzlich zu den Sicherheitsverfahren bezüglich der Datencenter, Netzwerke und Mitarbeiter integriert Windows Azure Platform verschiedene Sicherheitsverfahren auf Anwendungsebene, um allen Benutzern eine möglichst sichere Erfahrung zu bieten. Dies bezieht sich sowohl auf die Entwicklung der Anwendung als auch auf Anwendungsfeatures, die dem Dienstadministrator zur Verfügung stehen.

Sicherheitsfunktionen

Windows Azure bietet Kunden virtuelle Computer und somit Zugriff auf die meisten in Windows Server verfügbaren Sicherheitsoptionen. Die finderbox verwendet SSL-Clientzertifikate zur Kontrolle von Aktualisierungen an der Software und Konfiguration.

Fehlertoleranz und Redundanz

Windows Azure Platform ist auf Fehlertoleranz und Redundanz ausgelegt. Von der geografischen Trennung der Datencenter bis hin zu replizierten Rolleninstanzen und Speichern bieten viele Aspekte des Diensts Fehlertoleranz und Redundanz. Trotz all dieser Schritte kann die vollständige Fehlertoleranz von Windows Azure Platform nicht garantiert werden.

Dienstredundanz

Jede Ebene der Windows Azure Platform-Infrastruktur ist darauf ausgelegt, beim Auftreten eines Fehlers weiter zu funktionieren. Dies wird u. a. durch redundante Netzwerkgeräte auf jeder Ebene gewährleistet sowie durch die Tatsache, dass für jedes Datencenter zwei Internetdienstanbieter zur Verfügung stehen. Der Failover erfolgt in den meisten Fällen automatisch (ohne die Notwendigkeit menschlichen Eingreifens), und das Netzwerk wird rund um die Uhr durch das Netzwerkbetriebszentrum überwacht, damit jegliche Anomalien oder möglichen Netzwerkprobleme erkannt werden.

Redundanz von Datencentern

Finderbox nutzt zwei europäische Datencenter in Amsterdam und in Irland. Beim Ausfall eines kompletten Datencenters aufgrund einer Katastrophe wird automatisch auf das andere Datencenter gewechselt.

Aktualisierungen

Microsoft ist berechtigt, die hier beschriebenen Sicherheitsmaßnahmen im Einklang mit anderen Aktualisierungen von Windows Azure Platform anzupassen, oder um auf neu auftretende Sicherheitsbedrohungen zu reagieren oder neue Sicherheitstechnologien und -verfahren zu implementieren.

Zertifizierung

Die o.g. Sicherheitsmaßnahmen werden nach ISO 27001 jährlich überprüft und zertifiziert. Das von der British Standards Institution (BSI) für Microsoft ausgestellte Zertifikat ist öffentlich verfügbar. Zudem wird nach ISO/IEC 27002 ein “code of best practices” für das Sicherheits-system eingehalten.

Zertifikatsnummer: IS 577753 Mehr Informationen: http://www.windowsazure.com/de-de/support/trust-center/compliance/