Technische und organisatorische Maßnahmen

gem. Art. 32 Abs. 1 Datenschutz Grundverordnung (DSGVO) für Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

Version 1.7

Angaben zum Auftragsverarbeiter

Name	Timebutler GmbH
Straße	Rathausgasse 1
Postleitzahl	12529
Ort	Schönefeld
Handelsregister:	Amtsgericht Cottbus, HRB 18094 CB
E-Mail-Adresse	info@timebutler.de
Internet-Adresse	www.timebutler.de

Terminologie

Dieses Dokument verwendet die Terminologie und die Definitionen gemäß der Datenschutz-Grundverordnung (im folgenden „DSGVO“ bezeichnet). Darüber hinaus bezeichnet

- **„Auftragnehmer“** den Auftragsverarbeiter gemäß den Angaben oben in diesem Dokument;
- **„Auftraggeber“** den Verantwortlichen gemäß DSGVO, der mit dem Auftragsverarbeiter einen Vertrag zur Auftragsverarbeitung vereinbart hat.
- **„Software“** die SaaS-Lösung, die der Auftragnehmer zur Nutzung für den Auftraggeber bereitstellt, um die Verarbeitung der Daten durchzuführen.

Zur Absicherung der Daten des Auftraggebers werden folgende technischen und organisatorischen Maßnahmen für die Systeme des Auftragnehmers verbindlich festgelegt:

1. Vertraulichkeit

a. Zutrittskontrolle

Hierunter fallen alle Maßnahmen, damit Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, auf denen personenbezogene Daten des Auftraggebers verarbeitet werden.

Zutrittskontrolle durch den Hosting Anbieter:

Die Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten des Auftraggebers verarbeitet werden, werden in einem zertifizierten Rechenzentrum von Amazon Web Services (AWS) betrieben, welche umfassende Sicherheitskonzepte für Ihr Hosting-Angebot vorsieht.

AWS betreibt viele Rechenzentren und ist Marktführer im Segment der Hosting-Anbieter. Tausende Unternehmen verwenden die Hosting-Dienstleistungen von AWS.

AWS bietet entsprechend hohe Sicherheitsstandards bei der Zutrittskontrolle zu den Rechenzentren. Detaillierte Informationen zu den Zutrittskontrollen finden sich im Anhang „AWS Zutrittskontrollen, Zugangskontrollen, Schutz der Daten“ in diesem Dokument.

Zutrittskontrolle durch den Auftragnehmer:

Die personenbezogenen Daten des Auftraggebers werden auf den oben genannten Servern im Rechenzentrum des Hosting Anbieters verarbeitet. In den Büroräumen des Auftragnehmers werden die personenbezogenen Daten nicht dauerhaft gespeichert oder verarbeitet.

Der Zugriff auf die personenbezogenen Daten erfolgt ausschließlich über die Arbeitsplatzrechner des Auftragnehmers.

Der Zugang zu den Büroräumen ist durch Schließsysteme vor dem Zugang durch Unbefugte geschützt.

In den Büroräumen finden keine Besuche von Kunden statt, da die Software ausschließlich über das Internet bereitgestellt wird und keine Vor-Ort-Kundentermine angeboten werden. Stattdessen finden Kundentermine ausschließlich über virtuelle Konferenzlösungen ohne physische Präsenz statt. Sollte sich die Vorgehensweise ändern und Besucher empfangen werden, so wird der Auftragnehmer ein Protokoll der Besucher führen und jeder Besucher wird während des gesamten Besuchs von einem Mitarbeitenden des Auftragnehmers begleitet werden.

b. Zugangskontrolle

Hierunter fallen Maßnahmen, damit Unbefugte an der Benutzung der Datenverarbeitungsanlagen und Datenverarbeitungsverfahren gehindert werden.

Zugangskontrolle durch den Hosting Anbieter:

Die Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten des Auftraggebers verarbeitet werden, werden in einem zertifizierten Rechenzentrum von Amazon Web Services (AWS) betrieben, welche umfassende Sicherheitskonzepte für Ihr Hosting-Angebot vorsieht.

AWS betreibt viele Rechenzentren und ist Marktführer im Segment der Hosting-Anbieter. Tausende Unternehmen verwenden die Hosting-Dienstleistungen von AWS.

AWS bietet entsprechend hohe Sicherheitsstandards bei der Zugangskontrolle zu den Rechenzentren. Detaillierte Informationen zu den Zutrittskontrollen finden sich im Anhang „AWS Zutrittskontrollen, Zugangskontrollen, Schutz der Daten“ in diesem Dokument.

Zugangskontrolle durch den Auftragnehmer:

Auf Seiten des Auftragnehmers findet der Zugriff auf die Hosting-Systeme, auf denen die für den Auftraggeber zur Verfügung gestellte Software betrieben wird, ausschließlich über Arbeitsplatzrechner statt, die nur mit Benutzername und Passwort entsperrt werden können.

Die Arbeitsplatzrechner werden vom Arbeitgeber bereitgestellt. Es kommen keine eigenen Geräte der Arbeitnehmer zum Einsatz (kein sog. BYO / „Bring your own“).

Des Weiteren findet der Zugriff von den Arbeitsplatzrechnern auf die Systeme des Hosting-Anbieters nur über SSL-gesicherte (Secure Socket Layer) Zugriffe statt.

Auf die Systeme des Hosting-Anbieters kann nur unter Kenntnis des Benutzernamens und Passwortes zugegriffen werden. Diese Benutzernamen und Passwörter sind ausschließlich dem Auftragnehmer und seinen mit der Betreuung der Systeme beauftragten Mitarbeitern bekannt.

Alle Mitarbeiter des Auftragnehmers haben sich auf die Vertraulichkeit der Daten verpflichtet. Die Mustervorlage für die Verpflichtung der Mitarbeiter auf die Vertraulichkeit der Daten, die von jedem Mitarbeiter des Auftragnehmers unterzeichnet wird, ist dem Auftragnehmer bekannt (über die Webseite www.timebutler.de/avv/tom abrufbar).

Beim Auftragnehmer kommt eine Benutzerverwaltung zum Einsatz. Bei Austritt eines Mitarbeiters aus dem Unternehmen werden sämtliche Zugänge gesperrt. Jede Nutzerkennung ist eindeutig und personenbezogen.

Die Arbeitsplatzrechner sind mit einer automatischen Pausenschaltung (Automatische Sperrung des PC nach einer bestimmten Anzahl Minuten ohne Aktivität) versehen. Updates des Betriebssystems und sicherheitsrelevanter Software werden automatisiert eingespielt und aktuell gehalten.

Der Zugriff auf die Arbeitsplatzrechner ist ausschließlich mit einem Benutzernamen und Passwort möglich. Die Arbeitsplatzrechner erhalten eine automatisierte und vollständige Verschlüsselung der Speicherlaufwerke, damit auch bei Verlust der Arbeitsplatzrechner ein Zugriff auf die Daten und Zugangsdaten durch Dritte nicht möglich ist.

Die Zugangspasswörter unterliegen einer Passwort-Policy.

Die Systeme sind mit einer Firewall geschützt. Es wird eine sichere Konfiguration der Betriebssysteme und Anwendungssoftware gemäß Herstellerempfehlungen und Best Practices angestrebt.

c. Zugriffskontrolle

Hierunter fallen Maßnahmen, mit denen gewährleistet wird, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können.

Der Auftragnehmer kann auf die Systeme des Hosting-Anbieters zugreifen, auf dem die Software betrieben wird, auf der die vom Auftraggeber bereitgestellten Daten verarbeitet und gespeichert werden.

Die Mitarbeiter des Auftragnehmers haben Zugriff auf die Systeme, um Aufgaben der Wartung der Server, der Software, der Datenbestände und auch der Weiterentwicklung, Systemadministration und entsprechende Aufgaben erfüllen zu können.

Alle Mitarbeiter des Auftragnehmers haben sich auf die Vertraulichkeit der Daten verpflichtet. Die Mustervorlage für die Verpflichtung der Mitarbeiter auf die Vertraulichkeit der Daten, die von jedem Mitarbeiter des Auftragnehmers unterzeichnet wird, ist dem Auftragnehmer bekannt (über die Webseite www.timebutler.de/avv/tom abrufbar).

Ein Berechtigungskonzept stellt sicher, dass nur befugte Mitarbeiter auf die notwendigen Systeme und Daten zugreifen können. Der Auftragnehmer kann stets die Befugnisse und Zugriffsmöglichkeiten seiner Mitarbeiter benennen und diese anpassen.

d. Auftragskontrolle

Hierunter fallen Maßnahmen, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Auftragskontrolle durch den Hosting Anbieter:
Der Hosting Anbieter führt keine Änderungen an den personenbezogenen Daten des Auftraggebers durch, sondern stellt lediglich die Infrastruktur für den technischen Betrieb der Server zur Verfügung.

Auftragskontrolle durch den Auftragnehmer:
Der Auftragnehmer führt in der Regel keine Änderungen an den personenbezogenen Daten des Auftragnehmers durch. Der Auftragnehmer stellt dem Auftraggeber mit der Software Funktionalitäten zur Verfügung, mit denen der Auftraggeber die personenbezogenen Daten selbständig bearbeiten, ändern, einsehen und löschen kann, ohne den Auftragnehmer anzuweisen.

In den seltenen Fällen, in denen der Auftraggeber eine Bearbeitung, Änderung oder Löschung von personenbezogenen Daten durch den Auftragnehmer anweist, sind die Anweisungen detailliert und in schriftlicher Form zu übermitteln. Der Auftragnehmer wird gegenüber dem Auftraggeber offene Frage klären und die durchzuführenden Änderungen schriftlich vereinbaren. Ohne diese Voraussetzung nimmt der Auftragnehmer keine Änderungen vor.

Der Auftraggeber kann sich über die Funktionsweise und somit die Verarbeitung der personenbezogenen Daten in der Software selbständig informieren und in Erfahrung bringen, wie die Software die personenbezogenen Daten je nach Nutzung durch den Auftraggeber ändert.

e. Trennungskontrolle

Hierunter fallen alle Maßnahmen, die gewährleisten, dass die personenbezogenen Daten des Auftraggebers getrennt von anderen Kundendaten verarbeitet werden.

Die vom Auftragnehmer zur Verfügung gestellte Software wird von tausenden Unternehmen verwendet. Die Software ist von Beginn an für die Verwendung durch verschiedenste Unternehmen über das Internet konzipiert und implementiert worden, so dass auch von Beginn an die Mandantenfähigkeit (Abtrennung der Daten in getrennte Bereiche), gewährleistet ist.

Die Benutzerkonten sind verschiedenen Nutzerkreisen (Mandanten) zugewiesen. Benutzer eines Nutzerkreises können immer nur maximal die Daten der Nutzer des gleichen Benutzerkreises einsehen oder bearbeiten (jeweils im Rahmen der Benutzerrechte des Benutzerkontos).

Eine Einsichtnahme oder das Bearbeiten von Daten von Benutzern anderer Nutzerkreise ist aufgrund der Softwarearchitektur nicht möglich und wurde während der Programmierung der Software sichergestellt.

Während der gesamten Laufzeit der Software seit 2003 ist kein Fall bekannt geworden, bei dem Daten eines Mandanten durch einen nicht autorisierten anderen Mandanten eingesehen, geändert oder gelöscht werden konnten. Der Auftragnehmer aktualisiert und prüft die Software in regelmäßigen Abständen. Der Auftraggeber informiert den Auftragnehmer unverzüglich bei Erlangung von Erkenntnissen über fehlende Daten- oder Softwaresicherheit.

Die Entwicklungs-, Test- und Produktivsysteme sind physisch und logisch voneinander getrennt. Die Entwicklung und Tests erfolgt auf den Arbeitsplatzrechner der Mitarbeiter. Die Produktivsysteme werden hingegen im Rechenzentrum des Hosting Anbieters betrieben.

f. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. A DS-GVO, Art. 25 Abs. 1 DS-GVO)

Damit die Zwecke der Auftragsverarbeitung erreicht werden können, ist eine Pseudonymisierung der personenbezogenen Daten nicht möglich.

Verschlüsselung auf den Systemen des Auftragnehmers

Die persönlichen Daten werden in der Datenbank der Software in Klartext gespeichert mit Ausnahme des Passwortes. Das Passwort wird nur verschlüsselt gespeichert ohne die Möglichkeit, das ursprüngliche Passwort zu berechnen. Somit ist es auch dem Auftragnehmer nicht möglich, die Passwörter einzusehen oder in ein lesbares Format umzuwandeln. Der Auftragnehmer sieht das als zwingende Notwendigkeit an, da zum einen die Kenntnis über das Passwort für den Betrieb und die Verfügbarkeit der Software nicht notwendig ist, zum anderen manche Nutzer das gleiche Passwort für verschiedene Internetdienste nutzen.

Neben der Datenbank werden die Daten in einem Backup gespeichert. Auch dort bleibt die Verschlüsselung des Passwortes erhalten. Das Backup wird auf einem gesicherten Backup-Server gespeichert, auf das ohne Kenntnis des Benutzers und Passworts kein Zugriff möglich ist.

Der für den Zugriff erforderliche Benutzername und das Passwort sind lediglich den befugten Mitarbeitern des Auftragnehmers bekannt. Die Mitarbeiter wurden zur Vertraulichkeit verpflichtet.

Verschlüsselung bei der Kommunikation der beteiligten Systeme bei Verwendung der Software

Bei der Verwendung der Software sind die Internet-Browser des Auftraggebers, der Server der Software, und die Arbeitsplatzrechner oder Endgeräten der Mitarbeiter des Auftragnehmers beteiligt, zusammen mit den Systemen, die den Transport der Informationen über das Internet gewährleisten.

Damit die Daten nicht von dritten beteiligten Systemen außer den Systemen des Auftragnehmers und des Auftraggebers ausgelesen werden können, und die Informationen fälschungssicher zugestellt werden, stellt der Auftragnehmer sicher, dass die Software sämtliche Kommunikation per SSL/TLS (Secure Socket Layer / Transport Layer Security) verschlüsselt. Sollte eines der genannten Systeme des Auftraggebers eine ungesicherte Verbindung aufbauen wollen, wird die Software die Anfrage mit einem Verweis auf Verwendung einer gesicherten Verbindung quittieren, ohne dabei persönliche Daten zu übermitteln. Die Antwort mit Verweis auf die gesicherte Verbindung ist dabei so gestaltet, dass das anfragende System die Möglichkeit hat, automatisch auf die gesicherte Verbindung zu wechseln und die Anfrage zu wiederholen.

Verschlüsselung bei der Kommunikation per elektronischer Email

Die Software versendet Emails an die Nutzer der Software, somit an die Mitarbeiter des Auftraggebers.

Der Auftragnehmer stellt sicher, dass der Email-Verkehr verschlüsselt über SSL/TLS (Secure Socket Layer / Transport Layer Security) stattfinden kann, sowohl beim Versand von Emails als auch beim Empfang von Emails. Damit werden Emails außerhalb der beteiligten E-Mail-Verarbeitungssysteme des Auftraggebers und des Auftragnehmers abhör- und fälschungssicher.

Damit der verschlüsselte Transport möglich ist, muss der Auftraggeber bei seinen E-Mail-Systemen ebenfalls die verschlüsselte Kommunikation einstellen und ermöglichen. Der Auftraggeber ist somit dafür verantwortlich, die Transport-Verschlüsselung für den E-Mail-Versand und –Empfang an seinen E-Mail-Systemen bereitzustellen und aktuell zu halten.

Sollte eine Transport-Verschlüsselung am E-Mail-System des Auftraggebers nicht möglich sein, hat der Auftraggeber die Möglichkeit, den E-Mail-Versand bei den Nutzerkonten zu deaktivieren: in der Software kann an jedem Nutzerkonto im Nutzerprofil der Versand der Emails aktiviert oder deaktiviert werden.

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

a. Weitergabekontrolle

Hierunter fallen Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

Die für die Verarbeitung der vom Auftraggeber bereitgestellten Daten zuständige Software ist über das Internet erreichbar. Die Software stellt dabei sicher, dass die Kommunikation stets über eine SSL-gesicherte Verbindung mit aktuellen Sicherheitsstandards erfolgt.

So stellt die Software auch zu jedem Zeitpunkt sicher, dass ein wissentlich oder unwissentlich ungesicherter Verbindungsversuch eines Nutzers vollautomatisiert mit einer technischen Weiterleitung auf eine gesicherte Verbindung beantwortet wird, ohne persönliche Daten über die nicht gesicherte Kommunikation zu transportieren (Prüfung auf die gesicherte https-Kommunikation bei jedem Request und automatisierte Weiterleitung bei ungesicherten http-Anfragen auf gesicherte https-Kommunikation).

Der Zugriff zwischen den Arbeitsplatzrechnern des Auftragnehmers und den Systemen, auf dem die Software betrieben wird und dem Backup-Server erfolgt stets über SSL gesicherte Kommunikation.

Backups werden mit einer starken Verschlüsselung gespeichert, die ohne den privaten Schlüssel mit aktuellen technischen Mitteln nicht in akzeptabler Zeit entschlüsselt werden können. Die Übertragung von Daten des Servers zum Backup Server findet per verschlüsselter Kommunikation statt.

b. Eingabekontrolle

Hierunter fallen Maßnahmen die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Bei dem Erstellen eines neuen Benutzerkontos protokolliert die Software den Ersteller des Benutzerkontos, so dass nachträglich nachvollziehbar ist, wer das neue Benutzerkonto angelegt hat.

Ebenso wird die Bearbeitungshistorie von Abwesenheitseinträgen, wie beispielsweise die Neueintragung einer Dienstreise, die Freigabe eines Urlaubsantrages oder das Ablehnen eines Antrags auf Abbau von Überstunden protokolliert und in der Software dargestellt.

Die Software protokolliert jedoch nicht jede Änderung an personenbezogenen Daten. Ein Benutzer kann beispielsweise die Daten zu seiner E-Mail-Adresse, die Telefonnummer oder die Abteilungszugehörigkeit ändern und die Software protokolliert nicht, welches Datum durch welchen Benutzer eingetragen, geändert oder gelöscht wurde. Das beinhaltet insbesondere auch den Fall, wenn ein Benutzer sein Benutzerkonto löscht: das Löschen erfordert, dass das Benutzerkonto und alle zugehörigen personenbezogenen Daten vollständig gelöscht werden, so dass es nicht möglich ist, zu protokollieren, wer das Benutzerkonto gelöscht hat, da dafür personenbezogene Daten gespeichert werden müssten.

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

a. Verfügbarkeitskontrolle

Hierunter fallen Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Verfügbarkeitskontrolle durch den Hosting Anbieter:

Die Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten des Auftraggebers verarbeitet werden, werden in einem zertifizierten Rechenzentrum von Amazon Web Services (AWS) betrieben, welche umfassende Sicherheitskonzepte für Ihr Hosting-Angebot vorsieht.

AWS betreibt viele Rechenzentren und ist Marktführer im Segment der Hosting-Anbieter. Tausende Unternehmen verwenden die Hosting-Dienstleistungen von AWS.

AWS bietet entsprechend hohe Sicherheitsstandards bei der Zugangskontrolle zu den Rechenzentren. Detaillierte Informationen zu den Zutrittskontrollen finden sich im Anhang „AWS Zutrittskontrollen, Zugangskontrollen, Schutz der Daten“ in diesem Dokument.

Verfügbarkeitskontrolle durch den Auftragnehmer:

Der Auftragnehmer führt automatisiert Backups aller Daten durch. Das Backup wird automatisiert auf einem speziell für Datensicherungen vorgesehenen Server übertragen. Die Backup Server sind redundant und somit vor Datenverlust gesichert.

Auf die Systeme der Backups hat nur der Auftragnehmer Zugriff.

Durch die physische Trennung des Backup Systems vom Server, auf dem die Software betrieben wird, ist bei einem mit Datenverlust verbundenen Hardware- oder Softwareausfall die Verfügbarkeit der Daten durch das getrennt gespeicherte Daten-Backup gewährleistet.

Der Auftraggeber führt regelmäßige Sicherungen seiner Daten auf Speichersystemen außerhalb des Verantwortungsbereichs des Auftragnehmers durch. Die Software stellt mit den Funktionen der API (Schnittstelle) und dem Berichts- und Downloadcenter Funktionen bereit, damit der Auftraggeber die Daten bequem und schnell aus der Software exportieren kann.

b. Wiederherstellbarkeit

Hierunter fallen Maßnahmen, die sicherstellen, dass personenbezogene Daten bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Der Auftragnehmer setzt ein technisches Verfahren ein, mit dem der Datenbestand automatisiert und regelmäßig auf einem von der Laufzeitumgebung physisch und logisch getrennten System gesichert wird. Im Falle eines physischen oder technischen Zwischenfalls auf dem System der Laufzeitumgebung können die Daten aus dem Backup-Server wiederhergestellt werden und dem Auftraggeber wieder zur Verfügung gestellt werden.

Der Auftragnehmer hat ein Wiederanlaufkonzept nach einem physischen oder technischen Zwischenfall erarbeitet, das dem Auftragnehmer bekannt ist (über die Webseite www.timebutler.de/avv/tom abrufbar). Der Auftraggeber erkennt an, dass die im Wiederanlaufkonzept nach einem physischen oder technischen Zwischenfall beschriebenen Maßnahmen seinen Anforderungen entsprechen.

c. Löschkonzept

Hierunter fallen Maßnahmen, die sicherstellen, dass die richtigen personenbezogenen Daten zum richtigen Zeitpunkt gelöscht werden.

Daten in der Software werden nur vom Auftraggeber gelöscht. Der Auftragnehmer löscht keine Daten, außer in dem Fall, wenn der Auftraggeber den Auftragnehmer entsprechende Anweisung erteilt.

Die Backup-Daten werden für einen begrenzten Zeitraum vorgehalten und dann durch entsprechende automatisierte Routinen, deren Funktionalität der Auftragnehmer gewährleisten muss, gelöscht.

Der Auftragnehmer hat ein Löschkonzept erstellt, in dem die Maßnahmen für das richtige Löschen der personenbezogenen Daten beschrieben sind. Das Löschkonzept ist dem Auftragnehmer bekannt (über die Webseite www.timebutler.de/avv/tom abrufbar).

4. Anpassung an den technischen Fortschritt

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

ANHANG / AWS Zutrittskontrollen, Zugangskontrollen, Schutz der Daten

Amazon Web Services veröffentlicht folgende Informationen auf seiner Webseite:

Sicheres Design

Standortauswahl
Bevor wir uns für einen Standort entscheiden, führt AWS eine erste Bewertung der Umgebung und der geografischen Lage durch. Die Rechenzentrumsstandorte werden sorgfältig ausgewählt, um Umweltrisiken wie Überschwemmungen, extreme Wetterbedingungen und seismische Aktivitäten so gering wie möglich zu halten. Unsere Availability Zones sind so gebaut, dass sie unabhängig und räumlich voneinander getrennt sind.

Redundanz
Rechenzentren sind darauf ausgelegt, Funktionsausfälle zu antizipieren und zu tolerieren und dabei Servicelevel aufrecht zu erhalten. Für das Eintreten eines Funktionsausfalls wird der Datenverkehr von dem vom Ausfall betroffenen Bereich auf einen anderen umgeleitet. Für wichtige Anwendungen gilt ein N+1-Standard. Kommt es in einem Rechenzentrum zu einem Funktionsausfall, stehen genügend Kapazitäten zur Verfügung, damit der Datenverkehr auf die verbleibenden Standorte aufgeteilt werden kann.

Verfügbarkeit
AWS kennt alle kritischen Systemkomponenten, die erforderlich sind, um die Verfügbarkeit unseres Systems zu erhalten und den Betrieb im Fall eines Ausfalls wieder aufzunehmen. Kritische Systemkomponenten werden an mehreren, voneinander isolierten Standorten (Availability Zones genannt) gesichert. Jede Availability Zone ist auf einen unabhängigen Betrieb mit hoher Zuverlässigkeit ausgelegt. Die Availability Zones sind vernetzt. Dies ermöglicht Ihnen die Nutzung von Anwendungen, für die ein automatischer, unterbrechungsfreier Failover zwischen den Availability Zones eingerichtet ist. Extrem ausfallsichere Systeme und eine daraus resultierende Serviceverfügbarkeit sind Bestandteil des Systemdesigns. AWS-Kunden profitieren durch den Einsatz von Availability Zones und Datenreplikation von extrem kurzen Wiederherstellungszeiträumen und Wiederherstellungspunktzielen sowie höchstmöglicher Serviceverfügbarkeit.

Kapazitätsplanung
AWS überwacht kontinuierlich die Service-Nutzung, um Infrastruktur bereitzustellen und unseren Verfügbarkeitsverpflichtungen nachzukommen und Anforderungen zu unterstützen. AWS überprüft die Infrastrukturnutzung und -anforderungen mindestens einmal im Monat anhand eines Kapazitätsplanungsmodell. Mit diesem Modell lässt sich auch der künftige Bedarf prognostizieren. Es umfasst auch Überlegungen zu Informationsverarbeitung, Telekommunikation und der Speicherung von Audit-Protokollen.

Betriebskontinuität und Notfallwiederherstellung

Plan zur Aufrechterhaltung des Betriebs (Business Continuity Plan)
Der AWS-Betriebskontinuitätsplan umfasst Maßnahmen zur Vermeidung und Verringerung von Störungen durch Umwelteinflüsse. Er enthält betriebliche Details zu den Maßnahmen, die vor, während und nach einem entsprechenden Ereignis ergriffen werden. Der Betriebskontinuitätsplan wird durch Tests gestützt, die auch Simulationen verschiedener Szenarios umfassen. Während und nach diesen Tests dokumentiert AWS die Leistung seiner Mitarbeiter und Prozesse, Korrekturmaßnahmen und die abgeleiteten Erfahrungen zur kontinuierlichen Verbesserung.

Reaktion auf Pandemien
AWS berücksichtigt bei seiner Notfallwiederherstellungsplanung auch Reaktionsrichtlinien und -verfahren für Pandemien, um im Fall des Ausbruchs einer Infektionskrankheit schnell reagieren zu können. Die Abhilfemaßnahmen umfassen alternative Personalmodelle, bei denen kritische Prozesse an Ressourcen in anderen Regionen ausgelagert werden, sowie die Aktivierung eines Krisenmanagementplans, der kritische betriebliche Operationen unterstützen soll. Die Pandemiepläne enthalten Informationen zu internationalen

Gesundheitsbehörden und -bestimmungen einschließlich Kontaktdaten für internationale Behörden.

Physischer Zugriff
Mitarbeiterzugang zu Rechenzentren
Nur autorisiertes AWS-Personal erhält Zugang zu den physischen Rechenzentren. Alle Mitarbeiter, die Zugang zu einem Rechenzentrum benötigen, müssen zunächst einen Antrag auf Zugang stellen und eine gültige geschäftliche Begründung vorlegen. Dieser Antrag wird basierend auf dem Prinzip geringstmöglicher Berechtigungen gewährt, d. h. Mitarbeiter müssen in der Anfrage angeben, auf welche Ebene des Rechenzentrums und für welchen Zeitraum sie Zugang benötigen. Die Anfrage wird geprüft und von autorisiertem Personal genehmigt. Der Zugang wird nach Ablauf des beantragten Zeitraums wieder entzogen. Mitarbeiter mit Zugang zu einem Rechenzentrum sind durch ihre Berechtigungen auf bestimmte Bereiche beschränkt.

Zugang von Dritten zu Rechenzentren
Der Zugang von Dritten muss von autorisierten AWS-Mitarbeitern beantragt werden, die auch eine gültige geschäftliche Begründung für diesen Zugang vorlegen müssen. Dieser Antrag wird basierend auf dem Prinzip geringstmöglicher Berechtigungen gewährt, d. h. Mitarbeiter müssen in der Anfrage angeben, auf welche Ebene des Rechenzentrums und für welchen Zeitraum sie Zugang benötigen. Diese Anfragen werden von autorisiertem Personal genehmigt. Der Zugang wird nach Ablauf des beantragten Zeitraums wieder entzogen. Mitarbeiter mit Zugang zu einem Rechenzentrum sind durch ihre Berechtigungen auf bestimmte Bereiche beschränkt. Personen mit einem Besucherausweis müssen diesen bei Ankunft am Standort vorlegen und werden von autorisiertem Personal angemeldet und begleitet.

Zugang zu Rechenzentren in der Region AWS GovCloud
Der physische Zugang zu den Rechenzentren in der AWS GovCloud (US) ist auf Mitarbeiter beschränkt, die nachweislich US-Bürger sind.

Überwachung und Protokollierung

ZUGANGSPRÜFUNG FÜR RECHENZENTREN
Der Zugang zu den Rechenzentren wird regelmäßig geprüft. Der Zugriff wird automatisch aufgehoben, sobald die Akte eines Mitarbeiters aus dem Personalsystem von Amazon gelöscht wird. Darüber hinaus wird der Zugang von Mitarbeitern oder Zeitarbeitskräften nach Ablauf des genehmigten Zeitraums auch dann widerrufen, wenn sie weiterhin als Mitarbeiter von Amazon tätig sind.

Zugangsprotokolle für Rechenzentren
Der physische Zutritt zu AWS-Rechenzentren wird protokolliert, überwacht und gespeichert. AWS fasst die über die logischen und physischen Überwachungssysteme erfassten Informationen zusammen, um die Sicherheit bei Bedarf noch zu erhöhen.

Überwachung des Zugangs zu Rechenzentren
Wir überwachen unsere Rechenzentren über unsere globalen Security Operations Center, die für die Überwachung, Analyse und Durchführung von Sicherheitsprogrammen zuständig sind. Sie leisten rund um die Uhr weltweit Unterstützung mit der Verwaltung und Überwachung der Zugangsaktivitäten zu Rechenzentren und unterstützen lokale und andere Supportteams durch Analyse, Beratung und Beauftragung bei der Reaktion auf Sicherheitsverstöße.

Überwachung und Erkennung

CCTV
Physische Zugangspunkte zu Serverräumen werden von CCTV-Kameras mit Aufzeichnungsfunktion überwacht. Die Aufnahmen werden gemäß behördlichen und Compliance-Anforderungen aufbewahrt.

Eingänge zu Rechenzentren
Der physische Zugang wird durch professionelles Sicherheitspersonal an den Gebäudeeingängen kontrolliert. Dabei werden Überwachung, Meldeanlagen und andere elektronische Vorrichtungen eingesetzt. Autorisiertes Personal erlangt über Multi-Faktor-Authentifizierungsmechanismen Zugang zu den

Rechenzentren. Die Eingänge zu den Serverräumen sind mit Geräten abgesichert, die Alarm auslösen, wenn die Tür aufgebrochen oder offen gehalten wird.

Einbruchserkennung
In der Datenebene sind elektronische Einbruchmeldesysteme installiert, die sicherheitsrelevante Ereignisse erkennen und automatisch die zuständigen Mitarbeiter alarmieren. Die Ein- und Ausgänge der Serverräume sind durch Geräte gesichert, an denen Personal Multi-Faktor-Authentifizierungsverfahren durchlaufen müssen, bevor sie den Raum betreten oder verlassen können. Diese Geräte lösen einen Alarm aus, wenn die Tür ohne Autorisierung aufgebrochen oder offen gehalten wird. Die Türalarmsysteme sind so konfiguriert, dass sie erkennen, wenn jemand eine Datenebene ohne Multi-Faktor-Autorisierung betritt oder verlässt. In diesem Fall wird umgehend ein Alarm ausgelöst und an die AWS Security Operations Center zur Protokollierung, Analyse und Reaktion gesendet.

Gerätemanagement

Komponentenmanagement
Die AWS-Komponenten werden über ein Inventarmanagementsystem zentral verwaltet. Hier werden Eigentümer, Standort, Status, Wartung und beschreibende Informationen für AWS-Komponenten gespeichert und erfasst. Nach dem Erwerb werden Komponenten gescannt und erfasst. Bei der Wartung werden der Eigentümer, der Status und Problemlösungen zu den Komponenten erfasst.

Zerstörung von Medien
Medienspeichergeräte, auf denen Kundendaten gespeichert sind, werden von AWS als kritisch eingestuft und deshalb über ihren gesamten Lebenszyklus als höchst dringlich behandelt. AWS hat bestehende Normen, wie die Geräte installiert, betrieben und irgendwann zerstört werden, wenn sie nicht mehr verwendet werden. Wenn ein Speichergerät das Ende seines Lebenszyklus erreicht hat, wird es gemäß den in NIST 800-88 beschriebenen Techniken stillgelegt. Medien, auf denen Kundendaten gespeichert wurden, werden erst nach erfolgter Stilllegung aus der Hand von AWS gegeben.

Betriebliche Support-Systeme

Power
Die elektrischen Anlagen unserer Rechenzentren wurden so entwickelt, dass sie vollständig redundant sind und ohne Beeinträchtigung des Betriebs gewartet werden können – und das rund um die Uhr. AWS stellt sicher, dass die Rechenzentren mit einer Notstromversorgung ausgestattet sind, damit im Fall eines Stromausfalls der Betrieb von kritischen Lasten der Anlage gewährleistet ist.

Klimatisierung und Temperatur
Die AWS-Rechenzentren verfügen über Klimaanlagen zur Kontrolle der Betriebstemperatur für Server und andere Hardware, um eine Überhitzung zu vermeiden und das Risiko von Serviceausfällen zu verringern. Temperatur und Luftfeuchtigkeit werden in angemessener Weise vom Personal und den technischen Systemen überwacht und geregelt.

Branderkennung und -bekämpfung
Die AWS-Rechenzentren sind mit automatischen Geräten zur Branderkennung und -bekämpfung ausgestattet. Die Branderkennungssysteme setzen Rauchsensoren in vernetzten, mechanischen und Infrastrukturbereichen ein. Diese Bereiche sind darüber hinaus durch Brandbekämpfungssysteme geschützt.

Leckerkennung
Um Wasserlecks erkennen zu können, stattet AWS seine Rechenzentren mit Wassererkennungssensoren aus. Wenn Wasser entdeckt wird, wird dieses entfernt, um zusätzliche Wasserschäden zu vermeiden.

Infrastrukturwartung

Gerätewartung
AWS überwacht und wartet die elektrischen und mechanischen Geräte präventiv, um den unterbrechungsfreien Betrieb der Systeme in den AWS-Rechenzentren zu gewährleisten. Die

Gerätewartung wird von qualifiziertem Personal entsprechend einem dokumentierten Wartungszeitplan durchgeführt.

UMWELTMANAGEMENT
AWS überwacht elektrische und mechanische Systeme und Anlagen, sodass Probleme sofort erkannt werden. Hierfür werden fortlaufend Audit-Tools und Informationen der Gebäudemanagement- und elektrischen Überwachungssysteme ausgewertet. Es werden vorbeugende Wartungen vorgenommen, um eine kontinuierliche Funktionsfähigkeit der Anlagen sicherzustellen.

Governance und Risiko
Fortlaufendes Risikomanagement für Rechenzentren
Das AWS Security Operations Center führt regelmäßig Bedrohungs- und Schwachstellenprüfungen der Rechenzentren durch. Die fortlaufende Bewertung und Abwehr von potenziellen Schwachstellen erfolgt über die Risikobewertungsaktivitäten der Rechenzentren. Diese Bewertung wird zusätzlich zum Risikobewertungsprozess auf Unternehmensebene durchgeführt, um Risiken für das Unternehmen als Ganzes zu erkennen und zu verwalten. Dabei werden auch regionale behördliche und Umweltrisiken berücksichtigt.

Sicherheitsbescheinigungen von Dritten
Durch Prüfungen der AWS-Rechenzentren durch Dritte, wie in unseren Drittanbieterberichten dokumentiert, stellt AWS sicher, dass angemessene Sicherheitsmaßnahmen implementiert wurden, die zum Erwerb von Sicherheitszertifikaten erforderlich sind. Abhängig vom Compliance-Programm und dessen Anforderungen können externe Prüfer die Entsorgung von Medien testen, die Aufzeichnungen der Sicherheitskameras prüfen, die Eingänge und Korridore eines Rechenzentrums beobachten, die elektronischen Zugangskontrollgeräte testen und die Anlagen des Rechenzentrums untersuchen.

Datenhoheit
Sie entscheiden, ob Ihre Kundendaten in einer oder mehreren AWS-Regionen auf der ganzen Welt gespeichert werden sollen. Außerdem können Sie AWS-Services mit der Gewissheit nutzen, dass Ihre Kundendaten in der von Ihnen ausgewählten AWS-Region verbleiben. Eine kleine Zahl von AWS-Services beinhaltet die Übertragung von Daten, unter anderem, um die Services weiter zu entwickeln und zu verbessern. Sie können jedoch jederzeit ihre Zustimmung zu diesen Datentransfers zurückziehen, solange sie keinen unverzichtbaren Teil des Service darstellen (beispielsweise bei Content Delivery Services). Wir verbieten den Fernzugriff von AWS-Mitarbeitern auf die Kundendaten zu jedem Zweck, einschließlich der Serverwartung. Der Zugriff wird lediglich gestattet, wenn die Kunden dies ausdrücklich wünschen oder er notwendig ist, um Betrug oder Missbrauch zu verhindern beziehungsweise die Einhaltung von Gesetzen ihn erforderlich machen. Wenn wir Informationsanfragen von Strafverfolgungsbehörden erhalten, widersprechen wir diesen grundsätzlich, wenn die Anfragen im Widerspruch zu geltendem Recht stehen, zu allgemein formuliert sind oder wir andere gewichtige Gründe dafür sehen. Zudem stellen wir einen halbjährlichen Bericht über Informationsanfragen zur Verfügung, der die Art und Anzahl der Informationsanfragen beschreibt, die AWS von Strafverfolgungsbehörden erhält.

Sicherheit
Bei AWS hat Sicherheit oberste Priorität. Die Sicherheit in der Cloud ist eine geteilte Verantwortung von AWS und unseren Kunden. Finanzdienstleister, Gesundheitsdienstleister und Behörden gehören zu den Kunden, die uns einige ihrer sensibelsten Informationen anvertrauen. Mit unseren umfassenden Services können Sie Ihre Fähigkeit verbessern, zentrale Sicherheits-, Vertraulichkeits- und Compliance-Anforderungen zu erfüllen, sei es durch Amazon GuardDuty oder unser AWS-Nitro-System, die zugrunde liegende Plattform für unsere EC2-Instances. Unser Nitro-System ist so ausgelegt, dass die Workload vertraulich behandelt wird und kein Bediener Zugang hat. Beim Nitro-System gibt es keinen Mechanismus, mit dem sich Systeme oder Personen bei EC2-Servern anmelden, den Speicher von EC2-Instances auslesen oder auf Daten zugreifen können, die im Instance-Speicher und in verschlüsselten EBS-Volumes gespeichert sind. Darüber hinaus ermöglichen Services wie AWS CloudHSM und AWS Key Management Service die sichere Generierung und Verwaltung von Verschlüsselungsschlüsseln. Und schließlich bieten AWS Config und AWS CloudTrail Überwachungs- und Protokollierungsfunktionen für Compliance und Audits.

Datenkontrolle und Ablage
Mit AWS haben Sie die Kontrolle über Ihre Daten. Mithilfe der leistungsstarken AWS-Services und -Tools können Sie bestimmen, wo die Daten gespeichert werden, wie sie gesichert sind und wer Zugriff darauf hat. Mit Services wie AWS Identity and Access Management (IAM) können Sie den Zugriff auf AWS-Services und -Ressourcen sicher verwalten. AWS CloudTrail und Amazon Macie ermöglichen Compliance, Erkennung und Auditing, während AWS CloudHSM und AWS Key Management Service (KMS) die sichere Generierung und Verwaltung von Verschlüsselungsschlüsseln erlauben. AWS Control Tower bietet Governance und Kontrollen für die Datenresidenz.

Datenschutz
Wir legen die Messlatte für den Datenschutz kontinuierlich höher mit Services und Funktionen, die es Ihnen ermöglichen, Ihre eigenen Datenschutzkontrollen zu implementieren, einschließlich erweiterter Zugriffs-, Verschlüsselungs- und Protokollierungsfunktionen. Wir machen es einfach, Daten bei der Übertragung und im Ruhezustand zu verschlüsseln, indem wir Schlüssel verwenden, die entweder von AWS oder vollständig von Ihnen verwaltet werden. Sie können eigene Schlüssel mitbringen, die außerhalb von AWS erzeugt und verwaltet wurden. Wir implementieren konsistente und skalierbare Prozesse zur Verwaltung des Datenschutzes. Dazu gehört die Art und Weise, wie Daten erfasst, verwendet, abgerufen, gespeichert und gelöscht werden. Wir bieten eine Vielzahl von Best-Practice-Dokumenten, Schulungen und Anleitungen, die Sie zum Schutz Ihrer Daten nutzen können, z. B. die Säule „Sicherheit“ des AWS-Well-Architected-Framework. Wir verarbeiten Kundendaten – d. h. alle personenbezogenen Daten, die Sie in Ihr AWS-Konto hochladen – nur nach Ihren dokumentierten Anweisungen. Ihre Daten werden von uns nicht abgerufen, nicht verwendet und nicht ohne Ihre Zustimmung weitergegeben, sofern dies nicht zur Verhinderung von Betrug und Missbrauch oder zur Einhaltung von Gesetzen erforderlich ist. Einzelheiten entnehmen Sie unserer AWS-Kundenvereinbarung und dem DSGVO-Zusatz zur Datenverarbeitung von AWS. Tausende von Kunden, die der Datenschutz-Grundverordnung (DSGVO), PCI und HIPAA unterliegen, nutzen AWS-Services für diese Art von Workloads. AWS hat eine Vielzahl international anerkannter Zertifizierungen und Akkreditierungen erhalten, die die Einhaltung strenger internationaler Standards belegen. Dazu zählen ISO 27017 für Cloud-Sicherheit, ISO 27701 für Datenschutzmanagement und ISO 27018 für Cloud-Datenschutz. Wir nutzen keine Kundendaten und leiten daraus keine Informationen für Marketing- oder Werbezwecke ab.

AWS Digital Sovereignty Pledge: Kontrolle ohne Kompromisse
Wir waren immer der Meinung, dass die Cloud ihr volles Potenzial nur dann erschließen kann, wenn Kunden die volle Kontrolle über ihre Daten haben. Diese Datensouveränität des Kunden genießt bei AWS schon seit den Anfängen der Cloud Priorität, als wir der einzige große Anbieter waren, bei dem Kunden sowohl Kontrolle über den Speicherort als auch über die Übertragung ihrer Daten hatten. Die Bedeutung dieser Grundsätze hat über die vergangenen 16 Jahre stetig zugenommen: Die Cloud ist im Mainstream angekommen, sowohl Gesetzgeber als auch Regulatoren entwickeln ihre Vorgaben zu IT-Sicherheit und Datenschutz stetig weiter.

Kontrolle bzw. Souveränität über digitale Ressourcen ist heute wichtiger denn je.

Unsere Innovationen und Entwicklungen haben stets darauf abgezielt, unseren Kunden eine Cloud zur Verfügung zu stellen, die skalierend und zugleich verlässlich global nutzbar ist. Dies beinhaltet auch unseren Kunden die Kontrolle zu gewährleisten die sie benötigen, damit sie alle ihre regulatorischen Anforderungen erfüllen können. Regulatorische Anforderungen sind länder- und sektorspezifisch. Vielerorts – wie auch in Europa – entstehen neue Anforderungen und Regularien zu digitaler Souveränität, die sich rasant entwickeln. Kunden sehen sich einer hohen Anzahl verschiedenster Regelungen ausgesetzt, die eine enorme Komplexität mit sich bringen. Innerhalb der letzten achtzehn Monate haben sich viele unserer Kunden daher mit der Sorge an uns gewandt, vor eine Wahl gestellt zu werden: Entweder die volle Funktionalität und Innovationskraft von AWS zu nutzen, oder auf funktionseingeschränkte „souveräne“ Cloud-Lösungen zurückzugreifen, deren Kapazität für Innovation, Transformation, Sicherheit und Wachstum aber limitiert ist. Wir sind davon überzeugt, dass Kunden nicht vor diese „Wahl“ gestellt werden sollten.

Deswegen stellen wir heute den „AWS Digital Sovereignty Pledge“ vor – unser Versprechen allen AWS Kunden, ohne Kompromisse die fortschrittlichsten Souveränitäts-Kontrollen und Funktionen in der Cloud

anzubieten.

AWS bietet schon heute eine breite Palette an Datenschutz-Funktionen, Zertifizierungen und vertraglichen Zusicherungen an, die Kunden Kontrollmechanismen darüber geben, wo ihre Daten gespeichert sind, wer darauf Zugriff erhält und wie sie verwendet werden. Wir werden diese Palette so erweitern, dass Kunden überall auf der Welt, ihre Anforderungen an Digitale Souveränität erfüllen können, ohne auf Funktionsumfang, Leistungsfähigkeit, Innovation und Skalierbarkeit der AWS Cloud verzichten zu müssen. Gleichzeitig werden wir weiterhin daran arbeiten, unser Angebot flexibel und innovativ an die sich weiter wandelnden Bedürfnisse und Anforderungen von Kunden und Regulatoren anzupassen.

Sovereign-by-design
Wir werden den „AWS Digital Sovereignty Pledge" so umsetzen, wie wir das seit dem ersten Tag machen und die AWS Cloud gemäß unseres „sovereign-by-design" Ansatz fortentwickeln. Wir haben von Anfang an, durch entsprechende Funktions- und Kontrollmechanismen für spezielle IT-Sicherheits- und Datenschutzanforderungen aus den verschiedensten regulierten Sektoren Lösungen gefunden, die besonders sensiblen Branchen wie beispielsweise dem Finanzsektor oder dem Gesundheitswesen frühzeitig ermöglichten, die Cloud zu nutzen. Auf dieser Basis haben wir die AWS Verschlüsselungs- und Schlüsselmanagement-Funktionen entwickelt, Compliance-Akkreditierungen erhalten und vertragliche Zusicherungen gegeben, welche die Bedürfnisse unserer Kunden bedienen. Dies ist ein stetiger Prozess, um die AWS Cloud auf sich verändernde Kundenanforderungen anzupassen. Ein Beispiel dafür sind die Data Residency Guardrails, um die wir AWS Control Tower Ende letzten Jahres erweitert haben. Sie geben Kunden die volle Kontrolle über die physikalische Verortung ihrer Daten zu Speicherungs- und Verarbeitungszwecken. Dieses Jahr haben wir einen Katalog von AWS Diensten veröffentlicht, die den Cloud Infrastructure Service Providers in Europe (CISPE) erfüllen. Damit verfügen Kunden über eine unabhängige Verifizierung und zusätzliche Versicherung, dass unsere Dienste im Einklang mit der DSGVO verwendet werden können. Diese Instrumente und Nachweise stehen schon heute allen AWS Kunden zur Verfügung.

Wir haben uns ehrgeizige Ziele für unsere Roadmap gesetzt und investieren kontinuierlich in Funktionen für die Verortung von Daten (Datenresidenz), granulare Zugriffsbeschränkungen, Verschlüsselung und Resilienz:

1. Kontrolle über den Ort der Datenspeicherung

Bei AWS hatten Kunden immer schon die Kontrolle über Datenresidenz, also den Ort der Datenspeicherung. Aktuell können Kunden ihre Daten z.B. in 8 bestehenden Regionen innerhalb Europas speichern, von denen 6 innerhalb der Europäischen Union liegen. Wir verpflichten uns dazu, noch mehr Dienste und Funktionen zur Verfügung zustellen, die dem Schutz der Daten unserer Kunden dienen. Ebenso verpflichten wir uns, noch granularere Kontrollen für Datenresidenz und Transparenz auszubauen. Wir werden auch zusätzliche Kontrollen für Daten einführen, die insbesondere die Bereiche Identitäts- und Abrechnungs-Management umfassen.

2. Verifizierbare Kontrolle über Datenzugriffe

Mit dem AWS Nitro System haben wir ein innovatives System entwickelt, welches unberechtigte Zugriffsmöglichkeiten auf Kundendaten verhindert: Das Nitro System ist die Grundlage der AWS Computing Services (EC2). Es verwendet spezialisierte Hardware und Software, um den Schutz von Kundendaten während der Verarbeitung auf EC2 zu gewährleisten. Nitro basiert auf einer starken physikalischen und logischen Sicherheitsabgrenzung und realisiert damit Zugriffsbeschränkungen, die unautorisierte Zugriffe auf Kundendaten auf EC2 unmöglich machen – das gilt auch für AWS als Betreiber. Wir werden darüber hinaus für weitere AWS Services zusätzliche Mechanismen entwickeln, die weiterhin potentielle Zugriffe auf Kundendaten verhindern und nur in Fällen zulassen, die explizit durch Kunden oder Partner ihres Vertrauens genehmigt worden sind.

3. Möglichkeit der Datenverschlüsselung überall und jederzeit

Gegenwärtig können Kunden Funktionen und Kontrollen verwenden, die wir zur Verschlüsselung von Daten

während der Übertragung, persistenten Speicherungen oder Verarbeitung in flüchtigem Speicher anbieten. Alle AWS Dienste unterstützen schon heute Datenverschlüsselung, die meisten davon auf Basis der Customer Managed Keys – d.h. Schlüssel, die von Kunden verwaltet werden und für AWS nicht zugänglich sind. Wir werden auch in diesem Bereich weiter investieren und Innovationen vorantreiben. Es wird zusätzliche Kontrollen für Souveränität und Verschlüsselung geben, damit unsere Kunden alles jederzeit und überall verschlüsseln können – und das mit Schlüsseln, die entweder durch AWS oder durch den Kunden selbst bzw. ausgewählte Partner verwaltet werden können.

4. Resilienz der Cloud

Digitale Souveränität lässt sich nicht ohne Ausfallsicherheit und Überlebensfähigkeit herstellen. Die Kontrolle über Workloads und hohe Verfügbarkeit z.B. in Fällen von Lieferkettenstörungen, Netzwerkausfällen und Naturkatastrophen ist essenziell. Aktuell bietet AWS die höchste Netzwerk-Verfügbarkeit unter allen Cloud-Anbietern. Jede AWS Region besteht aus mehreren Availability Zones (AZs), die jeweils vollständig isolierte Partitionen unserer Infrastruktur sind. Um Probleme besser zu isolieren und eine hohe Verfügbarkeit zu erreichen, können Kunden Anwendungen auf mehrere AZs in derselben Region verteilen. Kunden, die Workloads on-premises oder in Szenarien mit sporadischer Netzwerk-Anbindung betreiben, bieten wir Dienste an, welche auf Offline-Daten und Remote Compute und Storage Anwendungsfälle angepasst sind. Wir werden unser Angebot an souveränen und resilienten Optionen ausbauen und fortentwickeln, damit Kunden den Betrieb ihrer Workloads auch bei Trennungs- und Disruptionsszenarien aufrechterhalten können.

Vertrauen durch Transparenz und Zusicherungen
Der Aufbau eines Vertrauensverhältnisses mit unseren Kunden, ist die Grundlage unserer Geschäftsbeziehung bei AWS. Wir wissen, dass der Schutz der Daten unserer Kunden der Schlüssel dazu ist. Wir wissen auch, dass Vertrauen durch fortwährende Transparenz verdient und aufgebaut wird. Wir bieten schon heute transparenten Einblick, wie unsere Dienste Daten verarbeiten und übertragen. Wir werden auch in Zukunft Anfragen nach Kundendaten durch Strafverfolgungsbehörden und Regierungsorganisationen konsequent anfechten. Wir bieten Rat, Compliance-Nachweise und vertragliche Zusicherungen an, damit unsere Kunden AWS Dienste nutzen und gleichzeitig ihre Compliance und regulatorischen Anforderungen erfüllen können. Wir werden auch in Zukunft die Transparenz und Flexibilität an den Tag legen, um auf sich weiterentwickelnde Datenschutz- und Soveränitäts-Regulierungen passende Antworten zu finden.

Den Wandel als Team bewältigen
Regulatorik, Technologie und Risiken sind stetigem Wandel unterworfen: Kunden dabei zu helfen, ihre Daten in diesem Umfeld zu schützen, ist Teamwork. Wir würden nie erwarten, dass unsere Kunden das alleine bewältigen müssen. Unsere Partner genießen hohes Vertrauen und spielen eine wichtige Rolle dabei, Lösungen für Kunden zu entwickeln. Zum Beispiel bietet T-Systems in Deutschland Data Protection as a Managed Service auf AWS an. Das Angebot umfasst Hilfestellungen bei der Konfiguration von Kontrollen zur Datenresidenz, Zusatzdienste im Zusammenhang mit der Schlüsselverwaltung für kryptographische Verfahren und Rat bei der Erfüllung von Anforderungen zu Datensouveränität in der AWS Cloud. Wir werden die Zusammenarbeit mit lokalen Partnern, die besonderes Vertrauen bei unseren gemeinsamen Kunden genießen, intensivieren, um bei der Erfüllung der Digitalen Souveräntitätsanforderungen zu unterstützen.

Wir verpflichten uns dazu unseren Kunden bei der Erfüllung ihre Anforderungen an digitale Souveränität zu helfen. Wir werden weiterhin Souveränitäts-Funktionen, Kontrollen und Zusicherungen für die globale AWS Cloud entwickeln, die das gesamte Leistungsspektrum von AWS erschließen.