timebutler

Technical and Organizational Measures

In accordance with article 32 (1) of the General Data Protection Regulation (GDPR) for Processors (Article 30 (2)(d))

(Translated version from German version 1.8 | translation without guarantee | status: 11/2026)

Details of the Data Processor

Name	Timebutler GmbH
Street	Rathausgasse 1
Postal code	12529
City	Schönefeld
Handelsregister:	Amtsgericht Cottbus, HRB 18094 CB
Email address	info@timebutler.de
Website	www.timebutler.com

Terminology

This document uses the terminology and definitions as set out in the General Data Protection Regulation (hereinafter referred to as "GDPR"). In addition, the following terms are defined as:

- "Processor" refers to the data processor, as specified above in this document;
- "Controller" refers to the data controller under the GDPR who has entered into a data processing agreement with the processor;
- "Software" refers to the SaaS solution provided by the processor to the controller for the purpose of carrying out data processing activities.

To ensure the protection of the controller's data, the following technical and organizational measures are bindingly defined for the processor's systems:

1. Confidentiality

A. **Physical Access Control**
This includes all measures to ensure that unauthorized persons do not gain access to data processing systems where the controller's personal data is processed.

Access control by the hosting provider:
The data processing systems used to process the controller's personal data are operated in a certified data center by Amazon Web Services (AWS), which has comprehensive security protocols for its hosting services.
AWS operates numerous data centers and is a market leader in the hosting provider segment. Thousands of companies rely on AWS hosting services.
AWS ensures a high level of physical access control to its data centers.
Detailed information about access controls can be found in the annex titled "AWS Access Controls, System Access, Data Protection" included in this document.

Access control by the processor:
The controller's personal data is processed exclusively on the aforementioned servers in the data centers of the hosting provider.
No personal data is permanently stored or processed on-site in the processor's office spaces.

Access to the personal data is solely via the processor's workstation computers.

Access to office premises is protected against unauthorized entry by locking systems.

There are no customer visits to the office premises, as the software is provided solely via the internet, and no on-site meetings are offered. Instead, all customer interactions are conducted via virtual conferencing tools without physical presence. Should this approach change and visitors be received on-site, the processor will maintain a visitor log, and all visitors will be accompanied by a staff member throughout the entire duration of their visit.

B. **Access Control**
This includes measures to prevent unauthorized individuals from using data processing systems and procedures.

Access control by the hosting provider:
The data processing systems used to handle the controller's personal data are operated in a certified data center by Amazon Web Services (AWS), which implements comprehensive security measures for its hosting services.

AWS operates numerous data centers and is a market leader in the hosting provider sector. Thousands of companies rely on AWS for their hosting needs.

Accordingly, AWS offers a high standard of security when it comes to access control to its data centers. Detailed information on physical and system access controls can be found in the annex titled "AWS Access Controls, System Access, Data Protection" included in this document.

Access Control by the Processor:
Access to the hosting systems, on which the software provided to the controller is operated, is granted exclusively via workstation computers. These can only be unlocked using a username and password.

The workstation computers are provided by the employer. Personal devices of employees are not used (i.e., no "Bring Your Own Device" or BYOD policy).

Access from these workstations to the hosting provider's systems is carried out solely via SSL-secured (Secure Socket Layer) connections. Access to the hosting provider's systems is only possible with personal access credentials, in accordance with the authentication rules described in this section. These credentials are known only to the processor and the employees responsible for maintaining the systems.

Access to systems that contain customer data or that can access customer data is protected by strong authentication. Where applicable, access uses central single sign-on based on the processor's Google Workspace (SAML). Google Workspace enforces two-factor authentication for all accounts. Where single sign-on is not applicable, access requires a username, a password and, where applicable, a second authentication factor (two-factor authentication).

All employees of the processor are contractually obligated to maintain data confidentiality. A sample template of the employee confidentiality agreement, which is signed by every employee, is available to the controller (accessible at www.timebutler.de/avv/tom).

The processor uses a user management system. When an employee leaves the company, all access rights are revoked. Each user account is unique and assigned to a specific individual.

Workstations are equipped with an automatic lock mechanism (automatic screen lock after a defined period of inactivity). Operating system updates and security-relevant software patches are applied automatically and kept up to date.

Access to the workstation computers is only possible using a username and password. All workstation drives are automatically and fully encrypted to prevent unauthorized access to data and login credentials in case of loss.

Password use is governed by a strict password policy.

All systems are protected by a firewall, and secure configuration of operating systems and application software is ensured in accordance with vendor recommendations and best practices.

C. **Access Control**

This includes measures that ensure only authorized individuals can access the personal data within the scope of their access rights when using data processing systems.

The processor has access to the hosting provider's systems on which the software is operated that processes and stores the data provided by the controller.

Employees of the processor have access to these systems in order to perform server maintenance, software upkeep, data management, further development, system administration, and other related tasks.

All employees of the processor are contractually bound to maintain data confidentiality. A sample template of the employee confidentiality agreement, which is signed by each employee, is available to the controller (accessible at www.timebutler.de/avv/tom).

An authorization concept ensures that only authorized employees can access the necessary systems and data. The processor is able to identify and adjust access rights and permissions for its employees at any time.

D. **Order Control**

This includes measures to ensure that personal data processed on behalf of the controller is processed strictly according to the controller's instructions.

Order control by the hosting provider:
The hosting provider does not make any changes to the controller's personal data but solely provides the infrastructure required for the technical operation of the servers.

Order control by the processor:
As a rule, the processor does not make changes to the controller's personal data. The processor provides the controller with software functionalities that enable the controller

to independently edit, modify, view, and delete personal data without instructing the processor.

In the rare cases where the controller instructs the processor to edit, modify, or delete personal data, such instructions must be provided in detail and in written form. The processor will clarify any open questions with the controller and agree in writing on the changes to be made. Without fulfilling these conditions, the processor will not perform any changes.

The controller can independently learn about how the software works and understand how the software processes and modifies personal data depending on how it is used by the controller.

E. **Separation Control**
This includes all measures to ensure that the personal data of the controller is processed separately from other customer data.

The software provided by the processor is used by thousands of companies. From the outset, it was designed and implemented for use by multiple organizations via the internet, with built-in multi-tenancy to ensure strict data separation between clients.

User accounts are assigned to different user groups (tenants). Users within a tenant group can only view or edit data belonging to that same group (according to the access rights of their account).
Access to or editing of data from other tenant groups is not possible due to the software architecture, which was implemented with this separation in mind during development.

Since the software was launched in 2003, there has been no known case in which one tenant was able to view, modify, or delete another tenant's data without authorization. The processor updates and reviews the software regularly. The controller is required to promptly notify the processor if they become aware of any issues regarding data or software security.

Development, testing, and production systems are physically and logically separated. Development and testing take place on employees' workstations, while production systems are operated in the hosting provider's data center.

F. **Pseudonymization and Encryption** (*Art. 32 (1) lit. a GDPR, Art. 25 (1) GDPR*)
To fulfill the purposes of the data processing on behalf of the controller, pseudonymization of personal data is not feasible.

Encryption on the Contractor's Systems
All data in the software's database, including personal data, is stored encrypted at rest. The encryption covers the database storage as a whole, so the data cannot be read

from the storage media without the encryption key. In addition, passwords are stored only in a one-way encrypted form, with no possibility of reconstructing the original password. This means the contractor cannot view or convert the passwords into a readable format. The contractor considers this essential, as knowing the password is not necessary for operating the software, and some users may reuse the same password across multiple online services.

In addition to the database, the data is stored in backups. The backups are also stored encrypted, and the one-way encryption of the passwords is retained in the backups as well. The backup is stored on a secured backup system, which cannot be accessed without valid personal access credentials (see “Access Control by the Processor”).

The credentials required to access the system are only known to authorized employees of the contractor. All such employees have signed a confidentiality agreement.

Encryption During Communication Between Systems When Using the Software
When using the software, several systems are involved: the client’s internet browser, the software’s server, and the contractor’s employees’ workstations or end devices, along with the systems that transmit the information via the internet.

To prevent third-party systems—other than those of the contractor and the client—from reading the data, and to ensure that information is delivered securely and without tampering, the contractor ensures that all communication by the software is encrypted using SSL/TLS (Secure Socket Layer / Transport Layer Security).

If any of the client’s systems attempt to establish an unsecured connection, the software will respond with a prompt to use a secure connection, without transmitting any personal data. This response is designed in such a way that the requesting system can automatically switch to a secure connection and repeat the request.

Encryption in Communication via Email
The software sends emails to its users, and thus to the client’s employees.

The processor ensures that email communication can be encrypted using SSL/TLS (Secure Socket Layer / Transport Layer Security), both when sending and receiving emails. This ensures that emails cannot be intercepted or tampered with outside the email processing systems of the client and the processor.

For encrypted transport to be possible, the client must also configure and enable encrypted communication on their email systems. The client is therefore responsible for providing and maintaining transport encryption for sending and receiving emails on their systems.

If transport encryption is not possible on the client's email system, the client has the option to disable email delivery for user accounts: within the software, email notifications can be activated or deactivated for each user in the user profile settings.

2. Integrity (Article 32 (1)(b) GDPR)

A. **Data Transfer Control**
This includes measures to ensure that personal data cannot be read, copied, modified, or removed without authorization during electronic transmission, transport, or storage on data carriers:

The software responsible for processing the data provided by the controller is accessible via the Internet. The software ensures that communication always takes place via an SSL-secured connection using current security standards.

The software also ensures at all times that any user attempting to establish an unsecured connection—either knowingly or unknowingly—is automatically redirected to a secured connection, without transmitting any personal data via the unsecured channel (verification of secure HTTPS communication with every request and automatic redirection of unsecured HTTP requests to secure HTTPS communication).

Access between the contractor's workstations and the systems on which the software and the backup server are operated always occurs via SSL-secured communication.

The software's database is stored encrypted at rest, so personal data cannot be read without authorization from the storage media. Backups are stored using strong encryption that cannot be decrypted in a reasonable time without the private key, even with current technical capabilities. Data transfers from the main server to the backup server are also encrypted.

B. **Input Control**
This includes measures that ensure it is possible to retrospectively verify whether and by whom personal data has been entered into, modified in, or removed from data processing systems.

When a new user account is created, the software logs the creator of the account, allowing traceability of who set up the new user.

Additionally, the software tracks the editing history of absence entries — for example, the creation of a business trip entry, the approval of a vacation request, or the rejection of a request to reduce overtime — and displays this history within the system.

However, the software does not log every change made to personal data. For instance, a user can modify their email address, phone number, or department assignment without the system recording which value was changed, by whom, or when.
This especially applies when a user deletes their own account: in that case, the account and all associated personal data must be fully erased, which makes it impossible to log who deleted the account — since doing so would require storing personal data post-deletion.

3. Availability and Recovery (Art. 32 (1)(b) GDPR)

A. **Availability Control**
This includes measures that ensure personal data is protected against accidental destruction or loss.

Availability Control by the Hosting Provider:
The data processing systems used to process the personal data of the controller are operated in a certified data center by Amazon Web Services (AWS), which provides a comprehensive security framework for its hosting services.

AWS operates numerous data centers and is a market leader in the hosting provider segment. Thousands of companies rely on AWS hosting services.

AWS ensures a high level of security standards for controlling access to its data centers. Detailed information about access controls can be found in the appendix "AWS Physical Access Controls, System Access Controls, and Data Protection" included in this document.

Availability Control by the Processor:
The processor (contractor) performs automated backups of all data daily, on a fixed schedule. These backups are automatically transferred to a system specifically designated for data backups. The backup systems are redundant and therefore protected against data loss.

Only the processor has access to the backup systems.

Due to the physical separation of the backup system from the server on which the software is operated, the availability of the data is ensured through the independently stored data backup in the event of a hardware or software failure that results in data loss.

The controller (client) is responsible for regularly backing up their data on storage systems outside the processor’s area of responsibility. The software provides functions via an API (interface) as well as a reporting and download center, enabling the controller to easily and quickly export data from the software.

B. **Recoverability**
This includes measures that ensure personal data can be quickly restored in the event of a physical or technical incident.

The processor uses a technical process that automatically backs up the data daily, on a fixed schedule, to a system that is both physically and logically separated from the live environment. In addition, the processor can restore the data to any point in time within the backup retention period (point-in-time restore). In the event of a physical or technical failure of the live environment system, the data can be restored from the backup server and made available to the controller again.

The processor has developed a recovery plan for physical or technical incidents, which is known to the processor and available at www.timebutler.de/avv/tom. The controller acknowledges that the measures described in the recovery plan meet their requirements.

C. **Deletion Policy**
This includes measures that ensure the correct personal data is deleted at the appropriate time.

Data within the software is deleted exclusively by the controller. The processor does not delete any data unless explicitly instructed to do so by the controller.

Backup data is retained for a limited period and then deleted through automated routines, the functionality of which must be ensured by the processor.

The processor has developed a deletion policy that outlines the measures for properly deleting personal data. This deletion policy is known to the processor and is available at www.timebutler.de/avv/tom.

4. Adaptation to Technological Progress

The technical and organizational measures are subject to technological advancements and ongoing development. In this context, the processor is permitted to implement alternative adequate measures. However, the security level of the defined measures must not be compromised.

ANNEX / AWS Access Controls, Access Management, Data Protection

Amazon Web Services provides the following information on its website:

Secure Design

Site Selection

Prior to choosing a location, AWS performs initial environmental and geographic assessments. Data center locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. Our Availability Zones are built to be independent and physically separated from one another.

Redundancy

Data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Availability

AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

Capacity Planning

AWS continuously monitors service usage to deploy infrastructure to support our availability commitments and requirements. AWS maintains a capacity planning model that assesses our infrastructure usage and demands at least monthly. This model supports planning of future demands and includes considerations such as information processing, telecommunications, and audit log storage.

Business Continuity & Disaster Recovery

Business Continuity Plan

The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

Pandemic Response

AWS incorporates pandemic response policies and procedures into its disaster recovery planning to prepare to respond rapidly to infectious disease outbreak threats. Mitigation strategies include alternative staffing models to transfer critical processes to out-of-region resources, and activation of a crisis management plan to support critical business operations. Pandemic plans reference international health agencies and regulations, including points of contact for international agencies.

Physical Access

Employee Data Center Access

AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the

requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

Third-Party Data Center Access

Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.

AWS GovCloud Data Center Access

Physical access to data centers in AWS GovCloud (US) is restricted to employees who have been validated as being US citizens.

Monitoring & Logging

Data Center Access Review

Access to data centers is regularly reviewed. Access is automatically revoked when an employee's record is terminated in Amazon's HR system. In addition, when an employee or contractor's access expires in accordance with the approved request duration, his or her access is revoked, even if he or she continues to be an employee of Amazon.

Data Center Access Logs

Physical access to AWS data centers is logged, monitored, and retained. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis.

Data Center Access Monitoring

We monitor our data centers using our global Security Operations Centers, which are

responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses.

Surveillance & Detection

CCTV
Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

Data Center Entry Points
Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

Intrusion Detection
Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry and badge before exiting. These devices will sound alarms if the door is forced open without authentication, held open, or opened for exit during an emergency. Door alarming devices are also configured to detect instances where an individual enters a data layer without providing multi-factor authentication or exits without proper badging. Alarms are immediately dispatched to the 24/7 AWS Security Operations Centers for immediate logging, analysis, and response.

Device Management

Asset Management

AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for AWS-owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution.

Media Destruction

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

Operational Support Systems

Power

Our data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

Climate and Temperature

AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Fire Detection and Suppression

AWS data centers are equipped with automatic fire detection and suppression equipment. Fire

detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

Leakage Detection

In order to detect the presence of water leaks, AWS equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.

Infrastructure Maintenance

Equipment Maintenance

AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

Environmental Management

AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment.

Governance & Risk

Ongoing Data Center Risk Management

The AWS Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration.

Third-Party Security Attestation

Third-party testing of AWS data centers, as documented in our third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.

AWS Digital Sovereignty Pledge: Kontrolle ohne Kompromisse

by David Surey on 26 March 2024 | translated from German into English

We have always believed that the cloud can only reach its full potential if customers have full control over their data. This data sovereignty for customers has been a priority at AWS since the early days of the cloud, when we were the only major provider giving customers control over both the location and the transmission of their data. The importance of these principles has steadily increased over the past 16 years: the cloud has become mainstream, and both legislators and regulators are continuously evolving their requirements for IT security and data protection.

Control or sovereignty over digital resources is more important today than ever.

Our innovations and developments have always aimed to provide our customers with a cloud that is scalable and reliably usable worldwide. This also includes ensuring our customers have the control they need to meet all their regulatory requirements. Regulatory requirements vary by country and sector. In many regions — including Europe — new regulations and requirements for digital sovereignty are rapidly evolving. Customers face a large number of diverse rules, resulting in enormous complexity. Over the past eighteen months, many of our customers have expressed concerns about being forced to choose between either leveraging the full functionality and innovative power of AWS or relying on functionally limited “sovereign” cloud solutions that offer limited capacity for innovation, transformation, security, and growth. We firmly believe customers should never have to make this “choice.”

Therefore, today we are introducing the “AWS Digital Sovereignty Pledge” — our promise to all AWS customers to offer the most advanced sovereignty controls and features in the cloud, without compromise.

AWS already offers a broad range of data protection features, certifications, and contractual assurances that give customers control over where their data is stored, who can access it, and how it is used. We will expand this portfolio so that customers worldwide can meet their digital sovereignty requirements without sacrificing functionality, performance, innovation, or scalability of the AWS Cloud. At the same time, we will continue to work on keeping our offerings flexible

and innovative to adapt to the ever-changing needs and requirements of customers and regulators.

Sovereign-by-design

We will implement the “AWS Digital Sovereignty Pledge” in the same way we have since day one, continuing to develop the AWS Cloud according to our “sovereign-by-design” approach. From the beginning, we have found solutions through specific features and control mechanisms tailored to IT security and data protection requirements across various regulated sectors. This early enabled highly sensitive industries - such as finance and healthcare - to adopt the cloud.

Building on this foundation, we developed AWS encryption and key management functions, obtained compliance accreditations, and provided contractual assurances that meet our customers’ needs. This is an ongoing process aimed at adapting the AWS Cloud to evolving customer requirements. For example, in late 2021, we expanded AWS Control Tower with Data Residency Guardrails, giving customers full control over the physical location of their data for storage and processing purposes.

In February 2022, we published a catalog of AWS services that comply with the Cloud Infrastructure Service Providers in Europe (CISPE) Code of Conduct. This gives customers independent verification and additional assurance that our services can be used in accordance with the General Data Protection Regulation (GDPR). These tools and proofs are already available to all AWS customers today.

We have set ambitious goals for our roadmap and continue to invest in features for data localization (data residency), granular access restrictions, encryption, and resilience:

1. Control over data storage location

AWS customers have always had control over data residency—that is, where their data is stored. Currently, customers can store their data in eight existing regions within Europe, six of which are located inside the European Union. We commit to offering even more services and features that protect our customers’ data. Likewise, we commit to expanding more granular controls for data residency and transparency. We will also introduce additional controls for data, especially concerning identity and billing management.

2. Verifiable Control over Data Access

With the AWS Nitro System, we have developed a unique platform that prevents unauthorized access to customer data. Nitro is the foundation of Amazon Elastic Compute Cloud (Amazon EC2). It uses specialized hardware and software to ensure the protection of customer data during processing on EC2. Nitro is based on strong physical and logical security boundaries, implementing access restrictions that make unauthorized access to customer data on EC2 impossible—even for AWS as the operator. Furthermore, we will develop additional

mechanisms for other AWS services to prevent potential unauthorized access to customer data, allowing access only in cases explicitly approved by customers or their trusted partners.

3. Data Encryption Capability Anytime, Anywhere

Currently, we provide customers with features and controls for encrypting data in transit, at rest, or in use in volatile memory. All AWS services already support data encryption, most of which rely on Customer Managed Keys—keys managed by customers and inaccessible to AWS. We will continue to invest and innovate in this area. Additional controls for sovereignty and encryption will be introduced, enabling our customers to encrypt everything anytime and anywhere—with keys managed either by AWS, by the customer themselves, or by selected trusted partners.

4. Cloud Resilience

Digital sovereignty cannot be achieved without fault tolerance and survivability. Control over workloads and high availability - especially in cases of supply chain disruptions, network outages, and natural disasters - is essential. Currently, AWS provides the highest network availability among all cloud providers. Each AWS Region consists of multiple Availability Zones (AZs), each a fully isolated partition of our infrastructure. To better isolate problems and ensure high availability, customers can distribute their applications across multiple AZs within the same region. For customers running workloads on-premises or in scenarios with intermittent network connectivity, we offer services tailored for offline data and remote compute and storage use cases. We commit to expanding and evolving our sovereign and resilient options to enable customers to maintain workload operations even under separation and disruption scenarios.

Trust through Transparency and Assurances

Building a relationship of trust with our customers is the foundation of our business at AWS. We understand that protecting our customers' data is key to that trust. We also know that trust is earned and maintained through ongoing transparency. Today, we already provide clear insights into how our services process and transfer data. We will continue to vigorously challenge requests for customer data from law enforcement and government agencies. We offer guidance, compliance evidence, and contractual assurances to enable our customers to use AWS services while meeting their compliance and regulatory requirements. Going forward, we will maintain transparency and flexibility to respond appropriately to evolving privacy and sovereignty regulations.

Facing Change Together as a Team

Regulations, technology, and risks are constantly evolving—helping customers protect their data in this environment requires teamwork. We would never expect our customers to do this alone. Our partners enjoy a high level of trust and play a critical role in developing solutions for customers. For example, T-Systems (part of Deutsche Telekom) offers Data Protection as a Managed Service on AWS in Germany. This offering includes assistance in configuring controls for data residency, additional services related to cryptographic key management, and guidance

on meeting data sovereignty requirements in the AWS Cloud. We are intensifying collaboration with local partners to support our customers in fulfilling digital sovereignty demands.

We will continue to develop sovereignty features, controls, and assurances for the global AWS Cloud that unlock the full range of AWS capabilities.