Data Protection for your AWS environment

AWS stance on data protection and trust

AWS is aware that customer trust is pivotal to its value proposition. This is why, from the physical infrastructure to the software applications that reside on them, AWS constantly reiterates its commitment to data protection and privacy.

To date, AWS provides more than 50 data protection services. Implemented correctly, these services ensure your business data is safeguarded: against cybercrime, fraudulent usage, and data breaches. Companies are protected from costly legal disputes due to non-compliance with local data protection regulations. AWS helps companies address these important and legitimate concerns in the digital age.

Pinpointing the most relevant data protection services in this portfolio and utilizing them properly requires expert domain knowledge, in-depth technical proficiency with cloud technology. In addition, experience in dealing with data privacy across various industries and regions with very specific regulations and compliance requirements is necessary.

Knowing that there is a plethora of services to protect your data is comforting. But it is key to data protection in the cloud to select the right services, configure them optimally, and implement them seamlessly.

Data protection and security in AWS is based on the shared responsibility model. This means that AWS maintains the security of the cloud infrastructure, and you as the customer manage security within the cloud while using AWS.

T-Systems' Data Protection as a Managed Service mitigates data privacy threats

You may not have the time or resources to devote to an extensive data protection strategy. We can help you with this. You can focus on your primary goal: generating business revenue, improving growth, and enhancing your products and services. Meanwhile we – at T-Systems with our team of security experts – will focus on your data protection needs.

T-Systems can help you optimally setup, configure, implement, deploy, and test the efficacy of your data protection services and recommend best practices for local regulatory compliance. We have gone a step further by defining four solution pillars dedicated to data privacy.

1. **Trusted Cloud Landing Zone**
2. **Data Residency Attestations**
3. **Data Confidentiality**
4. **European Customer Support**

The four pillars of Data Protection as a Managed Service, as defined by T-Systems, are:

T Systems

1 Trusted Cloud Landing Zone

Start your cloud journey in AWS with a Trusted Cloud Landing Zone, configured and operated by T-Systems, built on a well-architected framework integrated to the data privacy and data residency framework.
With our trusted cloud landing zone, you can expect:

1. A **sophisticated identity management** with embedded least privilege access
2. Continuous **traceability**
3. Multi-level security controls
4. **Automated** best practices*
5. **Proactive threat and incident** detection and resolution
6. Restriction of direct or manual access*
7. **Data in storage and in transit** secured via encryption, and access control

**Limit the potential for human error*

2 Data Residency Attestations

Using a T-Systems AWS account, you will have inbuilt controls for data residency from day 1. We can supply you with a data residency dashboard, with which you can obtain:

1. Preventive and detective guardrails for data residency management, such as region whitelisting and service restrictions for compliance (C5, SOC, PCI, etc.)
2. Data residency monitoring and reporting
3. Data residency consultancy

Attestation via Data Residencies Access Report, real-time monitoring on access and flag alerts, localization, and anonymization via external identity provider

3 Data Confidentiality

We can provide guidance and solutions on which cloud encryption tools to use based on the data classification scope. You can rest assured that the right level of encryption is applied to protect your data.

For data confidentiality, you can expect:

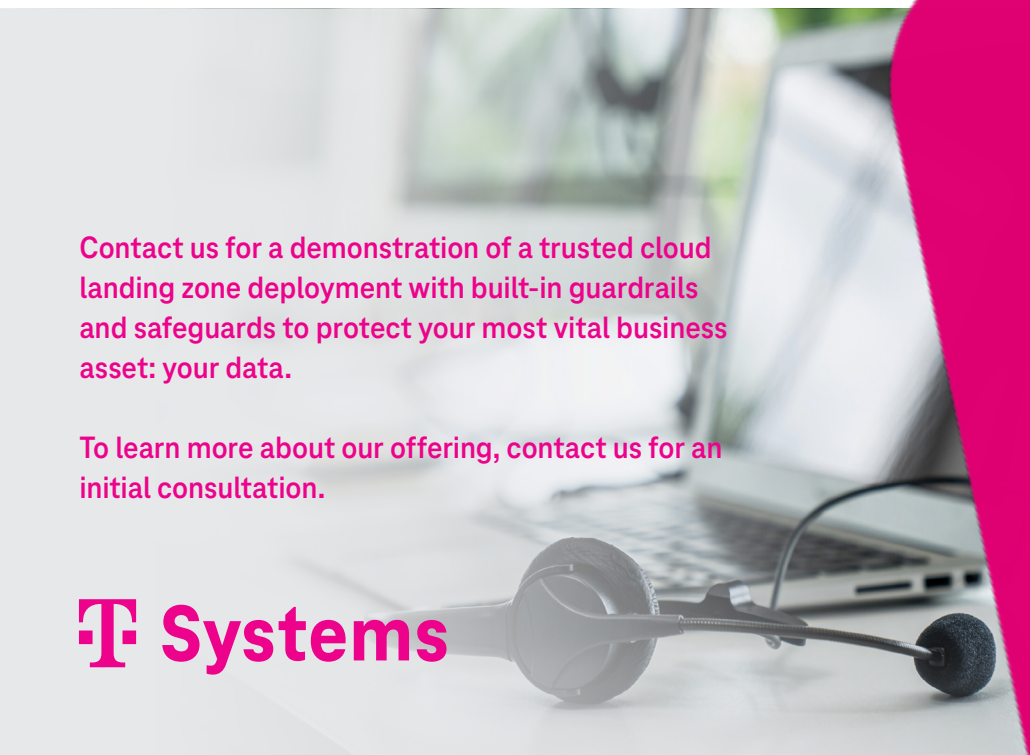
1. **Encryption by default**, ensuring that encryption is activated for all AWS services
2. **Customer managed keys**
3. **Managed storage encryption**
4. **Nitro architecture** for hardware-based isolation
5. **Anonymized IAM data**
6. Permission only **C5/CISPE/SOC** certified AWS Services
7. Data confidentiality and encryption **consultancy**

4 European Customer Support

Your technical and business support team will be based in Europe with a certified AWS partner.

With our Europe-based tech support team, you can expect:

1. Support from an **AWS Digital Sovereignity Competency Partner** in Germany (T-Systems)
2. **24/7 Service Desk**, located in Europe, in your local language
3. **AWS-certified** specialists
4. **Customized SLAs** with RTOs
5. Advice if and when **3rd Level AWS Support** requires **data access** to your account



Contact us for a demonstration of a trusted cloud landing zone deployment with built-in guardrails and safeguards to protect your most vital business asset: your data.

To learn more about our offering, contact us for an initial consultation.

T Systems

QUESTIONS?

For more information, please contact:

Email: info@t-systems.com
Internet: www.t-systems.com

PUBLISHER

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
Germany

Last update 11/2024