



Data Protection

Paul Ahlgren

Security & Compliance Business Acceleration Lead
Nordics & Baltics

Paul Ahlgren

- 40 years in the IT-Industry
- Done it all: Mainframes, Mini's, PC, Web and Cloud
 - Developer, Architect (35 years)
 - 17 years at Digital Equipment Corporation
 - 5 years at AWS (Partner SA and Security & Compliance)
- 20 years in Financial tech
 - Specialized in Securities trading
 - Chief Solutions Architect for Skandiabanken



Sorry to spoil the fun...

- There is no secret sauce.
- All customers, in all European countries use AWS with the standard terms
 - Which should be a relief.

Schrems II – timeline (short version)

- 2000 – EU and USA signs agreement "EU-US Safe Harbor"
- 2001 – EU creates the "Standard Contractual Clauses (SCC)"
- 2010 – Max Schrems – law student during a semester abroad at Santa Clara University
- 2013 – Max filed a complaint against Facebook with the Irish Data Protection Commissioner
- 2015 – Court of Justice of the European Union (CJEU) invalidates EU-US Safe Harbor (now known as Schrems I)
- 2016 – EU and USA signs agreement "EU-US Privacy Shield"
- 2020 – CJEU invalidates the EU-US Privacy Shield (Schrems II)

Schrems II – verdict (July 2020)

- Related to transfer of personal data to outside of the EU/EEA area.
 - SCC are still valid but transfers to some countries requires "supplementary measures"
 - Note that it's the data controller that needs to ensure these measures
 - In regard to transfers to USA the verdict mentions
 - FISA sec. 702
 - Executive order 12333

Schrems II – post-verdict

- 2020/09 – All national Data Protection Authorities publishes initial reactions
- 2020/11 – European Data Protection Board (EDPB) publishes provisional guidelines for transfers in accordance to Schrems II
- 2021/05 – EDPB approves two cloud code of conducts
 - CISPE
 - EU CCoC
- 2021/06 – EU adopts new SCC's
 - Must be used in new contracts as of Sep 27
 - Old SCC's are valid for 15 months after that
 - Only applicable when performing data transfer outside EU/EEA
- 2021/06 – EDPB publishes the final guidelines
- Ongoing negotiations between EU and US for a new agreement

Foreign Sovereign Immunities Act (1976)

- Establishes the limitations as to whether a foreign sovereign nation (or its political subdivisions, agencies, or instrumentalities) may be sued in U.S. courts—federal or state.

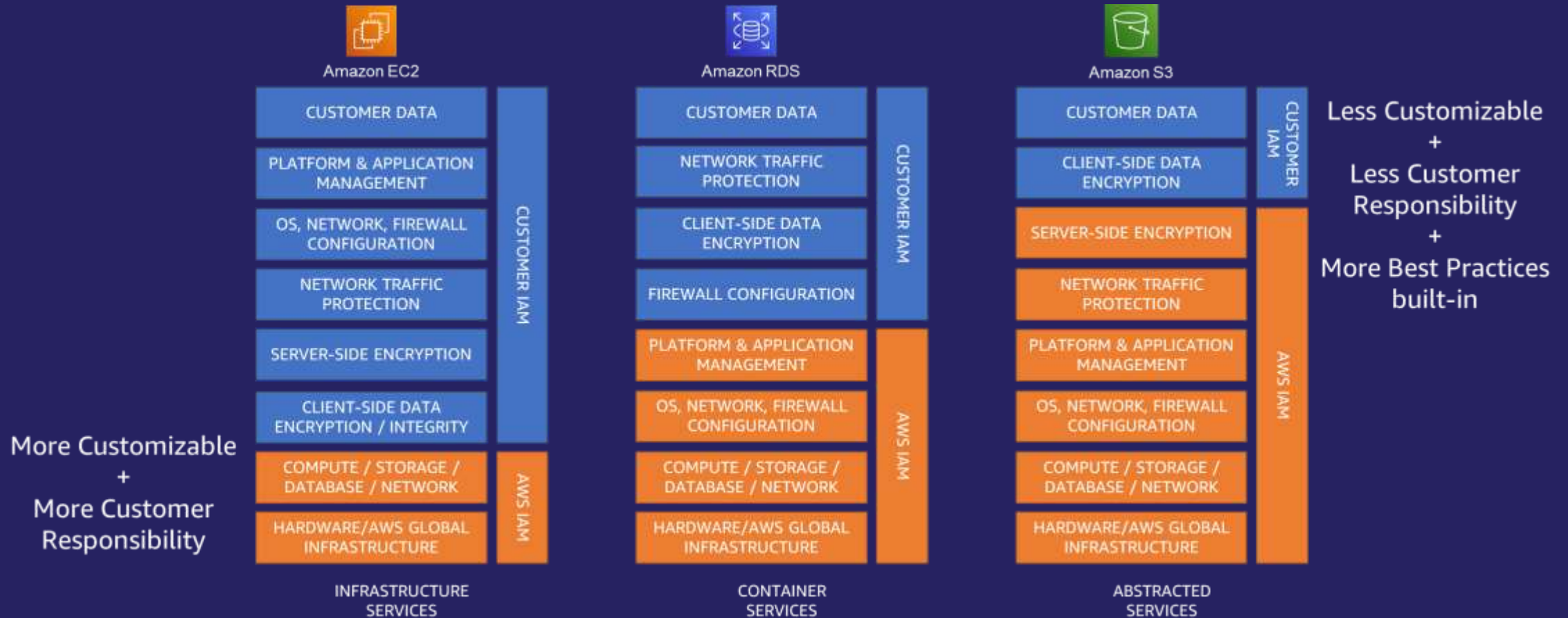
The FSIA only applies to lawsuits involving a "foreign state." The FSIA defines "foreign state" to include three entities:

- A foreign state
- A political subdivision of a foreign state
- An "agency or instrumentality" of a foreign state
- "Agency or instrumentality" is then defined as any entity which:
 - Has a separate legal identity and is either:
 - An "organ of a foreign state or political subdivision"
 - Has a "majority of [...] shares or other ownership interest" owned by a foreign state or political subdivision

Reading







- FISA sec. 702:
 - <https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF>
- CLOUD Act:
 - <https://www.justice.gov/dag/page/file/1153466/download>
- Executive Order 12333:
 - <https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF>
- Foreign Sovereign Immunities Act:
 - U.S.C 28. §1330,§1391(f), 1441(d),§1602-1611

Shared Responsibility Model – or rather models...



<https://aws.amazon.com/whitepapers/aws-security-best-practices/>

AWS security, identity, and compliance solutions

 Identity and access management	 Detective controls	 Infrastructure protection	 Data protection	 Incident response	 Compliance
<ul style="list-style-type: none"> AWS Identity and Access Management (IAM) AWS Single Sign-On AWS Organizations AWS Directory Service Amazon Cognito AWS Resource Access Manager 	<ul style="list-style-type: none"> AWS Security Hub Amazon GuardDuty Amazon Inspector Amazon CloudWatch AWS Config AWS CloudTrail VPC Flow Logs AWS IoT Device Defender 	<ul style="list-style-type: none"> AWS Firewall Manager AWS Network Firewall AWS Shield AWS WAF – Web application firewall Amazon Virtual Private Cloud AWS PrivateLink AWS Systems Manager 	<ul style="list-style-type: none"> Amazon Macie AWS Key Management Service (KMS) AWS CloudHSM AWS Certificate Manager AWS Secrets Manager AWS VPN Server-Side Encryption 	<ul style="list-style-type: none"> Amazon Detective CloudEndure DR AWS Config Rules AWS Lambda 	<ul style="list-style-type: none"> AWS Artifact AWS Audit Manager

Inherit global security and compliance controls



AWS and data protection



TL; DR

- AWS don't move data from the country where the customer stores it unless agreed with the customer
- AWS Support don't have access to customer data unless the customer requests us to do so
- AWS contractually commits to challenging legal requests in accordance with Schrems II and GDPR
- AWS is certified for ISO 27701 which provides proof that we handle data in accordance with GDPR

Customer Supplementary Measures

Control

Encryption

Monitor & Logging

SCC

AWS Services including Security and Encryption

AWS Organizational Procedures

AWS Contract

AWS DPA

AWS DPA Supplement

AWS Privacy Notice

AWS Compliance Programs

AWS Organizational
Procedures

AWS Technical Security

AWS Virtualization (Nitro)

AWS Custom Hardware

AWS Infrastructure

Resources



AWS Customer Agreement

- Available on the AWS website
- <https://aws.amazon.com/agreement/> - customer agreement
- <https://aws.amazon.com/service-terms/> - service terms
- The data processing addendum (includes SCC)
 - https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
 - https://d1.awsstatic.com/Supplementary_Addendum_to_the_AWS_GDPR_DPA.pdf
- <https://aws.amazon.com/privacy/> - privacy notice
- <https://aws.amazon.com/legal/> - additional information

AWS Compliance Web Pages

- <https://aws.amazon.com/compliance/eu-data-protection/>
- <https://aws.amazon.com/compliance/gdpr-center/>
- <https://aws.amazon.com/compliance/data-privacy/>
- <https://aws.amazon.com/compliance/>

Sub-processors

- <https://aws.amazon.com/compliance/sub-processors/>
 - AWS entities and processing
 - AWS Support center locations
 - Third-party service providers
 - Processing takes place in the region selected by the customer
 - Amazon Pinpoint, Amazon Chime, Amazon Simple Notification service
 - A2P Messaging
 - Amazon Location Service
 - Geolocation services (maps and places)

Service improvement

- Some AI Services collect data, which may lead to data transfer, to improve the services.
 - Service terms: 50.3, (52), 54.7
- The customer can opt out of participation
 - through the console (read the documentation)
 - https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_a_i-opt-out.html
 - by contacting AWS support

CISPE

- In May 2021 EDPB approved two Cloud Code of Conducts (GDPR, art. 40&41)
 - CISPE (AWS is a founder and is certified by it)
 - EU CCoC (Microsoft and Google)
- Links:
 - <https://aws.amazon.com/compliance/cispe/>
 - <https://cispe.cloud/publicregister/>
 - <https://aws.amazon.com/blogs/security/aws-announces-cispe-membership-and-compliance-with-first-ever-code-of-conduct-for-data-protection-in-the-cloud/>
 - https://edpb.europa.eu/news/news/2020/european-data-protection-board-thirty-seventh-plenary-session-guidelines-controller_en

AWS Artifact

AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include (but not limited to:

- ISO 9001, 27001, 27017, 27018
- SOC 1 & 2 (& 3)
- C5
- PCI DSS
- ... and many more



ISO/IEC 27701: 2019

- ISO/IEC 27701:2019 specifies requirements and guidelines to establish and continuously improve a Privacy Information Management System (PIMS), including processing of personally identifiable information/personal information (PII), and is an extension of the ISO/IEC 27001 and ISO/IEC 27002 standards for information security management.
- **AWS as a data processor** – When customers use AWS services to process personal data in the content they upload to the AWS services, AWS acts as a data processor. Customers can use the controls available in AWS services, including security configuration controls, for the handling of personal data. Under these circumstances, the customer may act as a data controller or data processor itself, and AWS acts as a data processor or sub-processor.
- **AWS as a data controller** – When AWS collects personal data and determines the purposes and means of processing that personal data – for example, when AWS stores account information (e.g. email addresses provided during the account registration) for account registration, administration, services access, or contact information for the AWS account to provide assistance through customer support activities – it acts as a data controller.

Blog posts

- EU Data protection:

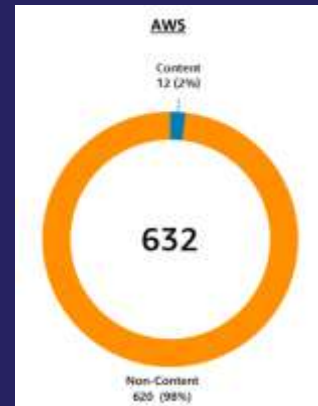
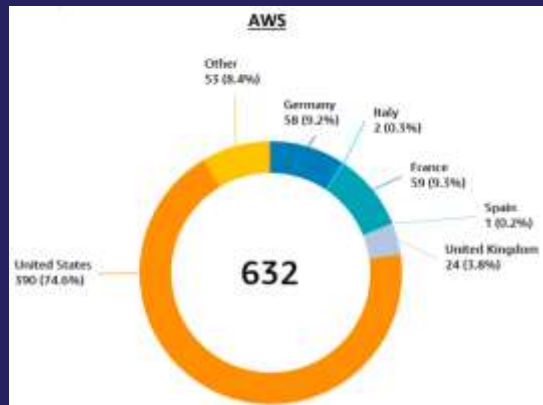
- <https://aws.amazon.com/blogs/security/how-aws-is-helping-eu-customers-navigate-the-new-normal-for-data-protection/>
- <https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/>

- GAIA-X:

- <https://aws.amazon.com/blogs/publicsector/what-next-europes-data-revolution-aws-joins-gaia-x-initiative/>

Law enforcement Information requests

<https://www.amazon.com/gp/help/customer/display.html?nodeId=GYS DRGWQ2C2CRYEF>
https://d1.awsstatic.com/Information_Request_Report_June_2021_x.pdf



How many requests resulted in the disclosure to the U.S. government of enterprise content data located outside the United States?

None.



Thank you!