Data Transfer Impact Assessment (DTIA) on the transfer of Content Data to the USA processed in Amazon EC2, Amazon S3, and Amazon RDS

Step 1: Describe the intended transfer

a)	Data exporter (or the sender in case of a relevant onward transfer):	Dutch government organisation [X]
b)	Country of data exporter:	Netherlands
c)	Data importer (or the recipient in case of a relevant onward transfer):	Amazon Web Services, Inc. ("AWS, Inc.", abbreviated in this DTIA to: "AWS")
d)	Country of data importer:	USA. Seller of Record is Amazon Web Services EMEA SARL ("AWS Europe"), a Luxembourg-based AWS entity. Both AWS and AWS Europe are wholly owned subsidiaries of Amazon.com, Inc. AWS works with Regions, a physical location in a country where data centers are clustered. AWS has Regions in the EU. Each AWS Region consists of a minimum of three, isolated, and physically separate AZs within a geographic area. AWS calls each group of logical data centers an Availability Zone.
e)	Context and purpose of the transfer:	Employees of the MOJ or any other Governmental entity that use Amazon EC2, Amazon S3, and Amazon RDS to store and process Content Data.
f)	Categories of data subjects concerned:	Employees of the Dutch government , possibly external data subjects whose data are processed by MOJ or any other governmental organisation as Content Data.
g)	Categories of personal data transferred:	Any kind of Content Data actively provided by the customer to the 3 tested AWS services
h)	Sensitive and special categories of personal data:	Data stored in the 3 AWS services may include classified information, personal data of a sensitive nature (for example location data, salary information, company or personal confidential information), data relating to children under 16 years and special categories of data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, Art. 9 GDPR). Content Data may also include personal data relating to criminal convictions and offences or related security measures (Art. 10 GDPR).
i)	Technical implementation of the transfer:	Customers of the 3 AWS services can decide for themselves within which availability zone they want to store their data. AWS does not operate a data centre in the Netherlands. Privacy Company chose to set-up the S3 buckets in the eu-central-1 region, an AWS Region based in Europe (Frankfurt). AWS does not have a Region in the Netherlands, but customers may choose to use AWS services deployed at an AWS Edge Location (available in The Netherlands), an AWS Local Zone (announced for Amsterdam, The Netherlands), or AWS Hybrid Solutions from customer or partner premises. Reference: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/an AWS data centre in Frankfurt
j)	Technical and organizational measures in place:	AWS provides HTTPS endpoints using the TLS protocol for communication, which provides encryption in transit when customers use AWS APIs. Customers should use TLS 1.2 or later. Customers can use the AWS Certificate Manager (ACM) service to generate, manage, and deploy the private and public certificates they use to establish encrypted transport between systems for their workloads. AWS KMS and ACM support the hybrid post-quantum TLS ciphers. AWS Certificate Manager supports the importing of third party certificates. AWS provides the customer with many security, identity, compliance services for consideration as supplementary technical and organizational measures. References: https://docs.aws.amazon.com/general/latest/gr/rande.html https://aws.amazon.com/blogs/security/tls-1-2-required-for-aws-endpoints/ https://aws.amazon.com/security/post-quantum-cryptography/ Elastic Load Balancing is integrated with ACM and is used to support HTTPS protocols. If Content Data are distributed through Amazon CloudFront, it supports encrypted endpoints. In the contract with the Dutch government, AWS guarantees that it has not purposefully created any "backdoors" or similar programming in the Services that could be used by AWS or by third parties to obtain unauthorised access to the system and/or personal data stored in the system. Customers can encrypt Content Data in block storage and S3. Depending on the risks of unauthorised access to the data, government organisations may want to use AWS Nitro, a collection of security measures that allows hardware based VM encryption and key management for customer virtual machines. See: https://aws.amazon.com/ec2/nitro/ SLM Rijk and AWS have signed the new Controller to Processor SCC.
k)	Relevant onward transfer(s) of personal data (if any):	AWS does **not** engage third party subprocessors to process Content Data from the 3 tested services, only uses infrastructure and services run by its own subsidiairies. The AWS Sub-Processors page lists the AWS services for which third-party service providers may be used, if a customer decides to use these extra services, such as for example messaging services. URL: https://aws.amazon.com/compliance/sub-processors/
l)	Countries of recipients of relevant onward transfer(s):	A small number of AWS services involve the transfer of Content Data, for example, to develop and improve those services. Customers can and are advised to opt-out of these transfers. Transfer may also be an essential part of the service (such as a content delivery service). Customers can identify these services on the 'Privacy Features of AWS Services' web page, at URL: https://aws.amazon.com/compliance/privacy-features/. The possible access to Content Data in third countries, as part of support tickets, is covered in the separate tab 'Support Data'. AWS recommends that customers never put confidential information or directly identifiable personal data such as their email addresses into tags or free-form text fields such as a Name field. This includes when they work with AWS Support or other AWS services using the console, API, AWS CLI, or AWS SDKs.

Step 2: Define the DTIA parameters

			Rationale
a)	Starting date of the transfer:	[Gov org to fill in the date]	
b)	Assessment period in years:	2	
c)	Ending date of the assessment based on the above:	X+2	
d)	Target jurisdiction for which the DTIA is made:	USA	
e)	Is importer an Electronic Communications Service Provider as defined in USC § 1881(b)(4):	Yes	
f)	Does importer/processor commit to legally resist every request for access :	Yes	
g)	Relevant local laws taken into consideration:	FISA Section 702, other FISA warrants such as business records, pen registers and trap and trace devices, National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA),NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants. Additionally, mass surveillance / cable interception based on EOP 12333 (mitigated by PPD-28).	*This DTIA takes the risks of two types of US legislation into account: traditional law enforcement, and court ordered subpoenas and warrants, as well as secret services powers, letters and FISC authorisations. Since AWS offers 'remote computing services' that are part of the definition of 'Electronic Communications Service Provider' as defined in article 50 of the US Code par. 1881(b) under 4, sub c, the US government has the authority to engage in bulk surveillance based on EOP 12333 and to issue direct orders to AWS based on FISA Section 702. Additionally, the US Stored Communications Act and US CLOUD Act apply. This DTIA does *not* assess the risks of requests for personal data ordered by EU law enforcement authorities through MLAT requests. AWS emphasises that EOP 12333 does not include any authorization to compel private companies to disclose data from their customers.*

Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider

		Probability per case	Cases per year	Cases remaining	Rationale
a)	Number of cases under the laws listed in Step 2g per year in which an authority in the USA is estimated to attempt to obtain relevant data through legal action during the period under consideration.		0,50		*The number of 0,5 case per year is an estimate based on AWS's own transparency reporting and assurance that none of the subpoenas, search warrants and court orders resulted in the disclosure to the U.S. government of Enterprise Content Data located outside the United States. Since AWS included the metric in the reports (July 2020), the reports notes:* *"How many requests resulted in the disclosure to the U.S. government of enterprise or government content data located outside the United States?* *None."* *AWS does not provide specific information if EU customer Content Data were disclosed to security services. AWS only mentions a range between 0 and 249. For clarity, under US law, providers can neither confirm nor deny having received any specific legal demands subject to a secrecy obligation. See: https://aws.amazon.com/compliance/amazon-information-requests/* *The estimate is also based on the historical data available in this sector, and on the requirement to calculate based on a number greater than zero.*
b)	Share of such cases in which the request occurs in connection with a case that due to its nature in principle permits the authority to obtain the data also from a provider	100%	0,50		*As documented in the AWS Supplementary Addendum, AWS will challenge any overbroad or inappropriate requests or gagging orders. AWS writes that it has repeatedly challenged government demands for customer information that it believed were overbroad, winning decisions that have helped to set the legal standards for protecting customer speech and privacy interests.See: https://d1.awsstatic.com/legal/aws-dpa/supplementary-addendum-to-the-aws-dpa.pdf.* *Additionally, in Clause 14 of the SCC AWS guarantees it has no reason to believe that it cannot fulfill its obligations under the clauses due to lawful access orders and requests.*

c)	Probability that in the remaining such cases it will be possible for the company to successfully cause the authority (by legal means or otherwise) to give up its request for the data **in plain text**	90%	0,05		*Assuming government organisations will apply the available disk encryption (possibly with the use of an external cloud-based HSM to store the self-generated keys) to protect stored sensitive and special categories of data, it is likely that AWS is not able to disclose Content Data in plain text. However, the chance is not zero, because AWS can theoretically be ordered to access the temporarily decrypted data. If a government organisation asks the KMS to decrypt some material and the keys and decryption process happen inside the KMS, the KMS will have to send the decrypted output somewhere.* *AWS adds: AWS KMS is designed so that no one, including AWS employees, can retrieve customer plaintext KMS keys from the service. AWS KMS uses hardware security modules (HSMs) that have been validated under FIPS 140-2, or are in the process of being validated, to protect the confidentiality and integrity of a customer's keys. Customers plaintext KMS keys never leave the HSMs, are never written to disk, and are only ever used in the volatile memory of the HSMs for the time needed to perform the customer's requested cryptographic operation. Updates to software on the service hosts and to the AWS KMS HSM firmware is controlled by multi-party access control that is audited and reviewed by an independent group within Amazon and a NIST-certified lab in compliance with FIPS 140-2.* *More details about these security controls can be found in the AWS KMS cryptographic details tech paper. Customers can also review the FIPS 140-2 certificate for AWS KMS HSM along with the associated Security Policy to get more details about how AWS KMS HSM meets the security requirements of FIPS 140-2.* *External key stores allow customers to protect their AWS resources using cryptographic keys outside of AWS. An external key store is a custom key store backed by an external key manager that customers own and manage outside of AWS. The customer's external key manager can be a physical or virtual hardware security modules (HSMs), or any hardware-based or software-based system capable of generating and using cryptographic keys. References: https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html and https://docs.aws.amazon.com/kms/latest/cryptographic-details/intro.html*
d)	Probability that in the remaining cases the requested data will be provided in one way or another (e.g., with consent or through legal or administrative assistance)	25%	0,04		*This is a very slim chance, in view of the circumstances described in F 31 through to 33. Consent from an EU Enterprise Customer is unlikely, in the absence of a data protection adequacy decision from the European Commission for the USA. Since AWS is a processor, and not a controller for the personal data in the Content Data, it will take time for the US authorities to force AWS to provide the requested data. Additionally, there will be a delay in obtaining an FISA 702 order. This delay enables AWS to inform the customer that it can no longer comply with SCC guarantees without disclosing that it has received a FISA 702 order.*
e)	Probability that in the remaining cases the authority will consider the data it is seeking to be so important that it will look for another way to obtain it	10%	0,00	0,00	*It is assumed this question tries to assess the probability that AWS is hacked or an invididual employee is blackmailed/bribed to hand over data. This cannot be excluded, but the chances are very slim if the customer applies the recommended encryption measures.*
	Number of cases per year in which the question of lawful access by a foreign authority arises			0,00	
	Number of cases in the period under consideration			0,01	

Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider

Legal Basis considered for the following assessment: Section 702 FISA, other FISA warrants such as business records, pen registers and trap and trace devices, National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA), NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants.

	Prerequisite for success	**Probability per case**			**Rationale**
a)	Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1)	100%		100%	*AWS is a well-known cloud services provider with a substantial amount of Enterprise and Edu Customers in the EU*
b)	Probability that an employee of the provider or its subcontractors will gain access to the data in plain text in a support-case ... (prerequisite no. 2)	100%	0,00%	1%	*Here, it is assumed the customer can intentionally provide access in plain text to an AWS support employee.*
	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	0%			*The US CLOUD Act does not require a provider to unencrypt so if the AWS customer uses encryption methods, the probability of access to the data in plain text is very low.*
c)	Probability that despite the technical countermeasures taken, employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside a support situation (e.g., using admin privileges) or are able to gain such access, e.g., by covertly installing a backdoor or "hacking" into the system (irrespective of whether they are allowed to do so) ... (prerequisite no. 2)	10%	1,00%		*Content Data within VM's can be encrypted by the Customer with the key managed in an HSM. AWS has designed Nitro System to protect the integrity and confidentiality of virtual machines, including RDS, even against access by AWS to the key material and the virtual machine contents. See: https://aws.amazon.com/ec2/nitro/ This security model is locked down and prohibits administrative access, eliminating the possibility of human error and tampering. Nitro provides customers with cryptographic proof of the integrity of the customer instance. This allows customers to verify that AWS has not modified the configuration of the instance, to for example create a back-door. This reduces the risk of disclosure of key material to non-trusted instances. With regard to Amazon S3 depending on the application requirements the customer can implement its own encryption on the data stored in S3, with self-managed keys.*
	... and are then able to search for, find and copy the data requested by the authority (prerequisite no. 3)	10%			
d)	Probability that the provider, the subcontractor or its parent company, respectively, is located within the jurisdiction of the authority (prerequisite no. 4)	50%		50%	*AWS is a US based company and has access to Content Data stored in its EU data centres. However, only the US CLOUD Act applies, and hence the probability is much lower compared to personal data stored in the USA.*
e)	Probability that despite the technically limited access and the technical and organizational countermeasures in place, the authority is permitted to order the provider, its subcontractor or the parent company, respectively, to obtain access to the data and produce it to the authority in plain text (prerequisite no. 5)	1%		1%	*Speculative estimate, as the US Cloud Act does not authorise US authorities to compel AWS to decrypt data, and it can be assumed Dutch government customers will apply the strongest encryption on the Content Data with the highest security risks (i.e. protection against hostile (state) actors).*
a)	Probability that if data were to be handed over to the foreign authority, this would lead to the criminal liability of employees of the provider or its subcontractors, the prosecution of which would be possible and realistic, and as a consequence, the data does not have to be produced or is not produced (prerequisite no. 6)	50%		50%	*As documented in the AWS Supplementary Addendum, AWS will challenge any overbroad or inappropriate requests or gagging orders. See the explanation in F32 above. According to the most recent CS-2020 audit, there were no findings of non-compliance with this policy. Customers can access these audit reports via AWS Artifact, URL: https://aws.amazon.com/artifact/*
g)	Probability that the government organisation does not succeed in removing the relevant data in time or otherwise withdrawing it from the provider's access (prerequisite no. 7)	50%		50%	*AWS can provide a signal based on Article 14 of the SCC, but government organisations may be slow to respond, and to move the Content Data to another cloud service provider. However, it can be assumed Dutch government customers will apply the strongest encryption on the Content Data with the highest security risks (i.e. protection against hostile (state) actors). In that case, the foreign authority would only gain access to encrypted data.*

Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures): **0,00%**

Step 4b: Probability of foreign lawful access by mass surveillance of contents

Legal Basis considered for the following assessment: Section 702 US Foreign Intelligence Surveillance Act (FISA), CIA surveillance based on Executive Order (EO) 12333

		Probability in the period			**Rationale**
a)	Probability that the data at issue is transmitted to the provider or its subcontractors in a manner that permits the telecommunications providers in the country to view it in plain text as part of an upstream monitoring of Internet backbones	0%	0,00%	0,00%	*TLS encryption, customers should use TLS 1.2 or later. AWS KMS and ACM support the hybrid post-quantum TLS ciphers.*
b)	Probability that the data transmitted will include content picked by selectors (i.e., intelligence search terms such as specific recipients or senders of electronic communications)	0%			*TLS encryption, customers should use TLS 1.2 or later. AWS KMS and ACM support the hybrid post-quantum TLS ciphers.*
c)	Probability that the provider or a subcontractor in the country is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the customer's permission as part of a downstream monitoring of online communications	0%	0,00%		*TLS encryption, customers should use TLS 1.2 or later. AWS KMS and ACM support the hybrid post-quantum TLS ciphers.*
d)	Probability that the provider or a subcontractor in the country above may be legally required to perform such as search (also) with the company's data	1%			*This refers to Upstream Data Collection. It is plausible that some Content Data from an EU gov organisation are interesting for law enforcement and/or security services, however, the probability is extremely low. Amazon has publicly stated it never participated in the NSA's PRISM program. URL: https://aws.amazon.com/blogs/security/privacy-and-data-security/*
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	10%			*It is plausible that some Content Data from an EU gov or university organisation are interesting for intelligence services. However, in view of the transport encryption, the probability of decryption, to obtain access in plain tekst is very low. Over time this probability may of course increase, with quantum computing.*

Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the **0,00%**

Step 5: Overall assessment

Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%) **0,75%**

Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures	0,00%
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite	0,00%
Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period:	0,00%
Description in words (based on Hillson*):	Very low
The number of years it takes for a lawful access to occur at least once with a **90 percent** probability:	∞
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability:	∞

... assuming that the probability neither increases nor decreases over time (like tossing a coin)

** Scale: <5% = "Very low", 5-10% = "Low", 11-25 = "Medium", 26-50% = "High" and >50% = "Very high" (by David Hillson, 2005, see https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*

Step 6: Data subject risks

				Rationale
a)	*Estimated probability of occurance of successful lawful access risk:*	*0,00%*	*Very Low*	*The Content Data can include special categories of data. Organisations are advised to apply their own encryption to such sensitive and special categories of data unless the data are already public (such as court hearings).* ***The risk is low in 3 circumstances: (1) if the European Commission adopts a new adequacy decision for the USA (2) if organisations do not store such special categories of data in AWS's services, or if they do, absent an adequacy decision (3) they can control the key (and they use pseudonyms for employee admins whose identity should remain confidential)***
b)	*Estimated impact of risk*	*3= regular personal data in the clear*	*High*	

Very High	Low	High	High	High	High
High	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	High
	0	1	2	3	4

Low

Step 7: Define the safeguards in place

				Rationale
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	*Describe why you still do not pursue this option*	*Yes, EU government customers can choose an EU availability zone for the Content Data at rest.*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		*No*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	*Ensure that data remains encrypted*	*Strong recommendation to admins to apply encryption with their own key to sensitive and special categories of data stored/processed in Amazon EC2, Amazon S3, and Amazon RDS. Data in transit are encrypted by AWS (SSL/TLS).*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*If the government organisation does not apply encryption with a self-controlled key, but applies AWS's disk encryption, theoretically it is possible that AWS is ordered to copy the decrypted data while they are being used. AWS Nitro System is designed to prevent access to even AWS from accessing the content on VMs, even while in use. With regard to Amazon S3 the customer can implement its own encryption on the data stored in S3, with self-managed keys. Not all applications allow for that type of encryption, if the data have to be shared with parties that cannot be trusted with the encryption keys.*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	*Ensure that the mechanism remains in place and is complied with*	*SLM Rijk and AWS have signed the new SCC Controller to Processor.*
	Based on the answers given above, the transfer is:	**permitted**		*Absent a new adequacy decision from the EU for the USA, admins should apply encryption to Content Data with a self-controlled key if they want to use AWS to store sensitive and special categories of data.*

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: **permitted**

Reassess at the latest by: X+2
(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
SLM Rijk / PRIVACY COMPANY

Place, Date:
Signed:
By: [Government org X]

Data Transfer Impact Assessment (DTIA) on the transfer to the USA of Diagnostic Data resulting from the use of Amazon EC2, Amazon S3, and Amazon RDS

Step 1: Describe the intended transfer

a)	Data exporter (or the sender in case of a relevant onward transfer):	Dutch government organisation [X]
b)	Country of data exporter:	Netherlands
c)	Data importer (or the recipient in case of a relevant onward transfer):	Amazon Web Services, Inc. ("AWS, Inc.", abbreviated in this DTIA to: "AWS") USA. Seller of Record is Amazon Web Services EMEA SARL ("AWS Europe"), a Luxembourg-based AWS entity. Both AWS and AWS Europe are wholly owned subsidiaries of Amazon.com, Inc. AWS works with Regions, a physical location in a country where data centers are clustered. AWS has Regions in the EU. Each AWS Region consists of a minimum of three, isolated, and physically separate AZs within a geographic area. AWS calls each group of logical data centers an Availability Zone. **Diagnostic Data** are generated in the AWS Region where the service is used, and depending on the scope of the customer's interactions with AWS Offerings, may be stored in or accessed from multiple countries, including the United States. References:
d)	Country of data importer:	https://aws.amazon.com/about-aws/global-infrastructure/regions_az/
e)	Context and purpose of the transfer:	Diagnostic Data about the individual actions of employees of the MOJ or any other Governmental entity that use Amazon EC2, Amazon S3, and Amazon RDS to store and process Content Data
f)	Categories of data subjects concerned:	Employees of the Dutch government.
g)	Categories of personal data transferred:	Diagnostic Data generated through the use by admins of Amazon EC2, Amazon S3, and Amazon RDS in service generated server logs and in security logs. The security logs are described in the separate tab 'Security Data, T&S' because of the role of AWS as data controller, in stead of processor. Diagnostic Data may reveal a work pattern of admins. However, based on the outcomes of the recent C5:20202 audit, in particular the results of the audit on the OPS-11 basic criterion, AWS was found to only collect and use the Diagnostic Data for the 3 purposes of *billing, incident management and security incident management purposes* . The audit report also states: "*Exclusively anonymous metadata to deploy and enhance the cloud service so that no conclusions can be drawn about the cloud customer or user.* "
h)	Sensitive and special categories of personal data:	Diagnostic Data may include Account Data from employee administrators whose identity should remain confidential. This DTIA assumes government organisations will pseudonymise admin account data by using identity federation. See row 13 below.
i)	Technical implementation of the transfer:	Diagnostic Data are generated at the location where the service is used, and may be transferred to the USA for further processing by AWS as controller for the agreed legitimate business purposes. Depending on the scope of the customer's interactions with AWS offerings, Diagnostic Data may be stored in or accessed from multiple countries, including the United States.
j)	Technical and organizational measures in place:	AWS has elaborate Security Standards, and has its compliance with these standards tested in different types of audits. The reports are available for customers. Admins can and should pseudonymise their Account Data (collected in the Diagnostic Data). AWS offers solutions to federate customer's employees, contractors, and partners (workforce) to AWS accounts and business applications, and offers federation support to customer's end-user-facing web and mobile applications. AWS supports commonly used open identity standards, including Security Assertion Markup Language 2.0 (SAML 2.0), Open ID Connect (OIDC), and OAuth 2.0. URL: https://aws.amazon.com/identity/federation/. As additional mitigating measures AWS strongly recommends that customers never put confidential information or directly identifiable personal data, such as their email addresses, into tags or free-form text fields such as a Name field. Additionally, AWS commits to use every reasonable effort to redirect valid and binding orders for Diagnostic Data to its Customer. If compelled to disclose Personal Data to a Requesting Party, AWS will (i) promptly notify Customer of the Request to allow Customer to seek a protective order or other appropriate remedy, if AWS is legally permitted to do so. If AWS is prohibited from notifying Customer about the Request, AWS will use all reasonable and lawful efforts to obtain a waiver of prohibition, to allow AWS to communicate as much information to Customer as soon as possible; and (ii) challenge any overbroad or inappropriate Request (including where such Request conflicts with the law of the European Union or applicable Member State law).
k)	Relevant onward transfer(s) of personal data (if any):	AWS does **not** engage third party subprocessors to process Content Data from the 3 tested services, only uses infrastructure and services run by its own subsidiairies. The AWS Sub-Processors page lists the AWS services for which third-party service providers may be used, if a customer decides to use these extra services, such as for example messaging services. URL: https://aws.amazon.com/compliance/sub-processors/ AWS applies encryption to all data in transit. SLM Rijk and AWS have signed the new Controller to Processor SCC. In the contract with the Dutch government, AWS guarantees that it has not purposefully created any "backdoors" or similar programming in the Services that could be used by AWS or by third parties to obtain unauthorised access to the systems and/or Diagnostic Data stored in the system.
l)	Countries of recipients of relevant onward transfer(s):	n/a

Step 2: Define the DTIA parameters

			Rationale
a)	Starting date of the transfer:	[Gov org to fill in the date]	
b)	Assessment period in years:	2	
c)	Ending date of the assessment based on the above:	X+2	
d)	Target jurisdiction for which the DTIA is made:	USA	
e)	Is importer an Electronic Communications Service Provider as defined in USC § 1881(b)(4):	Yes	
f)	Does importer/processor commit to legally resist every request for access :	Yes	
g)	Relevant local laws taken into consideration:	FISA Section 702, other FISA warrants such as business records, pen registers and trap and trace devices, National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA),NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants. Additionally, mass surveillance / cable interception based on EOP 12333 (mitigated by PPD-28),	*This DTIA takes the risks of two types of US legislation into account: traditional law enforcement, and court ordered subpoenas and warrants, as well as secret services powers, letters and FISC authorisations. Since AWS offers 'remote computing services' that are part of the definition of 'Electronic Communications Service Provider' as defined in article 50 of the US Code par. 1881(b) under 4, sub c, the US government has the authority to engage in bulk surveillance based on EOP 12333 and to issue direct orders to AWS based on FISA Section 702. Additionally, the US Stored Communications Act and US CLOUD Act apply. This DTIA does *not* assess the risks of requests for personal data ordered by EU law enforcement authorities through MLAT requests. AWS emphasises that EOP 12333 does not include any authorization to compel private companies to disclose data from their customers.*

Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider

		Probability per case	Cases per year	Cases remaining	Rationale
a)	Number of cases under the laws listed in Step 2g per year in which an authority is estimated to attempt to obtain relevant data through legal action during the period under consideration.		0,50		*The number of 0,5 case per year is an estimate based on AWS's own transparency reporting and assurance that none of the subpoenas, search warrants and court orders resulted in the disclosure to the U.S. government of Enterprise Content Data located outside the United States. Since AWS included the metric in the reports (July 2020), the reports notes:* *"How many requests resulted in the disclosure to the U.S. government of enterprise or government content data located outside the United States?* *None."* *AWS does not provide specific information if it has ever disclosed Diagnostic Data to law enforcement or security services. See: https://aws.amazon.com/compliance/amazon-information-requests/* *The low estimate is also based on AWS's commitments in the AWS Supplementary Addendum, the historical data available in this sector, and on the requirement to calculate based on a number greater than zero.*
b)	Share of such cases in which the request occurs in connection with a case that due to its nature in principle permits the authority to obtain the data also from a provider	100%	0,50		*As documented in the AWS Supplementary Addendum, AWS will challenge any overbroad or inappropriate requests or gagging orders. AWS writes that it has repeatedly challenged government demands for customer information that it believed were overbroad, winning decisions that have helped to set the legal standards for protecting customer speech and privacy interests.See: https://d1.awsstatic.com/legal/aws-dpa/supplementary-addendum-to-the-aws-dpa.pdf.* *Additionally, in Clause 14 of the SCC AWS guarantees it has no reason to believe that it cannot fulfill its obligations under the clauses due to lawful access orders and requests.*
c)	Probability that in the remaining such cases it will be possible for the company to successfully cause the authority (by legal means or otherwise) to give up its request for the data **in plain text**	10%	0,45		*The Diagnostic Data are available for AWS employees in the clear, customers cannot encrypt these data with self-controlled keys. Hence the probability is low that AWS can successfully resist an order to produce Diagnostic Data in plain text, in spite of its commitments.*
d)	Probability that in the remaining cases the requested data will be provided in one way or another (e.g., with consent or through legal or administrative assistance)	25%	0,34		*There is a chance that AWS is compelled to disclose Diagnostic Data, in spite of its commitments. Consent from an EU Enterprise Customer is unlikely, in the absence of a data protection adequacy decision from the European Commission for the USA. Since AWS is a processor, and not a controller for the personal data in the Content Data, it will take time for the US authorities to force AWS to provide the requested data. Additionally, there will be a delay in obtaining an FISA 702 order. This delay enables AWS to inform the customer that it can no longer comply with SCC guarantees without disclosing that it has received a FISA 702 order.*
e)	Probability that in the remaining cases the authority will consider the data it is seeking to be so important that it will look for another way to obtain it	10%	0,03	0,03	*It is assumed this question tries to assess the probability that AWS is hacked or an invididual employee is blackmailed/bribed to hand over Diagnostic Data. This cannot be excluded.*

Number of cases per year in which the question of lawful access by a foreign authority arises	0,03
Number of cases in the period under consideration	0,07

Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider

Legal Basis considered for the following assessment: Section 702 FISA, other FISA warrants such as business records, pen registers and trap and trace devices, National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA), NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants.

Prerequisite for success		Probability per case			Rationale
a)	Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1)	100%		100%	*AWS is a well-known cloud services provider with a substantial amount of Enterprise and Edu Customers in the EU*
b)	Probability that an employee of the provider or its subcontractors will gain access to the data in plain text in a support-case ... (prerequisite no. 2)	100%	100,00%	100%	*Authorised AWS employees can have access to Diagnostic Data when necessary for their tasks*
	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	100%			*Idem*
c)	Probability that despite the technical countermeasures taken, employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside a support situation (e.g., using admin privileges) or are able to gain such access, e.g., by covertly installing a backdoor or "hacking" into the system (irrespective of whether they are allowed to do so) ... (prerequisite no. 2)	100%	100,00%		*Authorised AWS employees can have access to Diagnostic Data when necessary for their tasks. AWS restricts its personnel from processing Personal Data without authorisation by AWS as described in the AWS Security Standards. AWS imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security. AWS guarantees that it has not purposefully created any "backdoors" or similar programming in the Services that could be used by AWS or by third parties to obtain unauthorised access to the system and/or Personal Data stored in the system. There are no findings of non-compliance with the access rules in the C5:20202 audit.*
	... and are then able to search for, find and copy the data requested by the authority (prerequisite no. 3)	100%			*Idem*
d)	Probability that the provider, the subcontractor or its parent company, respectively, is located within the jurisdiction of the authority (prerequisite no. 4)	100%		100%	*AWS is a US based company and has access to the Diagnostic Data stored either in the EU availability zone, or transferred to the USA.*
e)	Probability that despite the technically limited access and the technical and organizational countermeasures in place, the authority is permitted to order the provider, its subcontractor or the parent company, respectively, to obtain access to the data and produce it to the authority in plain text (prerequisite no. 5)	100%		100%	*Though the probability is estimated at the maximum of 100%, AWS has robust controls in place and has these controls audited. There are no findings in the recent C5:2020 audit about disclosure to authorities.*
f)	Probability that if data were to be handed over to the foreign authority, this would lead to the criminal liability of employees of the provider or its subcontractors, the prosecution of which would be possible and realistic, and as a consequence, the data does not have to be produced or is not produced (prerequisite no. 6)	80%		20%	*As documented in the AWS Supplementary Addendum, AWS will challenge any overbroad or inappropriate requests or gagging orders. See the explanation in F32 above. According to the most recent C5-2020 audit, there were no findings of non-compliance with this policy. Customers can access these audit reports via AWS Artifact, URL: https://aws.amazon.com/artifact/*
g)	Probability that the company does not succeed in removing the relevant data in time or otherwise withdrawing it from the provider's access (prerequisite no. 7)	100%		100%	*If AWS or its subprocessors receive a valid order/warrant or subpoena, AWS may be subjected to gagging order and not permitted to inform its Customer. Hence AWS may not be in a position to issue a timely warning to its customer that it can no longer comply with the data protection guarantees in the SCC.*

Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures): 20,00%

Step 4b: Probability of foreign lawful access by mass surveillance contents

Legal Basis considered for the following assessment: Section 702 US Foreign Intelligence Surveillance Act (FISA), CIA surveillance based on Executive Order (EO) 12333

		Probability in the period			Rationale
a)	Probability that the data at issue is transmitted to the provider or its subcontractors in a manner that permits the telecommunications providers in the country to view it in plain text as part of an upstream monitoring of Internet backbones	0%	0,00%	0,00%	*AWS applies encryption to all data in transit.*
b)	Probability that the data transmitted will include content picked by selectors (i.e., intelligence search terms such as specific recipients or senders of electronic communications)	0%			*AWS applies encryption to all data in transit.*
c)	Probability that the provider or a subcontractor in the country is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the customer's permission as part of a downstream monitoring of online communications	0%	0,00%		*AWS applies encryption to all data in transit.*
d)	Probability that the provider or a subcontractor in the country above may be legally required to perform such as search (also) with the company's data	50%			*This refers to Upstream Data Collection. It is plausible that some Diagnostic Data from an EU government organisation are interesting for law enforcement and/or security services. Even if processed on EU servers, the data can be decrypted and accessed by AWS in the USA if ordered to do so. However, it is unlikely that Diagnostic Data would be of interest, especially if the government organisations follow the recommendation to use identity federation (see above in I13).*
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	50%			*Idem*

Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures): 0,00%

Step 5: Overall assessment

Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%) 6,75%

Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures 20,00%

Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures) 0,00%

Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period: 1,35%

Description in words (based on Hillson*): Very low

The number of years it takes for a lawful access to occur at least once with a **90 percent** probability: ∞
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability: ∞
... assuming that the probability neither increases nor decreases over time (like tossing a coin)

** Scale: <5% = "Very low", 5-10% = "Low", 11-25 = "Medium", 26-50% = "High" and >50% = "Very high" (by David Hillson, 2005, see https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*

Step 6: Data subject risks

				Rationale
a)	*Estimated probability of occurance of successful lawful access risk:*	*1,35%*	*Very Low*	
b)	*Estimated impact of risk*	*1= pseudonymised diagnostic data*	*Low*	*If government organisations follow the recommendation that admins should use identity federation to pseudonymise Account Data (collected in the service generated server logs), the Diagnostic Data will not contain any directly identifying data, only pseudonymous data such as IP addresses*

Very High	Low	High	High	High	High
High	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	High
	0	1	2	3	4

Step 7: Define the safeguards in place

				Rationale
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	*Describe why you still do not pursue this option*	*Diagnostic Data are generated at the location where the service is used, and may be transferred to the USA for further processing by AWS as controller for the agreed legitimate business purposes. Depending on the scope of the customer's interactions with AWS offerings, Diagnostic Data may be stored in or accessed from multiple countries, including the United States.*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		*No.*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	*Ensure that data remains encrypted*	*Data in transit are encrypted by AWS (SSL/TLS). Admins can and should pseudonymise their Account Data with identity federation.*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*Yes. The logs can be accessed in the clear by authorised AWS employees when they are permitted access*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	*Ensure that the mechanism remains in place and is complied with*	*SLM Rijk and AWS have signed the new SCC Controller to Processor.*
Based on the answers given above, the transfer is:		**permitted**		*Organisations should apply identity federation to he Account Data for employees whose identity should remain confidential*

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: **permitted**

Reassess at the latest by: X+2
(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
SLM Rijk / PRIVACY COMPANY

Place, Date:

Signed: _____

By: [Government org X]

Data Transfer Impact Assessment (DTIA) on the transfer of Support Data to the USA relating to Amazon EC2, Amazon S3, and Amazon RDS

Step 1: Describe the intended transfer

a)	Data exporter (or the sender in case of a relevant onward transfer):	Dutch government organisation [X]
b)	Country of data exporter:	Netherlands
c)	Data importer (or the recipient in case of a relevant onward transfer):	Amazon Web Services, Inc. ("AWS, Inc.", abbreviated in this DTIA to: "AWS")
d)	Country of data importer:	USA. Seller of Record is Amazon Web Services EMEA SARL ("AWS Europe"), a Luxembourg-based AWS entity. Both AWS and AWS Europe are wholly owned subsidiaries of Amazon.com, Inc. AWS works with Regions, a physical location in a country where data centers are clustered. AWS has Regions in the EU. Each AWS Region consists of a minimum of three, isolated, and physically separate AZs within a geographic area. AWS calls each group of logical data centers an Availability Zone. Support tickets may include both Content Data and Diagnostic Data about the individual actions of employees of the MOJ or any other Governmental entity that use Amazon EC2, Amazon S3, and Amazon RDS to store and process Content Data. AWS adds: When customers create a support case, they own the information that they include in their support case. AWS doesn't access customer AWS account data without their permission. AWS doesn't share customer information with third parties. As a general risk mitigating measure, AWS strongly recommends that customers never put confidential information or directly identifiable personal data such as their email addresses….such as their email addresses into tags or free-form text fields such as a Name field. This includes when customers work with AWS Support or other AWS services using the console, API, AWS CLI, or AWS SDKs. If customers provide a URL to an external server, AWS strongly recommends to not include credentials information in the URL to validate the request to that server. References: https://docs.aws.amazon.com/awssupport/latest/user/data-protection.html
e)	Context and purpose of the transfer:	
f)	Categories of data subjects concerned:	Employees of the Dutch government , possibly external data subjects whose data are processed by MOJ or any other governmental organisation as Content Data, visitors of websites hosted on AWS (their IP addresses may be logged in AWS's security and infrastructure logs)
g)	Categories of personal data transferred:	Account Data, Diagnostic Data and possibly snippets of Content Data. See the separate tabs in this DTIA for Account, Diagnostic and Content Data
h)	Sensitive and special categories of personal data:	Support Data may include sensitive Account Data, if an employee admin works for a government organisation with a high level of sensitivity. However, government organisations are strongly advised to create pseudonymous admin accounts. Support Data can include Diagnostic Data, again with pseudonymous data if pseudonyms are used for the admin accounts
i)	Technical implementation of the transfer:	When customers create a support case, AWS doesn't gain access to the customers account. If necessary, support agents use a screen-sharing tool to view a customer's screen remotely and identify and troubleshoot problems. This tool is view-only. Support agents cannot export any data from the customer, and cannot act for customers during the screen-share session. Customers must give consent to share a screen with a support agent. EU customers can ask their AWS account manager to flag all of their support requests with an internal contextual alert. Such an alert is specific to a customer. AWS Support Engineering and Customer Service will see these alerts displayed when accessing a customer case. Such an alert could warn employees that the customer only wants problems solved by EU-based employees, or for example only employees in a country with an adequate data protection regime, such as Japan. If government organisations use that option, Support Data will no longer be (structurally) transferred out of the EU/to third countries. Additionally, in the contract with the Dutch government, AWS guarantees that it has not purposefully created any "backdoors" or similar programming in the Services that could be used by AWS or by third parties to obtain unauthorised access to the system and/or Personal Data stored in the system. References: https://docs.aws.amazon.com/awssupport/latest/user/security-for-support-cases.html https://docs.aws.amazon.com/awssupport/latest/user/security-iam.html
j)	Technical and organizational measures in place:	
k)	Relevant onward transfer(s) of personal data (if any):	AWS does engage subprocessors for Support, but customers can indicate they only want their tickets accessed by EU-based support employees, or support employees in countries with an adequate data protection regime, such as Japan. Hence, customers can and should prevent transfer of Support Data to third countries.
l)	Countries of recipients of relevant onward transfer(s):	N/a if the contextual alert solution is used.

Step 2: Define the DTIA parameters

			Rationale
a)	Starting date of the transfer:	[Gov org to fill in the date]	
b)	Assessment period in years:	2	
c)	Ending date of the assessment based on the above:	X+2	
d)	Target jurisdiction for which the DTIA is made:	USA	
e)	Is importer an Electronic Communications Service Provider as defined in USC § 1881(b)(4):	Yes	
f)	Does importer/processor commit to legally resist every request for access :	Yes	
g)	Relevant local laws taken into consideration:	FISA Section 702, other FISA warrants such as business records, pen registers and trap and trace devices, National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA),NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants. Additionally, mass surveillance / cable interception based on EOP 12333 (mitigated by PPD-28),	*This DTIA takes the risks of two types of US legislation into account: traditional law enforcement, and court ordered subpoenas and warrants, as well as secret services powers, letters and FISC authorisations. Since AWS offers 'remote computing services' that are part of the definition of 'Electronic Communications Service Provider' as defined in article 50 of the US Code par. 1881(b) under 4, sub c, the US government has the authority to engage in bulk surveillance based on EOP 12333 and to issue direct orders to AWS based on FISA Section 702. Additionally, the US Stored Communications Act and US CLOUD Act apply. This DTIA does *not* assess the risks of requests for personal data ordered by EU law enforcement authorities through MLAT requests. AWS emphasises that EOP 12333 does not include any authorization to compel private companies to disclose data from their customers.*

Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider

		Probability per case	Cases per year	Cases remaining	Rationale
a)	Number of cases under the laws listed in Step 2g per year in which an authority in the USA is estimated to attempt to obtain relevant data through legal action during the period under consideration.		0,50		*The number of 0,5 case per year is an estimate based on AWS's own transparency reporting and assurance that none of the subpoenas, search warrants and court orders resulted in the disclosure to the U.S. government of Enterprise Content Data located outside the United States. Since AWS included the metric in the reports (July 2020), the reports notes:* *"How many requests resulted in the disclosure to the U.S. government of enterprise or government content data located outside the United States?* *None."* *AWS does not provide specific information if it has ever disclosed Support Data to law enforcement or security services. See: https://aws.amazon.com/compliance/amazon-information-requests/* *The low estimate is also based on AWS's commitments in the AWS Supplementary Addendum, the historical data available in this sector, and on the requirement to calculate based on a number greater than zero.*
b)	Share of such cases in which the request occurs in connection with a case that due to its nature in principle permits the authority to obtain the data also from a provider	100%	0,50		*As documented in the AWS Supplementary Addendum, AWS will challenge any overbroad or inappropriate requests or gagging orders. AWS writes that it has repeatedly challenged government demands for customer information that it believed were overbroad, winning decisions that have helped to set the legal standards for protecting customer speech and privacy interests.See: https://d1.awsstatic.com/legal/aws-dpa/supplementary-addendum-to-the-aws-dpa.pdf.* *Additionally, in Clause 14 of the SCC AWS guarantees it has no reason to believe that it cannot fulfill its obligations under the clauses due to lawful access orders and requests.*
c)	Probability that in the remaining such cases it will be possible for the company to successfully cause the authority (by legal means or otherwise) to give up its request for the data **in plain text**	50%	0,25		*The Support Data can only be viewed by AWS employees, not exported. They are available in the clear, hence the probability is low that AWS can successfully resist an order. If EU government organisations use the internal alert-option to only allow access to EU based employees, the available powers are limited to US CLOUD Act orders. Hence the probability of successful refusal is much higher than for Diagnostic Data. This risk is of course very relative: as explained in row 35 below, the probability that a government authority is interested in obtaining access to support cases is extremely slim.*

d)	Probability that in the remaining cases the requested data will be provided in one way or another (e.g., with consent or through legal or administrative assistance)	25%	0,19		*There is a chance that AWS is compelled to disclose Support Data, in spite of its commitments. Consent from an EU Enterprise Customer is unlikely, in the absence of a data protection adequacy decision from the European Commission for the USA. Since AWS is a processor, and not a controller for the personal data in the Support Data, it will take time for the US authorities to force AWS to provide the requested data. Additionally, there will be a delay in obtaining an FISA 702 order. This delay enables AWS to inform the customer that it can no longer comply with SCC guarantees without disclosing that it has received a FISA 702 order.*
e)	Probability that in the remaining cases the authority will consider the data it is seeking to be so important that it will look for another way to obtain it	1%	0,00	0,00	*It is assumed this question tries to assess the probability that AWS is hacked or an invididual employee is blackmailed/bribed to hand over Support Data. This cannot be excluded. However the probability that a government is interested in obtaining access to support information, is extremely low.*

Number of cases per year in which the question of lawful access by a foreign authority arises 0,00
Number of cases in the period under consideration 0,00

Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider

Legal Basis considered for the following assessment: Section 702 FISA, other FISA warrants such as business records, pen registers and trap and trace devices, National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA), NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants.

	Prerequisite for success	**Probability per case**			**Rationale**
a)	Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1)	100%		100%	*AWS is a well-known cloud services provider with a substantial amount of Enterprise and Edu Customers in the EU*
b)	Probability that an employee of the provider or its subcontractors will gain access to the data in plain text in a support-case ... (prerequisite no. 2)	100%	100,00%		*Authorised AWS Support employees can view, but not export, Support Data when necessary for their tasks*
	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	100%			*Idem*
c)	Probability that despite the technical countermeasures taken, employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside a support situation (e.g., using admin privileges) or are able to gain such access, e.g., by covertly installing a backdoor or "hacking" into the system (irrespective of whether they are allowed to do so) ... (prerequisite no. 2)	100%	100,00%	100%	*By its nature, Support Data are not encrypted, but they can only be viewed by employees, not exported*
	... and are then able to search for, find and copy the data requested by the authority (prerequisite no. 3)	100%			*Idem*
d)	Probability that the provider, the subcontractor or its parent company, respectively, is located within the jurisdiction of the authority (prerequisite no. 4)	50%		50%	*AWS is a US based company and has access to the Support Data, even if the government organisation uses the option to ask for an internal alert to have support tickets exclusively accessed by EU based employees. However, in that case only the US CLOUD Act applies, lowering the probability compared to Diagnostic Data. Additionally, it follows from AWS's CS:2020 audit that there were no findings with regard to unauthorised access to personal data from customers.*
e)	Probability that despite the technically limited access and the technical and organizational countermeasures in place, the authority is permitted to order the provider, its subcontractor or the parent company, respectively, to obtain access to the data and produce it to the authority in plain text (prerequisite no. 5)	50%		50%	*The probability is estimated high at 50%, even though support employees can only view support tickets, and not act on customers. Additionally, AWS has robust controls in place and has these controls audited. There are no findings in the recent CS:2020 audit about disclosure to authorities*
f)	Probability that if data were to be handed over to the foreign authority, this would lead to the criminal liability of employees of the provider or its subcontractors, the prosecution of which would be possible and realistic, and as a consequence, the data does not have to be produced or is not produced (prerequisite no. 6)	80%		20%	*As documented in the AWS Supplementary Addendum, AWS will challenge any overbroad or inappropriate requests or gagging orders. See the explanation in F32 above. According to the most recent CS-2020 audit, there were no findings of non-compliance with this policy. Customers can access these audit reports via AWS Artifact, URL: https://aws.amazon.com/artifact/*
g)	Probability that the company does not succeed in removing the relevant data in time or otherwise withdrawing it from the provider's access (prerequisite no. 7)	80%		80%	*If AWS or its subprocessors receive a valid order/warrant or subpoena, AWS may be subjected to gagging order and not permitted to inform its Customer. Hence AWS may not be in a position to issue a timely warning to its customer that it can no longer comply with the data protection guarantees in the SCC.*

Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures): 4,00%

Step 4b: Probability of foreign lawful access by mass surveillance contents

Legal Basis considered for the following assessment: Section 702 US Foreign Intelligence Surveillance Act (FISA), CIA surveillance based on Executive Order (EO) 12333

		Probability in the period			**Rationale**
a)	Probability that the data at issue is transmitted to the provider or its subcontractors in a manner that permits the telecommunications providers in the country to view it in plain text as part of an upstream monitoring of Internet backbones	0%	0,00%		*AWS applies encryption to all data in transit.*
b)	Probability that the data transmitted will include content picked by selectors (i.e., intelligence search terms such as specific recipients or senders of electronic communications)	0%			*AWS applies encryption to all data in transit.*
c)	Probability that the provider or a subcontractor in the country is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the customer's permission as part of a downstream monitoring of online communications	0%		0,00%	*AWS applies encryption to all data in transit.*
d)	Probability that the provider or a subcontractor in the country above may be legally required to perform such as search (also) with the company's data	50%	0,00%		*This refers to Upstream Data Collection. It is not likely that Support Data from an EU government organisation are interesting for law enforcement and/or security services. Even if processed on EU servers, the data can be decrypted and accessed by AWS in the USA if ordered to do so. However, it is unlikely that Support Data would be of interest, especially if the government organisations follow the recommendation to use identity federation (see above in 113).*
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	5%			*Idem*

Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures): 0,00%

Step 5: Overall assessment

Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)	0,38%
Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures	4,00%
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures)	0,00%
Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period:	0,02%
Description in words (based on Hillson*):	Very low
The number of years it takes for a lawful access to occur at least once with a **90 percent** probability:	∞
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability:	∞

... assuming that the probability neither increases nor decreases over time (like tossing a coin)

** Scale: <5% = "Very low", 5-10% = "Low", 11-25 = "Medium", 26-50% = "High" and >50% = "Very high" (by David Hillson, 2005, see https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*

Step 6: Data subject risks

				Rationale
a)	*Estimated probability of occurance of successful lawful access risk:*	*0,02%*	*Very Low*	
b)	*Estimated impact of risk*	*3= regular personal data in the clear*	*High*	*Support Tickets may include personal data (Content, Account and Diangostic Data), and these data currently can be viewed in the clear by AWS employees in the USA when necessary to solve the ticket. This DTIA assumes admins will follow 3 recommendations: (1) ask AWS to apply an internal alert to only give access to EU based support employees, (2) use pseudonymous admin accounts and (3) follow the instruction from SLM Rijk NOT to include any non-pseudonymised personal data in support tickets*

Very High	Low	High	High	High	High
High	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	High
	0	1	2	3	4

Low

Step 7: Define the safeguards in place

				Rationale
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	*Describe why you still do not pursue this option*	*EU customers can ask their AWS account manager to flag all of their support requests with an internal contextual alert to only have problems solved by EU-based employees, unless escalation is specifically asked by the customer. If government organisations use that option, Support Data will no longer be transferred out of the EU.*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	Yes	*Make sure that the prerequisites are fulfilled!*	*No*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	*Ensure that data remains encrypted*	*Data in transit are encrypted by AWS (SSL/TLS).*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*Yes. The Support Data can be viewed in the clear by AWS employees when they are permitted access*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	*Ensure that the mechanism remains in place and is complied with*	*SLM Rijk and AWS have signed the new SCC Controller to Processor.*

Based on the answers given above, the transfer is: **permitted**

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: **permitted**

Reassess at the latest by: X+2
(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
SLM Rijk / PRIVACY COMPANY

Place, Date:

Signed: _____

By: [Government org X]

Data Transfer Impact Assessment (DTIA) on the transfer of Security Data and Trust & Safety Data to AWS in the USA

Step 1: Describe the intended transfer

a)	Data exporter (or the sender in case of a relevant onward transfer):	Dutch government organisation [X]
b)	Country of data exporter:	Netherlands
c)	Data importer (or the recipient in case of a relevant onward transfer):	Amazon Web Services, Inc. ("AWS, Inc.", abbreviated in this DTIA to: "AWS")
d)	Country of data importer:	USA. Seller of Record is Amazon Web Services EMEA SARL ("AWS Europe"), a Luxembourg-based AWS entity. Both AWS and AWS Europe are wholly owned subsidiaries of Amazon.com, Inc. AWS works with Regions, a physical location in a country where data centers are clustered. AWS has Regions in the EU. Each AWS Region consists of a minimum of three, isolated, and physically separate AZs within a geographic area. AWS calls each group of logical data centers an Availability Zone.
e)	Context and purpose of the transfer:	AWS generates Security Data through the use by admins of Amazon EC2, Amazon S3, and Amazon RDS. The security logs are described separately because of the role of AWS as data controller, in stead of processor. The security logs may contain pseudonymous data like IP addresses from visitors if a website is hosted on a VM. However, based on the outcomes of the recent C5:20202 audit, in particular the results of the audit on the OPS-11 basic criterion, AWS was found to only collect and use the Diagnostic Data (including the Security Data) for the 3 purposes of billing, incident management and security incident management purposes, not for any type of profiling. AWS may also receive complaints or alerts about its customers activities. These data are sent to the Trust & Safety Team in the US. AWS guarantees in the privacy amendment with the Dutch government that it does not undertake automated scanning of Customer Content for purposes of identifying potentially abusive content or activity except under very limited circumstances (e.g., Amazon Simple Email Service scans a percentage of outgoing emails for SPAM and other types of email abuse in line with industry standards). The relevant AWS team ("AWS Trust & Safety") will investigate and take appropriate action when it receives an abuse report relating to Customer Content. The complaints may include both Content Data and Diagnostic Data about the individual actions of employees of the MOJ or any other Governmental entity that use Amazon EC2, Amazon S3, and Amazon RDS to store and process Content Data.
f)	Categories of data subjects concerned:	Employees of the Dutch government, possibly external data subjects that visit websites hosted on AWS
g)	Categories of personal data transferred:	If a website is dedicated to special categories of data, such as health data, the website visitor data captured incidentally by AWS are also sensitive data. If a complaint relates to illegal material, depending on the type of illegality, this could also imply sensitive personal data relating to criminal offences about the admin.
h)	Sensitive and special categories of personal data:	AWS does not engage in proactive detection (scanning) of illegal content processed in Amazon EC2, Amazon S3, and Amazon RDS. The T&S team replies to complaints. The category of Security Data can be used to flag an admin or contents processed by the 3 services as potentially abusive, or as a victim of malicious network activity. These data can potentially become special categories of data.
i)	Technical implementation of the transfer:	Security events and reports about illegal content are collected by AWS's central Network Operations Centre and Trust and Safety team in the USA.
j)	Technical and organizational measures in place:	Government organisations can consider supplementary customer controlled technical and organizational measures to address any residual perceived risk on pseudonymous data like the IP addresses of external data-subjects. For example, by using a webproxy to catch visitor IP addresses. As a processor, AWS may process personal data, when necessary and proportionate, to secure its services. AWS is explicitly authorised in the privacy amendment with the Dutch central government to 'further' process some personal data as independent data controller for the purpose of abuse detection, prevention and protection to protect the security of AWS customers, AWS and others. In the contract with the Dutch government, AWS guarantees that its Trust & Safety team shall not disclose Account Information to third parties without the Customer's permission, unless required by law or court order. If AWS Trust & Safety has a legal obligation to disclose Account Information to third parties, it will notify Customer, unless prohibited from doing so by law or a court order. AWS also guarantees that it has not purposefully created any "backdoors" or similar programming in the Services that could be used by AWS or by third parties to obtain unauthorised access to the system and/or Personal Data stored in the system. AWS adds: AWS Artifact is the central resource for compliance-related information, it provides on-demand access to security and compliance reports from AWS and ISVs who sell their products on AWS Marketplace. AWS offers distinct solutions to federate customer's employees, contractors, and partners (workforce) to AWS accounts and business applications, and for adding federation support to customer's end-user-facing web and mobile applications. AWS supports commonly used open identity standards, including Security Assertion Markup Language 2.0 (SAML 2.0), Open ID Connect (OIDC), and OAuth 2.0. References: https://aws.amazon.com/compliance/programs/ https://aws.amazon.com/artifact/ https://aws.amazon.com/identity/federation/
k)	Relevant onward transfer(s) of personal data (if any):	Not applicable
l)	Countries of recipients of relevant onward transfer(s):	N/a

Step 2: Define the DTIA parameters

			Rationale
a)	Starting date of the transfer:	[Gov org to fill in the date]	
b)	Assessment period in years:	2	
c)	Ending date of the assessment based on the above:	X+2	
d)	Target jurisdiction for which the DTIA is made:	USA	
e)	Is importer an Electronic Communications Service Provider as defined in USC § 1881(b)(4):	Yes	
f)	Does importer/processor commit to legally resist every request for access :	Yes	
g)	Relevant local laws taken into consideration:	FISA Section 702, other FISA warrants such as business records, pen registers and trap and trace devices, National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA),NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants. Additionally, mass surveillance / cable interception based on EOP 12333 (mitigated by PPD-28),	*This DTIA takes the risks of two types of US legislation into account: traditional law enforcement, and court ordered subpoenas and warrants, as well as secret services powers, letters and FISC authorisations. Since AWS offers 'remote computing services' that are part of the definition of 'Electronic Communications Service Provider' as defined in article 50 of the US Code par. 1881(b) under 4, sub c, the US government has the authority to engage in bulk surveillance based on EOP 12333 and to issue direct orders to AWS based on FISA Section 702. Additionally, the US Stored Communications Act and US CLOUD Act apply. This DTIA does *not* assess the risks of requests for personal data ordered by EU law enforcement authorities through MLAT requests. AWS emphasises that EOP 12333 does not include any authorization to compel private companies to disclose data from their customers.*

Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider

		Probability per case	Cases per year	Cases remaining	Rationale
a)	Number of cases under the laws listed in Step 2g per year in which an authority in the USA is estimated to attempt to obtain relevant data through legal action during the period under consideration.		0,50		*The number of 0,5 case per year is an estimate based on AWS's own transparency reporting and assurance that none of the subpoenas, search warrants and court orders resulted in the disclosure to the U.S. government of Enterprise Content Data located outside the United States. Since AWS included the metric in the reports (July 2020), the reports notes:* *"How many requests resulted in the disclosure to the U.S. government of enterprise or government content data located outside the United States?* *None."* *AWS does not provide specific information if it has ever disclosed Diagnostic Data to law enforcement or security services. See: https://aws.amazon.com/compliance/amazon-information-requests/* *The low estimate is also based on AWS's commitments in the AWS Supplementary Addendum, the historical data available in this sector, and on the requirement to calculate based on a number greater than zero.*
b)	Share of such cases in which the request occurs in connection with a case that due to its nature in principle permits the authority to obtain the data also from a provider	100%	0,50		
c)	Probability that in the remaining such cases it will be possible for the company to successfully cause the authority (by legal means or otherwise) to give up its request for the data **in plain text**	0%	0,50		*As contractually agreed with the Dutch government, the AWS Trust & Safety team shall not disclose Account Information to third parties without the Customer's permission, unless required by law or court order. If AWS Trust & Safety has a legal obligation to disclose Account Information to third parties, it will notify Customer, unless prohibited from doing so by law or a court order. Both the Security Data and the complaints are available for AWS employees in the clear, customers cannot encrypt these data with self-controlled keys. Because AWS acts as data controller for these data, it is unlikely that AWS can successfully resist an order to produce these personal data in plain text.*

d)	Probability that in the remaining cases the requested data will be provided in one way or another (e.g., with consent or through legal or administrative assistance)	100%	0,00		*There is a chance that AWS is compelled to disclose Security Data or data from the T&S team. AWS's public commitments to resist such disclosures (in the Addendum) only apply to the personal data for which AWS acts as processor, not to these personal data. However, as noted in 33F above, AWS does commit to resist and inform. Consent from an EU Enterprise Customer is unlikely, in the absence of a data protection adequacy decision from the European Commission for the USA.*
e)	Probability that in the remaining cases the authority will consider the data it is seeking to be so important that it will look for another way to obtain it	10%	0,00	0,00	*Data about security incidents, or reports about illegal content are probably not interesting enough to seek access through another way.*

Number of cases per year in which the question of lawful access by a foreign authority arises	0,00
Number of cases in the period under consideration	0,00

Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider

Legal Basis considered for the following assessment: Section 702 FISA, other FISA warrants such as business records, pen registers and trap and trace devices, National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA), NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants.

	Prerequisite for success	**Probability per case**			**Rationale**
a)	Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1)	100%		100%	*AWS is a well-known cloud services provider with a substantial amount of Enterprise and Edu Customers in the EU*
b)	Probability that an employee of the provider or its subcontractors will gain access to the data in plain text in a support-case ... (prerequisite no. 2)	100%	100,00%		*Authorised AWS employees can have access to Security and T&S Data when necessary for their tasks.*
	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	100%			*Idem*
c)	Probability that despite the technical countermeasures taken, employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside a support situation (e.g., using admin privileges) or are able to gain such access, e.g., by covertly installing a backdoor or "hacking" into the system (irrespective of whether they are allowed to do so) ... (prerequisite no. 2)	50%	50,00%	100%	*Idem. AWS guarantees in the privacy amendment with the Dutch government that the Trust & Safety team shall not disclose Account Information to third parties without the Customer's permission, unless required by law or court order. If AWS Trust & Safety has a legal obligation to disclose Account Information to third parties, it will notify Customer, unless prohibited from doing so by law or a court order. AWS also guarantees that it has not purposefully created any "backdoors" or similar programming in the Services that could be used by AWS or by third parties to obtain unauthorised access to the system and/or Personal Data stored in the system. There are no findings of non-compliance with the access rules in the recent C5:20202 audit.*
	... and are then able to search for, find and copy the data requested by the authority (prerequisite no. 3)	100%			*Idem*
d)	Probability that the provider, the subcontractor or its parent company, respectively, is located within the jurisdiction of the authority (prerequisite no. 4)	100%		100%	*AWS is a US based company and has access to the Security and T&S Data processed in the USA*
e)	Probability that despite the technically limited access and the technical and organizational countermeasures in place, the authority is permitted to order the provider, its subcontractor or the parent company, respectively, to obtain access to the data and produce it to the authority in plain text (prerequisite no. 5)	100%		100%	*Though the probability is estimated at the maximum of 100%, AWS has robust controls in place and has these controls audited. There are no findings in the recent C5:2020 audit about disclosure to authorities.*
f)	Probability that if data were to be handed over to the foreign authority, this would lead to the criminal liability of employees of the provider or its subcontractors, the prosecution of which would be possible and realistic, and as a consequence, the data does not have to be produced or is not produced (prerequisite no. 6)	80%		20%	*According to the most recent C5-2020 audit, there were no findings of non-compliance with disclosure policy. Customers can access these audit reports via AWS Artifact, URL: https://aws.amazon.com/artifact/*
g)	Probability that the company does not succeed in removing the relevant data in time or otherwise withdrawing it from the provider's access (prerequisite no. 7)	100%		100%	*If AWS receives a valid order/warrant or subpoena, AWS may be subjected to gagging order. As quated in F48 above, AWS contractually commits not to disclose Account Information to third parties without the Customer's permission, unless required by law or court order. If AWS Trust & Safety has a legal obligation to disclose Account Information to third parties, it will notify Customer, unless prohibited from doing so by law or a court order.*

Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures):	20,00%

Step 4b: Probability of foreign lawful access by mass surveillance contents

Legal Basis considered for the following assessment: Section 702 US Foreign Intelligence Surveillance Act (FISA), CIA surveillance based on Executive Order (EO) 12333

		Probability in the period			**Rationale**
a)	Probability that the data at issue is transmitted to the provider or its subcontractors in a manner that permits the telecommunications providers in the country to view it in plain text as part of an upstream monitoring of Internet backbones	0%	0,00%		*AWS applies encryption to all data in transit.*
b)	Probability that the data transmitted will include content picked by selectors (i.e., intelligence search terms such as specific recipients or senders of electronic communications)	0%			*AWS applies encryption to all data in transit.*
c)	Probability that the provider or a subcontractor in the country is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the customer's permission as part of a downstream monitoring of online communications	0%		0,00%	*AWS applies encryption to all data in transit.*
d)	Probability that the provider or a subcontractor in the country above may be legally required to perform such as search (also) with the company's data	50%	0,00%		*This refers to Upstream Data Collection. It is possible that some Security and T&S Data relating to an EU government organisation could be interesting for law enforcement and/or security services, depending on the nature of the illegal content or the type of security breach.*
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	50%			*Idem*

Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures):	0,00%

Step 5: Overall assessment

Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)	0,00%
Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures	20,00%
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures)	0,00%
Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period:	0,00%
Description in words (based on Hillson*):	Very low

The number of years it takes for a lawful access to occur at least once with a **90 percent** probability: ∞
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability: ∞
... assuming that the probability neither increases nor decreases over time (like tossing a coin)

** Scale: <5% = "Very low", 5-10% = "Low", 11-25 = "Medium", 26-50% = "High" and >50% = "Very high" (by David Hillson, 2005, see https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*

Step 6: Data subject risks

				Rationale
a)	*Estimated probability of occurance of successful lawful access risk:*	*0,00%*	*Very Low*	
b)	*Estimated impact of risk*	*3= regular personal data in the clear*	*High*	*If the Security Data reveal that a VM with sensitive data in the EU was breached, or was involved in malicious network activity, this in turn may lead to the processing of special categories of personal data about the admin(s) of the VM, or EC2-hosted website. AWS or third parties may then take steps to re-identify the responsible admin(s) or website visitors based on the pseudonymous data in the security events.*

Very High	Low	High	High	High	High
High	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	High
	0	1	2	3	4

Low

Step 7: Define the safeguards in place

				Rationale
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	*Describe why you still do not pursue this option*	*AWS processes the Security Data and T&S data in the USA, and does not have an EU based Trust & Safety Team*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	Yes	*Make sure that the prerequisites are fulfilled!*	*No.*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	*Ensure that data remains encrypted*	*Data in transit are encrypted by AWS (SSL/TLS).*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*Yes. The Security & T&S Data can be accessed in the clear by AWS employees in the USA when they are permitted access*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	*Ensure that the mechanism remains in place and is complied with*	*AWS as controller contractually commits not to disclose the Security Data and T&S data to third parties without customer authorisation. If AWS would receive a valid order, with a gagging order, the transfer would qualify as incidental.*
Based on the answers given above, the transfer is:		**permitted**		*Organisations should apply identity federation to he Account Data for employees whose identity should remain confidential*

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: **permitted**

Reassess at the latest by: X+2
(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
SLM Rijk / PRIVACY COMPANY

Place, Date:

Signed: _____

By: [Government org X]

Data Transfer Impact Assessment (DTIA) on the transfer of Admin Account Data to AWS in the USA

Step 1: Describe the intended transfer

a)	Data exporter (or the sender in case of a relevant onward transfer):	Dutch government organisation [X]
b)	Country of data exporter:	Netherlands
c)	Data importer (or the recipient in case of a relevant onward transfer):	Amazon Web Services, Inc. ("AWS, Inc.", abbreviated in this DTIA to: "AWS")
d)	Country of data importer:	USA. Seller of Record is Amazon Web Services EMEA SARL ("AWS Europe"), a Luxembourg-based AWS entity. Both AWS and AWS Europe are wholly owned subsidiaries of Amazon.com, Inc. AWS works with Regions, a physical location in a country where data centers are clustered. AWS has Regions in the EU. Each AWS Region consists of a minimum of three, isolated, and physically separate AZs within a geographic area. AWS calls each group of logical data centers an Availability Zone.
e)	Context and purpose of the transfer:	Account Data from employee admins of the MOJ or any other Governmental entity that use Amazon EC2, Amazon S3, and Amazon RDS to store and process Content Data
f)	Categories of data subjects concerned:	Employees of the Dutch government (admins)
g)	Categories of personal data transferred:	Account Data can also form part of Diagnostic Data and can be included in support requests. See the separate tabs in this DTIA for the Support Data and Diagnostic Data
h)	Sensitive and special categories of personal data:	Account Data may be considered confidential, if an employee works for a government organisation with a high level of sensitivity, or if the employee is a VIP. Admins that manage databases with confidential/secret or otherwise sensitive information can become targets of spearphishing if their identity is leaked.
i)	Technical implementation of the transfer:	Account Data may be stored in the United States
j)	Technical and organizational measures in place:	AWS has elaborate Security Standards, and has its compliance with these standards tested in different types of audits. The reports are available for customers. This DTIA assumes government organisations will pseudonymise admin account data by using identity federation. Additionally, AWS commits to use every reasonable effort to redirect valid and binding orders for Account Data to its Customer. If compelled to disclose Personal Data to a Requesting Party, AWS will (i) promptly notify Customer of the Request to allow Customer to seek a protective order or other appropriate remedy, if AWS is legally permitted to do so. If AWS is prohibited from notifying Customer about the Request, AWS will use all reasonable and lawful efforts to obtain a waiver of prohibition, to allow AWS to communicate as much information to Customer as soon as possible; and (ii) challenge any overbroad or inappropriate Request (including where such Request conflicts with the law of the European Union or applicable Member State law).
k)	Relevant onward transfer(s) of personal data (if any):	Admins can and should pseudonymise their Account Data (collected in the Diagnostic Data). AWS offers solutions to federate customer's employees, contractors, and partners (workforce) to AWS accounts and business applications, and offers federation support to customer's end-user-facing web and mobile applications. AWS supports commonly used open identity standards, including Security Assertion Markup Language 2.0 (SAML 2.0), Open ID Connect (OIDC), and OAuth 2.0. URL: https://aws.amazon.com/identity/federation/. Additionally, AWS applies encryption to all data in transit. SLM Rijk and AWS have signed the new Controller to Processor SCC. In the contract with the Dutch government, AWS guarantees that it has not purposefully created any "backdoors" or similar programming in the Services that could be used by AWS or by third parties to obtain unauthorised access to the system and/or Personal Data stored in the system. Additionally, AWS commits to use every reasonable effort to redirect valid and binding orders for Account Data to its Customer. If compelled to disclose Personal Data to a Requesting Party, AWS will (i) promptly notify Customer of the Request to allow Customer to seek a protective order or other appropriate remedy, if AWS is legally permitted to do so. If AWS is prohibited from notifying Customer about the Request, AWS will use all reasonable and lawful efforts to obtain a waiver of prohibition, to allow AWS to communicate as much information to Customer as soon as possible; and (ii) challenge any overbroad or inappropriate Request (including where such Request conflicts with the law of the European Union or applicable Member State law).
l)	Countries of recipients of relevant onward transfer(s):	Not applicable [apart from Support Data, see separate tab]

Step 2: Define the DTIA parameters

			Rationale
a)	Starting date of the transfer:	[Gov org to fill in the date]	
b)	Assessment period in years:	2	
c)	Ending date of the assessment based on the above:	X+2	
d)	Target jurisdiction for which the DTIA is made:	USA	
e)	Is importer an Electronic Communications Service Provider as defined in USC § 1881(b)(4):	Yes	
f)	Does importer/processor commit to legally resist every request for access :	Yes	
g)	Relevant local laws taken into consideration:	FISA Section 702, other FISA warrants such as business records, pen registers and trap and trace devices, National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA),NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants. Additionally, mass surveillance / cable interception based on EOP 12333 (mitigated by PPD-28),	*This DTIA takes the risks of two types of US legislation into account: traditional law enforcement, and court ordered subpoenas and warrants, as well as secret services powers, letters and FISC authorisations. Since AWS offers 'remote computing services' that are part of the definition of 'Electronic Communications Service Provider' as defined in article 50 of the US Code par. 1881(b) under 4, sub c, the US government has the authority to engage in bulk surveillance based on EOP 12333 and to issue direct orders to AWS based on FISA Section 702. Additionally, the US Stored Communications Act and US CLOUD Act apply. This DTIA does *not* assess the risks of requests for personal data ordered by EU law enforcement authorities through MLAT requests. AWS emphasises that EOP 12333 does not include any authorization to compel private companies to disclose data from their customers.*

Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider

		Probability per case	Cases per year	Cases remaining	Rationale
a)	Number of cases under the laws listed in Step 2g per year in which an authority in the USA is estimated to attempt to obtain relevant data through legal action during the period under consideration.		0,50		*The number of 0,5 case per year is an estimate based on AWS's own transparency reporting and assurance that none of the subpoenas, search warrants and court orders resulted in the disclosure to the U.S. government of Enterprise Content Data located outside the United States. Since AWS included the metric in the reports (July 2020), the reports notes:* *"How many requests resulted in the disclosure to the U.S. government of enterprise or government content data located outside the United States?* *None."* *AWS does not provide specific information if it has ever disclosed Account Data to law enforcement or security services. See: https://aws.amazon.com/compliance/amazon-information-requests/* *The low estimate is also based on AWS's commitments in the AWS Supplementary Addendum, the historical data available in this sector, and on the requirement to calculate based on a number greater than zero.*
b)	Share of such cases in which the request occurs in connection with a case that due to its nature in principle permits the authority to obtain the data also from a provider	100%	0,50		*As documented in the AWS Supplementary Addendum, AWS will challenge any overbroad or inappropriate requests or gagging orders. AWS writes that it has repeatedly challenged government demands for customer information that it believed were overbroad, winning decisions that have helped to set the legal standards for protecting customer speech and privacy interests.See: https://d1.awsstatic.com/legal/aws-dpa/supplementary-addendum-to-the-aws-dpa.pdf.* *Additionally, in Clause 14 of the SCC AWS guarantees it has no reason to believe that it cannot fulfill its obligations under the clauses due to lawful access orders and requests.*
c)	Probability that in the remaining such cases it will be possible for the company to successfully cause the authority (by legal means or otherwise) to give up its request for the data **in plain text**	100%	0,00		*The Account Data are available for AWS employees in the clear, customers cannot encrypt these data with self-controlled keys, but they can mask the identity with identity federation. Hence the probability is low that AWS can successfully resist an order to produce Account Data in plain text, in spite of its commitments.*
d)	Probability that in the remaining cases the requested data will be provided in one way or another (e.g., with consent or through legal or administrative assistance)	25%	0,00		*There is a chance that AWS is compelled to disclose Account Data, in spite of its commitments. Consent from an EU Enterprise Customer is unlikely, in the absence of a data protection adequacy decision from the European Commission for the USA. Since AWS is a processor, and not a controller for the personal data in the Account Data, it will take time for the US authorities to force AWS to provide the requested data. Additionally, there will be a delay in obtaining an FISA 702 order. This delay enables AWS to inform the customer that it can no longer comply with SCC guarantees without disclosing that it has received a FISA 702 order.*
e)	Probability that in the remaining cases the authority will consider the data it is seeking to be so important that it will look for another way to obtain it	10%	0,00	0,00	*It is assumed this question tries to assess the probability that AWS is hacked or an invididual employee is blackmailed/bribed to hand over Account Data. This cannot be excluded (though the risk for the employee can be minimised by using identity federation).*
Number of cases per year in which the question of lawful access by a foreign authority arises				0,00	
Number of cases in the period under consideration				0,00	

Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider

Legal Basis considered for the following assessment: Section 702 FISA, other FISA warrants such as business records, pen registers and trap and trace devices, National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA), NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants.

	Prerequisite for success	Probability per case			Rationale
a)	Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1)	100%		100%	*AWS is a well-known cloud services provider with a substantial amount of Enterprise and Edu Customers in the EU*
b)	Probability that an employee of the provider or its subcontractors will gain access to the data in plain text in a support-case ... (prerequisite no. 2)	50%			*It is assumed that government organisations follow the recommendation to use pseudonyms for admin Account Data. However, if an admin corresponds with a support employee, it is plausible that names and contact data are exchanged.*
	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	50%	49,00%		*See above.*
c)	Probability that despite the technical countermeasures taken, employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside a support situation (e.g., using admin privileges) or are able to gain such access, e.g., by covertly installing a backdoor or "hacking" into the system (irrespective of whether ... and are then able to search for, find and copy the data requested by the authority (prerequisite no. 3)	25% 0%	0,00%	49%	*Only the government organisation should know the identity of the admin, but it is possible that AWS is able to combine information from its Support Employees with the pseudonyms. AWS restricts its personnel from processing Personal Data without authorisation by AWS as described in the AWS Security Standards. AWS imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.*
d)	Probability that the provider, the subcontractor or its parent company, respectively, is located within the jurisdiction of the authority (prerequisite no. 4)	100%		100%	*AWS is a US based company and has access to the Account Data that may be processed in the USA.*
e)	Probability that despite the technically limited access and the technical and organizational countermeasures in place, the authority is permitted to order the provider, its subcontractor or the parent company, respectively, to obtain access to the data and produce it to the authority in plain text (prerequisite no. 5)	100%		100%	*Though the probability is estimated at the maximum of 100%, AWS has robust controls in place and has these controls audited. There are no findings in the recent C5:2020 audit about disclosure to authorities.*
f)	Probability that if data were to be handed over to the foreign authority, this would lead to the criminal liability of employees of the provider or its subcontractors, the prosecution of which would be possible and realistic, and as a consequence, the data does not have to be produced or is not produced (prerequisite no. 6)	80%		20%	*As documented in the AWS Supplementary Addendum, AWS will challenge any overbroad or inappropriate requests or gagging orders. See the explanation in F32 above. According to the most recent C5-2020 audit, there were no findings of non-compliance with this policy. Customers can access these audit reports via AWS Artifact, URL: https://aws.amazon.com/artifact/*
g)	Probability that the company does not succeed in removing the relevant data in time or otherwise withdrawing it from the provider's access (prerequisite no. 7)	100%		100%	*If AWS receives a valid order/warrant or subpoena, AWS may be subjected to gagging order and not permitted to inform its Customer. Hence AWS may not be in a position to issue a timely warning to its customer that it can no longer comply with the data protection guarantees in the SCC.*

Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures): 9,80%

Step 4b: Probability of foreign lawful access by mass surveillance contents

Legal Basis considered for the following assessment: Section 702 US Foreign Intelligence Surveillance Act (FISA), CIA surveillance based on Executive Order (EO) 12333

		Probability in the period			Rationale
a)	Probability that the data at issue is transmitted to the provider or its subcontractors in a manner that permits the telecommunications providers in the country to view it in plain text as part of an upstream monitoring of Internet backbones	0%	0,00%		*The probability is zero for Account Data transferred to AWS in the USA, due to TLS encryption*
b)	Probability that the data transmitted will include content picked by selectors (i.e., intelligence search terms such as specific recipients or senders of electronic communications)	0%			*Idem*
c)	Probability that the provider or a subcontractor in the country is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the customer's permission as part of a downstream monitoring of online communications	0%		0,00%	*Idem*
d)	Probability that the provider or a subcontractor in the country above may be legally required to perform such as search (also) with the company's data	50%	0,00%		*This refers to Upstream Data Collection. It is plausible that some Account Data from an EU government organisation are interesting for law enforcement and/or security services. However, it is unlikely that disclosure of the Account Data would cause risks if the government organisations follow the recommendation to use identity federation.*
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	5%			*The possibility that Account Data processed by AWS by an EU gov or university organisation are considered interesting for intelligence searches cannot be excluded, but the risk will be very low if government organisations apply the recommended pseudonymisation.*

Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures): 0,00%

Step 5: Overall assessment

Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%) 0,00%

Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures 9,80%

Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures) 0,00%

Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period: 0,00%

Description in words (based on Hillson*): Very low

The number of years it takes for a lawful access to occur at least once with a **90 percent** probability: ∞
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability: ∞
... assuming that the probability neither increases nor decreases over time (like tossing a coin)

** Scale: <5% = "Very low", 5-10% = "Low", 11-25 = "Medium", 26-50% = "High" and >50% = "Very high" (by David Hillson, 2005, see https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*

Step 6: Data subject risks

				Rationale
a)	*Estimated probability of occurance of successful lawful access risk:*	*0,00%*	*Very Low*	
b)	*Estimated impact of risk*	*3= regular personal data in the clear*	*High*	

Very High	Low	High	High	High	High
High	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	High
	0	1	2	3	4

Low

The risk assessment assumes the Customer will use identity federation for employee administrators accounts

Step 7: Define the safeguards in place

				Rationale
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	*Describe why you still do not pursue this option*	*AWS does not offer EU geolocalisation for Account Data*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		*Data in transit are encrypted by AWS (SSL/TLS). Admins can and should pseudonymise their Account Data (collected in the service generated server logs) with identity federation.*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	*Ensure that data remains encrypted*	*Recommendation to admins to pseudonymise admin Account Data with identity federation. All traffic over the internet is protected by encryption in transit (SSL/TLS).*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*Yes. The Account Data can be accessed in the clear by AWS employees when they are permitted access, and by the support employees that are permitted to work with Support Data.*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	*Ensure that the mechanism remains in place and is complied with*	*SLM Rijk and AWS have signed the new SCC Controller to Processor.*

Based on the answers given above, the transfer is: **permitted**

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: **permitted**

Reassess at the latest by: X+2
(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
SLM Rijk / PRIVACY COMPANY

Place, Date:

Signed: _____

By: [Government org X]

Data Transfer Impact Assessment (DTIA) on the transfer of restricted access Website Data to AWS in the USA

Step 1: Describe the intended transfer

a)	Data exporter (or the sender in case of a relevant onward transfer):	Dutch government organisation [X]
b)	Country of data exporter:	Netherlands
c)	Data importer (or the recipient in case of a relevant onward transfer):	Amazon Web Services, Inc. ("AWS, Inc.", abbreviated in this DTIA to: "AWS")
d)	Country of data importer:	USA. Seller of Record is Amazon Web Services EMEA SARL ("AWS Europe"), a Luxembourg-based AWS entity. Both AWS and AWS Europe are wholly owned subsidiaries of Amazon.com, Inc. AWS works with Regions, a physical location in a country where data centers are clustered. AWS has Regions in the EU. Each AWS Region consists of a minimum of three, isolated, and physically separate AZs within a geographic area. AWS calls each group of logical data centers an Availability Zone.
e)	Context and purpose of the transfer:	Employee admins that necessarily have to use the Admin Console (restricted access website) to manage the Amazon EC2, Amazon S3, and Amazon RDS services
f)	Categories of data subjects concerned:	Employees of the Dutch government
g)	Categories of personal data transferred:	Diagnostic Data generated in webserver access logs through the individual visits to the Admin Console. The webserver access logs contain pseudonymous data like user and device identifiers, and IP addresses
h)	Sensitive and special categories of personal data:	Website access logs may include Account Data from employee administrators whose identity should remain confidential.
i)	Technical implementation of the transfer:	Website Diagnostic Data may be generated in the region where the website is accessed or deployed, and depending on the scope of the customer's interactions, Website Data may be stored in or accessed from multiple countries, including the United States.
j)	Technical and organizational measures in place:	AWS has elaborate Security Standards, and has its compliance with these standards tested in different types of audits. The reports are available for customers. Additionally, AWS commits to use every reasonable effort to redirect valid and binding orders for Website Data to its Customer. If compelled to disclose personal sata to a Requesting Party, AWS will (i) promptly notify Customer of the Request to allow Customer to seek a protective order or other appropriate remedy, if AWS is legally permitted to do so. If AWS is prohibited from notifying Customer about the Request, AWS will use all reasonable and lawful efforts to obtain a waiver of prohibition, to allow AWS to communicate as much information to Customer as soon as possible; and (ii) challenge any overbroad or inappropriate Request (including where such Request conflicts with the law of the European Union or applicable Member State law).
k)	Relevant onward transfer(s) of personal data (if any):	AWS sets essential, functional, and performance cookies. Even though its cookie policy suggests the use of advertising cookies, AWS does not set advertising or third party cookies when a customer uses a browser to access the AWS console, including when using the console to access the EC2, S3, or RDS service management interfaces. Admins are advised to always use the minimum level of essential cookies.
l)	Countries of recipients of relevant onward transfer(s):	n/a

Step 2: Define the DTIA parameters

			Rationale
a)	Starting date of the transfer:	[Gov org to fill in the date]	
b)	Assessment period in years:	2	
c)	Ending date of the assessment based on the above:	X+2	
d)	Target jurisdiction for which the DTIA is made:	USA	
e)	Is importer an Electronic Communications Service Provider as defined in USC § 1881(b)(4):	Yes	
f)	Does importer/processor commit to legally resist every request for access :	Yes	
g)	Relevant local laws taken into consideration:	FISA Section 702, other FISA warrants such as business records, pen registers and trap and trace devices, National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA),NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants. Additionally, mass surveillance / cable interception based on EOP 12333 (mitigated by PPD-28),	*This DTIA takes the risks of two types of US legislation into account: traditional law enforcement, and court ordered subpoenas and warrants, as well as secret services powers, letters and FISC authorisations. Since AWS offers 'remote computing services' that are part of the definition of 'Electronic Communications Service Provider' as defined in article 50 of the US Code par. 1881(b) under 4, sub c, the US government has the authority to engage in bulk surveillance based on EOP 12333 and to issue direct orders to AWS based on FISA Section 702. Additionally, the US Stored Communications Act and US CLOUD Act apply. This DTIA does *not* assess the risks of requests for personal data ordered by EU law enforcement authorities through MLAT requests. AWS emphasises that EOP 12333 does not include any authorization to compel private companies to disclose data from their customers.*

Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider

		Probability per case	Cases per year	Cases remaining	Rationale
a)	Number of cases under the laws listed in Step 2g per year in which an authority in the USA is estimated to attempt to obtain relevant data through legal action during the period under consideration.		0,50		*The number of 0,5 case per year is an estimate based on AWS's own transparency reporting and assurance that none of the subpoenas, search warrants and court orders resulted in the disclosure to the U.S. government of Enterprise Content Data located outside the United States. Since AWS included the metric in the reports (July 2020), the reports notes:* *"How many requests resulted in the disclosure to the U.S. government of enterprise or government content data located outside the United States?* *None."* *AWS does not provide specific information if it has ever disclosed Website Data to law enforcement or security services. See: https://aws.amazon.com/compliance/amazon-information-requests/* *The low estimate is also based on AWS's commitments in the AWS Supplementary Addendum, the historical data available in this sector, and on the requirement to calculate based on a number greater than zero.*
b)	Share of such cases in which the request occurs in connection with a case that due to its nature in principle permits the authority to obtain the data also from a provider	100%	0,50		*As documented in the AWS Supplementary Addendum, AWS will challenge any overbroad or inappropriate requests or gagging orders. AWS writes that it has repeatedly challenged government demands for customer information that it believed were overbroad, winning decisions that have helped to set the legal standards for protecting customer speech and privacy interests.See: https://d1.awsstatic.com/legal/aws-dpa/supplementary-addendum-to-the-aws-dpa.pdf.* *Additionally, in Clause 14 of the SCC AWS guarantees it has no reason to believe that it cannot fulfill its obligations under the clauses due to lawful access orders and requests.*
c)	Probability that in the remaining such cases it will be possible for the company to successfully cause the authority (by legal means or otherwise) to give up its request for the data **in plain text**	10%	0,45		*The Website Data are available for AWS employees in the clear, customers cannot encrypt these data with self-controlled keys. Hence the probability is low that AWS can successfully resist an order to produce Website Data in plain text, in spite of its commitments.*
d)	Probability that in the remaining cases the requested data will be provided in one way or another (e.g., with consent or through legal or administrative assistance)	25%	0,34		*There is a chance that AWS is compelled to disclose Website Data, in spite of its commitments. Consent from an EU Enterprise Customer is unlikely, in the absence of a data protection adequacy decision from the European Commission for the USA. Since AWS is a processor, and not a controller for the personal data in the restricted access Website Data, it will take time for the US authorities to force AWS to provide the requested data. Additionally, there will be a delay in obtaining an FISA 702 order. This delay enables AWS to inform the customer that it can no longer comply with SCC guarantees without disclosing that it has received a FISA 702 order.*
e)	Probability that in the remaining cases the authority will consider the data it is seeking to be so important that it will look for another way to obtain it	10%	0,03	0,03	*It is assumed this question tries to assess the probability that AWS is hacked or an invididual employee is blackmailed/bribed to hand over Website Data. This cannot be excluded.*
	Number of cases per year in which the question of lawful access by a foreign authority arises			0,03	
	Number of cases in the period under consideration			0,07	

Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider

Section 702 FISA, other FISA warrants such as business records, pen registers and trap and trace devices, National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA), NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants.

Legal Basis considered for the following assessment:

	Prerequisite for success	Probability per case			Rationale
a)	Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1)	100%		100%	*AWS is a well-known cloud services provider with a substantial amount of Enterprise and Edu Customers in the EU*
b)	Probability that an employee of the provider or its subcontractors will gain access to the data in plain text in a support-case ... (prerequisite no. 2)	50%			*Authorised AWS employees can have access to Website Data when necessary for their tasks, but the probability that they need access to these data for a Support Case is (at most) half of the probability of general Diagnostic Data.*
			49.00%		

	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	50%			*Idem*
c)	Probability that despite the technical countermeasures taken, employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside a support situation (e.g., using admin privileges) or are able to gain such access, e.g., by covertly installing a backdoor or "hacking" into the system (irrespective of whether they are allowed to do so) ... (prerequisite no. 2)	50%	25,00%	62%	*Authorised AWS employees can have access to Website Data when necessary for their tasks. AWS restricts its personnel from processing Personal Data without authorisation by AWS as described in the AWS Security Standards. AWS imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.* *AWS guarantees that it has not purposefully created any "backdoors" or similar programming in the Services that could be used by AWS or by third parties to obtain unauthorised access to the system and/or Personal Data stored in the system. There are no findings of non-compliance with the access rules in the C5:20202 audit.*
	... and are then able to search for, find and copy the data requested by the authority (prerequisite no. 3)	50%			*Idem.*
d)	Probability that the provider, the subcontractor or its parent company, respectively, is located within the jurisdiction of the authority (prerequisite no. 4)	100%		100%	*AWS is a US based company and has access to the restricted access Website Data.*
e)	Probability that despite the technically limited access and the technical and organizational countermeasures in place, the authority is permitted to order the provider, its subcontractor or the parent company, respectively, to obtain access to the data and produce it to the authority in plain text (prerequisite no. 5)	100%		100%	*Though the probability is estimated at the maximum of 100%, AWS has robust controls in place and has these controls audited. There are no findings in the recent C5:2020 audit about disclosure to authorities.*
f)	Probability that if data were to be handed over to the foreign authority, this would lead to the criminal liability of employees of the provider or its subcontractors, the prosecution of which would be possible and realistic, and as a consequence, the data does not have to be produced or is not produced (prerequisite no. 6)	80%		20%	*As documented in the AWS Supplementary Addendum, AWS will challenge any overbroad or inappropriate requests or gagging orders. See the explanation in F32 above. According to the most recent C5-2020 audit, there were no findings of non-compliance with this policy. Customers can access these audit reports via AWS Artifact, URL: https://aws.amazon.com/artifact/*
g)	Probability that the company does not succeed in removing the relevant data in time or otherwise withdrawing it from the provider's access (prerequisite no. 7)	100%		100%	*If AWS or its subprocessors receive a valid order/warrant or subpoena, AWS may be subjected to gagging order and not permitted to inform its Customer. Hence AWS may not be in a position to issue a timely warning to its customer that it can no longer comply with the data protection guarantees in the SCC.*

Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures): **12,35%**

Step 4b: Probability of foreign lawful access by mass surveillance contents

Legal Basis considered for the following assessment: Section 702 US Foreign Intelligence Surveillance Act (FISA), CIA surveillance based on Executive Order (EO) 12333

		Probability in the period			Rationale
a)	Probability that the data at issue is transmitted to the provider or its subcontractors in a manner that permits the telecommunications providers in the country to view it in plain text as part of an upstream monitoring of Internet backbones	0%			*AWS applies encryption to all data in transit.*
b)	Probability that the data transmitted will include content picked by selectors (i.e., intelligence search terms such as specific recipients or senders of electronic communications)	0%	0,00%		*AWS applies encryption to all data in transit.*
c)	Probability that the provider or a subcontractor in the country is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the customer's permission as part of a downstream monitoring of online communications	0%		0,00%	*AWS applies encryption to all data in transit.*
d)	Probability that the provider or a subcontractor in the country above may be legally required to perform such as search (also) with the company's data	10%	0,00%		*This refers to Upstream Data Collection. It is unlikely that restricted access Website Data from an EU government organisation are interesting for law enforcement and/or security services, but there may be a legal requirement.*
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	5%			*The possibility that the restricted access Website Data processed by AWS for an EU gov are considered interesting for intelligence searches seems extremely slim, but cannot be excluded*

Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures): **0,00%**

Step 5: Overall assessment

Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)	6,75%
Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures	12,35%
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures)	0,00%
Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period:	0,83%
Description in words (based on Hillson*):	Very low
The number of years it takes for a lawful access to occur at least once with a **90 percent** probability:	∞
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability:	∞

... assuming that the probability neither increases nor decreases over time (like tossing a coin)

** Scale: <5% = "Very low", 5-10% = "Low", 11-25 = "Medium", 26-50% = "High" and >50% = "Very high" (by David Hillson, 2005, see https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*

Step 6: Data subject risks

					Rationale
a)	*Estimated probability of occurance of successful lawful access risk:*	*0,83%*	*Very Low*		
b)	*Estimated impact of risk*	*3= regular personal data in the clear*	*High*		

Very High	Low	High	High	High	High
High	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	High
	0	1	2	3	4

Low

The risk assessment assumes the Customer will use identity federation for employees whose identity should remain confidential

Step 7: Define the safeguards in place

				Rationale
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	*Describe why you still do not pursue this option*	*Website Data may be generated in the EU availability zone selected by the customer, but subsequently stored in or accessed from multiple countries, including the United States.*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		*Use of the website is required for admins to perform their regular work duties, therefore this involves a structural, not an incidental data transfer*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	*Ensure that data remains encrypted*	*Recommendation to admins to pseudonymise confidential Account Data with identity federation. All traffic over the internet is protected by encryption in transit (SSL/TLS).*

d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*Yes. The logs can be accessed in the clear by AWS employees when they are permitted access*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	*Ensure that the mechanism remains in place and is complied with*	*SLM Rijk and AWS have signed the new SCC Controller to Processor.*

Based on the answers given above, the transfer is: **permitted**

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: **permitted**

Reassess at the latest by: X+2
(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
SLM Rijk / PRIVACY COMPANY

Place, Date:

Signed: _____

By: [Government org X]