Notes on the Joint GEANT-EUNIS CLOUD Management workshop

Topics: GDPR, Schrems, Data classification, Security

Date and time:	Friday, 01 April 2022/ 10.00 - 12.00 CEST
Attendees:	42
Led by:	Denise Dittrich (EUNIS Cloud Community Group) & Maria Ristkok (GÉANT Cloud Team)
Hosted by:	Bas Cordewener (EUNIS Board member)
Links:	Agenda and slides

10.00 Welcome and opening *Bas Cordewener*

10.05 Brief update on EUNIS & GÉANT cloud groups collaborating. *Denise Dittrich (EUNIS) and Maria Ristkok (GÉANT Cloud Team)*

Current EUNIS activities:

Pre-congress workshop on multi-cloud management on 31 May in Goettingen in Germany. Programme tbc.

This will be a face-to-face event as is the Annual Congress, 1 to 3 June: info and registration here: https://www.eunis.org/eunis2022/

Current GÉANT activities:

1. Preparations for the GÉANT Cloud Activity 2022-2023, structuring tasks and teams as a community:
2. Proposal to be submitted mid-may by 40 NRENs and the GÉANT Community
3. Data and information on clouds gathered last year from NRENs: the focus on IaaS service consumption via OCRE framework but also GÉANT IaaS 2016 Framework shows a tremendous increase (2021 equals 4 previous years altogether)
4. Reviews on
   a. Community clouds, delivery and multi-cloud management and system software.
   b. Géant video conferencing solution
   c. TNC 22 Italy conference cloud sessions, 1 day-long cloud event on 13. June

10.10 "Getting to know each other" (break-out groups of 4 pp)
Exchange & discuss

- What are the main security issues concerning the cloud right now?
- What steps did you take concerning Schrems?

10.20 Schrems-2 Changing regulations, practical issues, possible approaches

Magdalena Rzaca (GÉANT GDPR & IPR legal advisor)

Focus on judgement.
Reminder: GDPR applies to personal data only.
Sending data internationally, transfer of data.
2015: Safe Harbour Schrems I decision
2016: Privacy shield initiated and validated
2020: Privacy Shield invalidated by Schrems II, CJEU. It was allowing data transfer in a more simple way between the EU and USA.
The judgement is an issue for big companies: what is the legal bound then?

March 22: EU-USA statement regarding new mechanism for transfer. It summarises the actions to take in 6 steps (knows your transfers, verify platforms, assess laws of platform country, identify and adopt extra measures, take any formal procedural steps, re-evaluate level of protection)

Q1: The concept of “personal data in the public domain" is interesting. But how does that apply? status of staff names, since these are available online already.
A1: Part of the evaluation of the ‘sensitivity’ of the source of personal data (maybe public domain was not the most fortunate word).

10.40 Schrems-2 Q&A, Menti poll Schrems-2 rules (menti.com 8221 4268) *(all)*

Question:
The most pressing problem I encounter with Schrems-2 GDPR rules in my daily work is …?’
Responses:

- Inconsistent decisions
- People’s fear
- How to provide services from enterprises outside of the EU legally/ Nearly impossible to use legally a cloud from international provider
- No concrete statement and rules from the government/a European Roadmap for HE would be welcome
- Individual approaches DPOs take to Schrems and how important their input is for the procurement process
- Legal advisors say no to some things, others still run. Other institutions have reverse decisions.
- End-users don’t care and install inappropriate software/use private accounts
- With which means of encryption or anonymisation can I use which Cloud services in a compliant way?/data Protection/I encrypt data in workloads hosted on premise and in public Cloud Data Centres
- How to deal with google Analytics
- Institutions respecting them
- Challenges are around SaaS. Sub Optimisation around other Saas
- No current issue; waiting for next Schrems to see if any impact
- handling the volume of DPIA's aligning legal and technical alignment. Handling the legal implications of US owned cloud providers
- It creates conflicting views within the organisation on the acceptance of cloud services

Discussion:

- No official template
- Services outside EU: evaluate if they are offering services for people based in EU
- Model : everything is global, not possible to separate every service
- End-user proper governance and internal policies
- Google analytics: not legal everywhere. compliance steps to follow, but difficult

- Data Protection Board: only recommendations, can be interpreted

10.50 Checklist concerning Schrems *Leanne Walsh (HEAnet)*

GDPR Transfer Guide for National Research and Education Networks (NRENs) on the 2020 IaaS+ Framework: https://clouds.geant.org/wp-content/uploads/2022/03/GDPR_Transfer_Guide_for_NRENs.pdf

This is the description of the processes for :

- Personal Data Transfer Checklist
- Data Transfer Checklist
- Data Encryption Options
- Transfer Impact Assessment (TIA)

Q1: My understanding of the Schrems II decision is that you can skip most of the steps if you are interacting with the USA since all safeguards, evaluations etc are not sufficient right now. And most likely the next Privacy Shield has slight chances…
https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems
A1: The successor of privacy shield will be invalidated sooner than later, hence SCC + TIA seems the most reliable (and time proof) solution

Q2: is there an example of the processes applied to AWS, Google, or other big suppliers?
A2: Leanne answers there are no examples available in HEAnet, yet. It might be helpful to have examples from actual tenders. Magdalena and Leanne will be in touch to see if these can be provided, (e.g. what OCRE has done) - on how to act in practice with providers that you cannot be totally clear about, and who at the same time cannot easily be removed, as they are crucial to your research or service provision.

Q3: Main issues are with American providers, which are not compliant with European guidance.
A3: If data centre is in Europe, it doesn't matter that the provider is American

Q4: Yes, but American law will still apply to these providers/ the data centres are less than half of the problem - the legal ownership is the major problem.
A4: More guidance from EU is definitely needed: a template, a successor to Privacy Shield

Q5: How to deal with user names on the internet.
A5: use pseudonyms, e.g. random numbers could be a solution

11:00 Five Minutes break (getting a new coffee ;))

11.05 Cloud security checklists for institutions *Slavko Gajin (University of Belgrade, GÉANT Cloud Team)*

List of actions, measures and requirements in order for institutions' Security Managers to assess the risks in Cloud Services and benchmark current status of security, and implement the good security levels, for cloud services but also internal services.

The Cloud security checklist covers several layers:
Physical layer, such as equipment stored on premises. Policies are required on access management (known risks and treatment), controls need to be in place, standards need to be complied to - also in case of removal. You need to know what machines you have (asset management), what data are used/need to be destroyed. In cloud-situations it may be the providers that have the knowledge and

are in control, but in the eyes of the users the institution that offers the (cloud)services is responsible for these things.
Network layer, here the institution is responsible for the network-infrastructure to access the services and must have proper configuration change management re operations and security. Various firewalls and detection must be in place - who can access the services and the data, are there violations, privacy policies, quality measurements.
Application layer, the institution should ensure services are operational , access policies work, provide back-up services, patch management, but also vulnerability testing and penetration checks must be in place - think of encryption, information control policies.
Data layer, for different types (e.g. personal data, research data) the appropriate security measures must be in place

Next to the layers there are other 'vertical' perspectives, such as
Threat modelling, so define what is required re assessment of Risks, Incidents and Business continuity.
Legal and Compliance, so check provision of sound Contracting, Data Location and Data Access.

11.15 Cloud & Security Risk assessments and management *Christian Fötinger (HS Augsburg, Germany)*

Since 2020 an increased usage of Cloud in Bavaria was noticed, loads of working groups were created around the topic of security and data protection in the cloud.
The questions are: what are we allowed to do, in terms of Cloud and Data Protection? What is the risk then? The level of risk? What are the decisions to make - how much of the risk are we willing to take?
There are several points of view to have regarding Cloud: on premises is under control, cloud and managed by others is less under control. Everything can potentially move to the Cloud, data and applications, whole integrated services like in Office 365. We need to be aware that cloud is not one, it is many things: infrastructure, platform and applications.
And in HE we talk about online learning methods, meetings, data storage, Software as a Service/Applications and integrated solutions, all in the cloud. And the more you move to the cloud, the more data and the more integration, the higher the risks, and the more trust you have to build that all is safe: trust in the cloud providers, the IT department and in the controls applied. The risks, especially concerning loss of protection, integrity, control, availability, rights and freedom.
In a table you can plot the kind of threat (e.g. identity theft), the level of such risks per educational use (e.g. webinar, meeting, data storage) to discover the biggest risk to work on.
German ZKI commission wrote a paper on the need to pay more attention to these matters:
https://www.zki.de/fileadmin/user_upload/Downloads/Ergebnisbericht-ZKIKommission_final.pdf

Q1 : All very valuable points, thats why we value data protection so much. How does the protection of this data look in the on-premise situation and are they held to the same standards, given several recent high-profile cases of institutions losing control of such data due to insufficient local IT-Security.

11.25 GEANT data classification sheet for risk assessment *Slavko Gajin (University of Belgrade, GÉANT Cloud Team)*

It is of major importance to understand data, classify data, in order to estimate the risks, low, medium and high, depending on the type of data. The risk is where data assets are under threat and are vulnerable.
Data classes relevant to security are: confidentiality, integrity, accessibility, storage period, storage location, disposal rules, and for each you can define low, medium and high risk. To identify the classes and levels of risk there is a tool, demonstrated in the workshop: an Excel file with a set of questions, and algorithm to map answers with corresponding classes.

The GÉANT Data Classification Tool information: https://clouds.geant.org/data-classification-for-cloud-services/

11:35 **Example licensing Microsoft M365 risk assessment** *Denise Dittrich (RWTH Aachen University, Germany)*

Risk assessment on one particular use case: the example is about licensing of Microsoft365, so not assessing the usage of M365. When doing a risk assessment the questions to deal with were: Which data are transferred? What are the risks inducted by using Cloud-managed licences? It proved hard to identity data transferred. One type was the data transferred to the cloud by us (for authentication) and the other type was data collected by Microsoft during the licensing process. Based on a list with cloud related risks fo0rm Bavaria University (Christian Foettinger) risks were explored using a Scale of 'Impact' versus 'Probability of occurrence' and identified as Low, Medium or High. The process steps taken are (1) identify risk + sources of risk, (2) assess impact/damage (3) calculate the initial score; (4) define measures, and (5) after application and refinement of the measures, calculate the final score.
Two example wer used to demonstrate the steps: identify theft due to a hacker attack; data access by 3rd parties.

Measures that were identified to lower risks: organisational (have data processing contracts in place, as well as support contract (to minimise the impact); and technical (minimise amount of transferred data, have back-ups in place, look at redundancies, pay attention to configuration sets, use local authentication methods and 2 FA).

The hardest part in the whole approach was to assess scores, it felt like guessing. We needed to get them verified. Benefit of the exercise is that all risks are visible, for all to see, even if in the end we did not end with any High risks. It will end indecisive discussions. The plan is now to do another risk assessment for Office 365 applications (e.g. Teams).

Q1: How to make the difference between risk assessment of services processing data and applications - that may comprise multiple services and data sources?
A1: Combine them. It's about data, but also about the process in which this data is used. Perhaps the risk assessment can help to identify what risk is increased by using some data.

Q2: Input from practitioners is very valuable. Risk of putting data and applications into the cloud. Did you evaluate the risk of NOT putting data and apps into the cloud? Potential situation where you chose for a smaller legal risk and not using more data that would cause this
A2: We assess only additional risks, I'm not talking about the risks which are already there. We indeed need to mitigate risks, and look at the full scope. But it is more practical for every step towards the cloud to look at the difference, the additional risks - to keep things manageable. Going into the cloud, we have protection in place, and it means we trust the provider, and have taken measures to do so. From that starting point we look in detail - what happens when we do a specific thing.

Q3: Do you know about institutions having legal issues for security risks? As it seems the providers are highly certified, do the local implementations and on premise infrastructure present a legal risk to the institutions?
A3: The increase of breaches within the universities, that become more and more visible, change the question from 'if' to 'when' and 'at what impact'. There is indeed an increasing pressure on institutions

Q3: What about the other risks? Like cyberattacks, storage, dataware, cloud, infrastructure - we are all in danger. We do need to use all the tools available, and need to share our concerns and solutions, and mitigate risk..

A3: That is all agreed. However, the issue with GRPR right now does not take risk into account (for privacy/security in the cloud); therefore t is difficult to balance risk of local data breaches vs legal issues on using cloud providers.

11.45 Cloud & Security Risk, Q&A, poll on Future topics (menti.com 8221 4268) *(all)*

Have you done a risk assessment concerning a cloud service before?

- Endpoint protection (advance it or not). How far shall we go?

Due to lack of time this online poll will be changed to an online survey.

---- Close --

11.55 Wrap-up and close (incl. Zoom exit poll)

We've addressed changes in the Schrems 2 and other GDPR regulations, and how to go about these in a Cloud environment. In the second part of the workshop we shifted our attention to checklists on various security and privacy aspects - ways to classify data and t]risks, as well as tools and approaches were presented and demonstrated. We hope the rich offering compensated for - perhaps - not enough discussion and interaction.

The exit poll: 32 votes: 15 votes (47%): very good; 17 votes (53%): good.

In about two weeks we will put a link to all slides and a report on the workshop on the EUNIS and GEANT websites. Thanks for your interest and openness.

12.00 End of Workshop