Notes on 2 hours EUNIS workshop

‘Data Protection and Cloud Services’

Organised by: SIG Information Security and GDPR
Date and time: Tuesday 27/10 14.00-16.00 CET
Attendees: 28
Introductory talk: Andrew Cormack - Chief Regulatory Adviser, Jisc, UK

Introductory talk ’2020 Hindsight: Clouds and the New Normal’
Slides: https://www.eunis.org/wp-content/uploads/2020/11/EUNIS-Infosec-Data-Protection-and-CLoud-Security-Andrew-Cormack-1.pdf

In his talk, Andrew Cormack addressed:

‘Schrems II’ about Facebook sending European data back and forth between Ireland and the US. The European Court of Justice found that US laws do not provide adequate protection for EU data subjects (at company level), Also Privacy Shield agreements (at government level) were rejected by the ECJ because of inadequate protection for exported data. There are Standard Contract Clauses for import/export but the importing government can overrule these. So if protection is needed, *maybe* this can be provided by technology (encryption), laws in the importing country (e.g. FERPA law in the US on education), *or* keep the data physically within Europe (in a data center).

‘European Data Protection Supervisor - Microsoft Report’ about issues with Cloud contracts - do roles (e.g. data processor / data controller) in the contract indeed match how the responsibilities look like in practice, as this defines if GDPR can be applied; are *all* data flows covered (e.g. data storage locations, telemetry data) as these need to be protected as well;can 3rd party audits take place and is transparency ensured?. Be aware not all contracts are the same and check thoroughly.

‘Covid-19 emergency and opportunity’ about the pros of rapid adoption of new cloud services (KluwerLaw stated) that made us continue with education, and the risks of Data Protection and IPR issues unsolved. In the near future we’ll need to check this thoroughly. Also Covid-19 (Gartner stated) sped up anticipated developments by about 5 years. So we need to decide what new processes/tools we do wish to keep, to get rid of, in a shorter time scale than expected.

‘In summary’
It is uncertain how/when the uncertainties following Schrems II will be resolved; as for cloud contracts and procurement: be realistic. Currently using the EDPS report as a checklist is the best option, as is talking to your provider - do not ask for GDPR compliance as it is unclear what that is. Comparative risk assessment between inhouse and optional cloud providers is key.

'Round of questions'
Andrew confirms that remote services count as data transfer to which these rules and laws apply. He also indicates that European regulators, and European law, are tending towards even stronger national security exemptions, with the risk of trade wars.

Discussions on Rapid Response tools and Privacy Shield developments

Q1: The winners in Covid-19 circumstances
Not surprisingly attendees voted conference tools (Zoom, Teams, Kaltura) as big winners to overcome Covid-19 drawbacks. Also mentioned were VPN solutions, and on-line education solutions such as Moodle and Panopta. Andrew commented that 'Acceptance of remote working' is probably the greatest win. Zoom's popularity may be due to its pan-European wide Geant licence agreement. Looking at these tools from a security perspective, an advice might be to not to use centralised tools for sensitive meetings, in some cases on premise may be available.

Q2: The tools/services you would like to get rid of?
Entries for: 'Teams' that it is 'too buggy'; 'Pexip' that is too slow; 'less managed Home Office laptops'. Getting remote assistance is also hard, as IT departments are overburdened and the equipment at home (e.g. small screens) is not always suitable for full day online working. Reduction of multiple decentralised solutions and use of centralised ones is advocated, and the worry for tools that collide with Schrems II is mentioned.

Google Analytics sending data to the US is flagged - in some countries the use is therefore seen as not law compliant, but enforcement is not a priority (yet). It is noteworthy that research indicates that targeting advertisements based on individual user data profiles is not more effective than advertisements based on the content of the page - the business model of analytics challenged!

Zoom's effort to increase security, e.g. its end-to-end encryption is valued by participants. [Martin Nelder shares a Zoomtopia link on these matters. Be aware you cannot use Zoom's end-to-end encryption and at the same time use Zoom on premise.
One entry states it is not about getting rid of, but about creating a balanced portfolio of commercial and open source (conference) software.

Q3:' Responses (users, regulators, to the end of the Privacy Shield'
Many answers indicate confusion, denial, a pause in decisions and postponement of implementing new services that entail a risk, avoiding US services. Users are doubtful and some have become more reluctant to use cloud services. Some entries state that local protection authorities published guidelines, e.g. to stop 'doubtful' services, get an overview of the complete supply chain, make assessment and implement additional measures,

There is no entry mentioning research, which Andrew agrees is a sore point. One reason is that research has always been left-out to sort things out on their own. Probably a first initiative (e.g. the UK agreeing with a European country) could get things moving quickly. A missing alternative or response could also be 'hosting in Europe', so no Privacy Shield considerations necessary.

Opinions of researchers themselves are scarcely available, however the EU may require measures for new projects. Andrew suggests its best to map out any service that is tied to an American, and after December also English, companies and assess risks and possible solutions. Martin Nelder and Andrew Cormack have mixed expectations about how soon solutions will be found.

Sharing Experiences

Agnethe Sidselrud: We have started, as our regulator advised, getting an overview of all systems and services provided by UNIT and UNINET (the internet service provider for the HE sector in Norway). For actual assessment we wait for more guidance from the Norwegian authority about additional measures that can be relevant the European Protection group is working on. It is hard to imagine what those will be as they will have to be suited to pass by the national surveillance laws, including these of the US.The Norwegian data protection authority is very strict but has indicated that in the current situation they will not yet act upon breaches, because all European countries are in the same position, waiting for the European Court of Justice. Establishing the overview is an excellent opportunity to tidy up documentation, update the contracts.
Andrew refers to an audit of the Department for Education in the UK, target shows the current situation is no good. He also shares information on the Wellcome Trust Wellbeing Code.

Martin Nelder: indicates that in the various Länder (singular Lands within) Germany the relationship with data protection authorities is not as good as in Norway - so he is not hoping for guidance, rather hopes they will do nothing so universities can do the job. An example is that doing online exams has proven very hard to conduct.
Andrew admits that giving advice is impossible but we can look at law and how that fits to what is being done, come up with plausible stories to the authorities and try to bring both sides together - and over a longer time this can lead to agreed codes of practice.

Thorsten Küfer refers to Münster University now creating the GDPR documentation and ince that is done assess where the data are going.

Przemysław Baszkiewicz, who himself is not deeply into cloud computing, indicates that many services in the University of Warsaw are on premise, although Google services are being used.

Risto Rahu of Tartu University tells that they are using cloud services mainly for email, and Microsoft Teams. They are aware of the issues and listen carefully today, as these are not sorted yet. And nobody wants an IT department to not do things- there is pressure to offer good solutions for remote working and collaboration.

Risto also refers to proctoring software, where you need to remotely control students computers that are located in a student home - data-wise that is more complicated than dealing with their data in a student classroom. In the software contracts they see standard privacy shield references replaced by specific clauses regarding this type of use.
Andrew comments that it is a hopeful sign that vendors do try to respond to the lack of clarity. The location of data in a European data center is also no guarantee for data security - if 24/7 services are offered, part of the services to data will be performed from outside the European time zone. Andrew comments that with GDPR became the rule, a number of examples that had been accepted by the regulators when self-assessment was the way, were unclear again. We might, in the common view that the current situation is a mess, again formulate example situations and get a regulator OK.

Wrap-up and close

We should have our documentation ready, know where our data are located and processed. We should wait for the authorities, and perhaps jointly look at these in half a year, possibly at the EUNIS 2021 conference. By the way there are authorities that immediately responded and said ‘do not use SCCs’ or ‘don't use Microsoft 365 anymore’. A general tendency is the push to use more Open Source tools.

Next week we’ll run another 2 hour workshop on How To Make Cloud Services Secure, with speaker Jeroen Vandeleur, NVISO, Belgium.

Other topics we could address:

Kari Kataja, from HAMK (Finland) would like to contribute to a workshop about privacy issues,sharing a big case form Finland health care: Hackers hijack and publish mental health data of hundreds of people *Christian Foetinger* shares a link on the privacy topic as well: https://streaming.privacyweek.at/. *Andrew Cormack shares a link on pseudonymisation. Asbjorn Thorsen,* earlier flagged the topic of digging deeper into Microsoft 365 security issues.

Q4: Why was attending the workshop worthwhile?
Participants rate the workshop very positive. Sharing issues and experiences on challenges we all share is appreciated, as well as presenting legal issues in an easy-as-possible way. Comparing country situations is very interesting and helpful.

Q5: How can the next workshop be improved?

- Provide coffee or pizza :-)
- Request to have a Calendar invite directly placed after registration. EUNIS currently uses the standard Zoom registration functionality. Bas will check.
- Request to by default turn cameras on, another one asked to ensure each participant was at least heard speaking once - do an introduction.
- Suggestion to have regular sessions, monthly, for a chat/exchange without a particular topic.(we will plan some 2 monthly meetings).
- The topic BI and security/privacy is coined.
- Request for required GDPR compliant registration to EUNIS workshops.
- Consider break-out sessions (we will definitely!)

Q6: Would you prefer a chat tool to communicate within the SIG ?
Results are: Yes: 2 / We could try: 5 / In doubt: 4 / No need: 2

On this basis we will explore options for IRC, Signal or DeltaChat which do not require a specific infrastructure. We'll also check the views of the audience in the upcoming workshop.

End of notes
