Workshop – Data Protection within International Organisations

17 June 2019

Gabriela Ramos (OECD – Chief of Staff): Introduction

- We have been working on digital transformation
- People engage with these technologies, but have the right to know how the data is used
- One of the first IOs where members agreed on a recommendation on AI
- Privacy is a key concern for people: based on a 2017 survey, 70% people gave data online and asked for access to such data. In 2017, 46% of all Internet users refused to allow the use of personal information for advertising purposes. More than 1/3 users read privacy statements.
- 2018 EU data protection reform: often complained about as too much, but then how much is too much when we see scandals like Cambridge Analytica?
- 2013 OECD Guidelines → now new regime applying to any individual whose data is processed. OECD has a system of data collection about tax – huge amount of data. Robust governance framework. Getting the new regime established was a huge step. In addition, awareness raising projects.

Giovanni Buttarelli – video message

- Share knowledge and experience with one another
- The position of IOs is not an easy one. Development of specific privacy measures despite the lack of a dedicated data protection framework. Take inspiration from the GDPR.

Session 2 – Use of social media

Moderator: Often questions on cookie banners etc. [redacted] reviewed the cookie policy which was a very complex exercise. We are starting a revision of the privacy policy. An assessment of the risks is necessary.

Panelist n. 1 ([redacted]:

- **use of social media to engage with beneficiaries**. Many open questions.
- Two examples. In 2016, the [redacted] in Syria decided to double the amount of food because the security situation forced them to reduce the frequency of the food distribution. We informed our beneficiaries through a short video on Facebook: it was viewed by many people, who also made comments and asked questions, to which we could answer. Another example concerns the use of a system in Kenya allowing to identify where accidents take place so that ambulances can go there.
- These examples seem to be useful, but from a data protection perspective there are a few issues. What kind of data are being generated and processed when we engage with beneficiaries? Not just the "disclosed" data but also the **"inferred" data**, created e.g. by Facebook. Facebook creates what is called a "shadow profile" of the user, which includes what the user posts as well as metadata and information about the user's behaviour. Through our use, **we may be incentivising beneficiaries to provide even more data: would**

this put them in danger? (e.g. links with opposition groups; other information that could be dangerous in a conflict situation).

- We have also been thinking in terms of **data flows and data transfers**: the platforms share data with partners not only for advertising purposes, but also for "surveillance", performed by governments as well as by groups. By using these social media, are we exposing our beneficiaries more? **Are we increasing our beneficiaries' presence on these platforms and somehow contributing to the exploitment of their data?** What could we do to ensure that people are informed / that providers do not use the data for purposes other than humanitarian action?
- Also, **who is the controller? CJEU decision on joint controllership** of fan page administrators. Therefore, can the IO administering a fan page be a joint controller as it takes part in the definition of the purposes and means? Is this interpretation specific to the EU and GDPR or can it be applied to IOs as well? Would we be liable when data is processed for purposes that are not related to humanitarian action?
- **Right to information** of the data subject
- Importance of **DPIAs** that should be carried out before any processing operation. We should **go beyond data protection: other rights might be affected** by the use of these platforms (ethical / social aspects). E.g. Facebook might influenced the course of conflicts / situations of violence.
- **Knowledge gap** (we do not know what risks we are creating) + **data literacy gap** + **ethical gap** (**how can we say that our mantra is "do no harm" if we start using tools we don't really master?**) + **financial gap** (some small IOs cannot find the answers, so the big ones have a duty to take the lead, find solutions, and put some pressure on platforms to change things for the better).

Panelist n. 2 (EDPS):

- It is not just a matter of compliance with a specific legal framework, but rather a matter of **trust**. Reputational issues
- Visitors should be provided:
    - Information about data processing
    - Information about cookies and similar technologies
    - Meaningful methods to accept and reject cookies
    - Safe transmission channels and servers
- **Trackers**: can track users not only while they are on the websites but also afterwards. We should prevent unconsented tracking and profiling of website visitors. The ecosystem is meant to share data. We should be responsible for our own website.
- **Cookie based tracking**: when a user accesses a website, he could receive one or more cookies. Afterwards, every time a resource from the same provider is embedded in a webpage visited by the user, this can be registered.
- **Web beacons and tracking**:
    - **Google Analytics** cookies are stored under your domain but they are third party cookies. A little transparent picture embedded in the website. Google Analytics is very good, it's free, but they use that information to send behavioural advertising. The visitors of your websites are subject to this processing if you use Google Analytics.
    - **DoubleClick:** ad company owned by Google. DC trackers are often set by other services (e.g. YouTube).

    - **YouTube:** embedded YT videos downoad cookies on visitor’s devices (by default!) and 2 of them contain identifiers. There is a “privacy enhanced mode” but even that one stores a device identifier (in Local Storage).
    - **AddThis:** a tool to facilitate online content sharing with social netwroks. It tracks your visitors (online behavioral advertising).
    - **NID:** used for advertisement and profiling
- **Security in transit:**
    - **Data transmitted over a non-secured chanel (http) is available to other users sharing the network**
    - Data transmitted over an encrypted channel (https / tls) is accessible just to the sender and the recipient.
- **Tip: avoid embedding YouTube video**: this way, the visitor will be affected only if he purposefully visits YouTube and not when he only visits your website
- Diamonds are forever, but security measures and standards are not ☺ You need to update and upgrade your systems.
- **Steps to success**
    - 1. Minimize personal data procssed by websites.
    - 2. Draft an inventory of third-party components, analyse their privacy impact and get rid of those endangering visitors’privacy
    - 3. Keep users in control
    - 4. Avoid vistors tracking!
    - 5. Ensure all connections to web servies are encrypted
    - 6. Conduct regular vulnerability assessments on your servers
    - 7. Monitor changes in the terms of use of third-party service providers.

Panelist n. 3 (EDPS):

- How have we got to this situation? Let’s zoom out. “Back to the future”: why is there tracking on everyone’s website?
- Through the WaybackMachine, we can see the Oxfam website in 1998. It is very simple. There was 1 cookie to store the language preference of the visitor. There were just 40 files with about 0.1 MB in total. No other tracking. There were about 825 lines of code (which gives an idea of the complexity). In 2008, we can see that about 68 files were used (about 1.2 MB); 3 cookies, of which 2 are behavioural tracking (probably Google Analytics); 2 resources from third-party hosts; about 11.000 lines of code (massive increase in complexity). Current website (2019): 66 files (3.7 MB in total); about 60 cookies; numerous behavioural tracking of website visitors; 16 resources from third-party hosts; 119.000 lines of code. The website complexity has massively increased.
- But does this correspond to an increase in web staff? Not really: it is possible to have such a complex program because most work is outsourced to commercial providers, offering very sophisticated products.
- Web serice add-ons market is often dominated by winner-takes-it-all, becuse there are zero marginal costs for software offerings. They can update their product much better because everyone uses it. Lack of competition → providers can decided on the terms of services for everyone.
- Establishing alternatives to the champions is hard. But there are some open souce alternatives.
- Demonstration of tools to inspect websites.

Moderator: **a first step could be transparency as to the third party cookies that are used. Then we should also encourage users to read: how can we do this? How can we keep users in control? →** having effective banner? But what if something is triggered even before someone can click accept. **People in the digital engagement team are worried that a cumbersome banner might result in less people visiting the website, which can be damaging as most of the funds come from private contributions**.

Panelist n. 2 (EDPS): if you want to be transparent, you should say everything, whereas "enhancing your experience" is not a transparent way of communicating. You should block all cookies until the user has consented. Users expect you to be privacy-friendly. There should be some options in the cookie banner. Then you should also think of replacing some cookies with less intrusive ones.

Panelist n.3 (EDPS): I doubt that most IOs really rely on the sophisticated tools offered by Google Analytics. The tools that are actually used can also be provided by other privacy friendly providers. Some analysis of the websites can be performed. Also, some "old style" tools could be used again e.g. mailing lists.

Audience ([redacted]: I deal with beneficiaries' data. I doubt we will find a way to properly explain everything to data subjects. **We are experts, yet we struggle to understand. I am really questioning our ability to enforce and provide the right to be informed**. We deal with particularly vulnerable categories so it's even more sensitive.

Audience ([redacted]: interesting yet alarming presentation. Am I correct in assuming that when I am tracked the recipient of the information about me only knows about my IP address, and not my name?

Panelist n. 2 (EDPS): they know a unique identifier that will stick with you for as long as they want. Android smartphones also make the link between your identity and your IP address. Also, your previous activity is linked with the activity on social media so your identity comes out.

Audience ([redacted]: if you turn on "block everything" and use a safe browser, what risks still remain?

Panelist n. 3 (EDPS): while the tools to block everything become more sophisticated, so do the trackers. There is no 100%, but it's the best we can do at the moment.

Audience ([redacted]: often we cannot trust the open souce tools; the more powerful tools were chosen for a reason. More of a managerial issue? Also, my expectation as a user have changed: I expect to be tracked and I expect Google to know what I am doing, as I feel that I have no say.

Panelist n. 2 (EDPS): However, you can look more attentively at the tools that are currently employed, and see if some can actually be replaced; we should not only look at how hard it is to change something you know. Also, it is not true that big providers are always more reliable than open source tools.

Panelist n. 3 (EDPS): A challenge could be taken to push things to the limit. E.g. a game: one cookie less per month ☺

Audience: what is the long term and serious impact of this? E.g. I don't get a loan. What is the real risk?

Panelist n. 1 ([redacted]: e.g. unanticipated transfers. There are many direct impacts. Only through thorough DPIAs you can identify them.

Panelist n. 2 (EDPS): It's not just selling things, it's really selling ideas! The impact is also increased by the collection of a lot of data over a long period of time.

Audience ([redacted]: I do not think I will be able to bring change individually. There should be a recommnedation from the HRCM (?), initiated by the UN Global Pulse. A common, institutional approach should be adopted. Individual lawyers in IOs cannot change everything.

Moderator: thanks! Let's focus on vulnerable categories that are using social media platforms. Beneficiaries need information, let's try to implement their rights at least to a certain extent. Let's speak to Facebook through a common channel so that engagement with beneficiaries can be done based on ethical principles (so that the data of beneficiaries are not monetized!).

Session 1 – Tour de Table

Moderator: the 2018 was important: GDPR + Convention 108+. New data protection rules have been adopted. C108+ is the only binding international treaty on data protection.

Participant ([redacted]: we upgraded our practices. We abandoned pre-approval model. We are trying to instill a different culture within the organisation. DPO and DPC do not pre-approve things, but block things if they are particularly risky: this is the new governance regime.

Participant ([redacted]: we don't have a data protection policy yet, because now our leaders want a broader data policy. However, we concretely apply what we have developed so far. We received 4 RTBF requests, 3 of which were refused and 1 of which was entertained.

Participant ([redacted]: we have had a DP policy since 2008 and we are updating it: we strongly cooperate with the CoE even if we are fully independent. Although we are a IO, we decided to use GDPR as a standard for our internal processes and use the tools provided by national DPAs. E.g. identification of personal data + risk assessment. Now we'd like to lower the risks we identified. We are also updating privacy notices.

Participant ([redacted]: increased our efforts in training our members around the world. We are working on sensitizing our counterpart on the status of IOs and on the fact that we are able to protect personal data although we are IOs(!). Raise awareness on our DP policy and status.

Participant: development of data management framework + data mapping exercise. Also, focus on digital ethics also in the context of big data. High level expert group.

Participant ([redacted]: new compliance function. We will be writing records of processing activities. We will look at GDPR as well as other very important regulations from Brazil, India, etc. in order to match the whole view and not just the European one. I work very closely with other organisations. I am using my experience in the private sector to design a new program.

Participant ([redacted]: same group as the World Bank. Struggling with authentication issue, with inventory. There is a multilateral development bank privacy forum (next event in October).

Participant ([redacted]: Data protection regulation since 2006, with DPO. 3 people working on DP.

Participant ([redacted]: two institutional developments. (a) Mapping exercise, (b) functional review. Outside of the data that the organisation itself is processing, there is also data held by allies, that could be exchanged. A policy was adopted regarding biometric data.

Participant ([redacted]: we developed a manual on beneficiaries' data protection in 2017, followed by an even more practical document providing help to our country offices. We have been testing the PIA tool that we have developed, and some countries have engaged in this exercise, which also involves inquiring into data subjects' views. We are trying to establish links with our regular risk assessment. Also, we have been trying to come up with tools to explain our beneficiaries which data we collect and what we want to do: this is a real challenge. The collection of consent is also something we are working on, although when people are in need it can be hard. On the legal side, we reviewed the contractual architecture and changed some definitions, which also helps colleagues to understand. As to tech developments, we have digitalised consent, developed cyber assessment tools for our technical providers, we are testing a self service tools for beneficiaries. Also, GDPR self assessment.

Participant ([redacted]: development of tools; negotiation of contracts; we have a standard partnership agreements and developed a DP annex. (....) Applying standards similar to GDPR. Happy to exchange practices regarding fund-raising activities. Important to liaise with national DPAs. We will participate in the International Conference.

Participant ([redacted]: adopted internal data protection rules applying to any person whose data is processed by us. Training exercise with e-learning and classroom courses.

Participant ([redacted]: long history of DP guidelines (since 1992, revised 2014) + now trying to update based on GDPR and Regulation 2018/1725.

Participant ([redacted]: working on medical procedure since 2 years + medical confidentiality policy. Additional guidelines issued. Medical data stored only on physical storages.

Participant ([redacted]): increase of DP awareness of staff > Mandatory data protection courses for all staff. Privacy by design in procurement requirements. Safeguards.

Participant ([redacted]: just published our policy on personal data, regarding any type of personal data. Raising awareness. Different regional offices have very different interpretation though. Updated all standard contracts adding data protection clauses.

Participant ([redacted]: relatively new institution but we do have DP policy, which we are updating. Records of data processing operations: ongoing work. Initial training will be face to face.

Participant ([redacted]: we have medical data + scientific medical data + technology data. All kinds of innovation tools and devices. 9 locations. 5k employees. DP framework + appointed supervisory authority (indept body). Privacy by design on new tools. Struggling w email policy. Struggling with how to get right clauses in the contracts with big players.

Participant ([redacted]: complex issue = handling DP activities relating to events held outside of our facilities. With respect to major providers, really hard to negotiate clauses.

Participant ([redacted]: no DPO, up to Legal Dept. Financing entity for medical services around the world. We don't process medical data but our implementing agencies (governments, others) need to report to us as to effecitveness of our investment. We are thinking about what kind of clauses we need to negotiate. We have recently put in place due diligence technologies. Training sessions, but not yet mandatory for all staff.

WW: conclusion, let's exchange experiences.

18 June 2019

Session 3 – Contractual arrangements

WW: introduction; the EDPS started investigation on MS.

Panelist 1 ([redacted]: our experience on contracts with software providers.

- We need to make a distinction between software run "in-house" and software as a service (SaaS), which raises the issue of sharing personal data with a third party. The policy we generally apply is: we only transfer personal data only if the third party affords appropriate protection for the personal data. This is evaluated through a risk assessment conducted during the selection process. The standard contractual provisions we use can be extremely strict (e.g. asking for background check / screening for all employees), and some of them can sometimes be negotiated.
- Sometimes we turned to resellers when providers were not open to negotiating
- The provider may have several reactions: (1) full and spontaneous acceptance; (2) reluctance; (3) full refusal.
- Even scenario n. 1 can trigger compliance problems: has the provider realised the full scope of the obligations? Often, it hasn't: however, although non-compliance is a ground for terminating the contract, this might not be the preferred outcome.
- Scenario n. 3: the provider does not even wish to enter any discussion or negotiation. Often, this is the case when the contract is for free or has a very low value, or when the provider is so strong and has such a leading position that he is not open to negotiating anything. This leads to looking for another supplier.
- In scenario n. 2, we try to negotiate terms with the supplier, unless the reluctance refers to conditions that are essential.
- The most important issue refers to privileges and immunities: we want to make sure data are stored in a place where we enjoy P&I. Therefore, we needto take into account the country in which the provider is based and the country in which the data is stored, as well as the country in which the backup is stored. There are only 50 countries where we enjoy P&I. In our original clause, we used to ask the provider to disregard any request from authorities and court orders, but this was not realistic. Now we ask them to disclose the existence of the request to us (to our IO), prior to any disclosure to authorities, so that we can assert P&I. However, this is a very theoretical issue. Only ¼ of our contract is SaaS: it is however significant enough to identify a global trend; we have never been confronted with requests to disclose data so far.
- Issue of segregation of our data in dedicated servers. We used to try to ask providers to do so, but now we mostly gave up on this.

Panelist 2 ([redacted]:

- We are the procurement department, this is not the opinion of our supervisory authority.
- We started speaking to MS but they thought we were too small.
- Strategic dependance and vendor lock-in
  - Generally good quality products
  - Users enjoy working with them
  - Competition is scarce → vendor lock-in: organisations must continue to meet the requirements and conditions set by the vendor. Also, vendors push organisations to purchase more and more functionalities: this raises the barriers to market entry for competitors or innovative European start-ups even further.

- Very difficult to influence a situational monopolist like Microsoft to change the way it offers services to meet national rules and maintain data sovereignty. Some vendors store little pieces of data scattered all over the world, which may be secure but might not be desirable from a sovereignty point of view. Also, migrating or including cloud services is often part of the upgrade of IT infrastructures undertaken by public institutions.
- DPIA results: data provided by and about users was being gathered through Windows 10 Enterprise and Microsoft Office, and stored in the US in a way that can pose a high risk to users' privacy.
    - Lack of transparency
    - No possiblity to influence the collection of diagnostic data
    - Unlawful storage of sensitive data both in metadata and content (eg subject lines of emails)
    - Incorrect qualification of MS as processor instaed of joint controller
    - Not enough control over subprocessors
    - Lack of purpose limitation, both for processing of historically connected diagnostic data and possibility to dynamically add new events.
    - Transfer of diagnostic data otustde the EEA; basis was shaky.
    - Indefinite retention preriod of diagnostic data + no tool to delete historical diagnostic data
- Agreement was reached regarding an improvement plan + MS promised to provide adequate information including a data viewer tool for the telemetry data
- June 2019: MS has improved and corrected some products. The improvements included
    - Purpose limitation: we agreed in contract that collected data can only be prcessed to provide the service contracted and keep the service up-to-date and safe. → MS cannot use the data for profiling, data analysis, training AI.
- NB: product changes became available for everyone VS contractual changes became only available for the Dutch Ministry.
- BUT
    - Product changes: only for customers with a so-called enterprise agreement in organisations with 500 users or more
    - Required contract changes: only available to participants in Dutch Central Government Contract.
    - MS requires every organisation worldwide to enter into individual conversations on their concerns and may address these. This is very long, burdensome and costly and cannot be done by many organisation.
- Strategy:
    - We need to get the improved contract available to all and apply the concepts to all hyperscalers. We need to work together. The only way is cooperation with organisations to pool resources.
    - Initial interest and support from several EU member states + EDPS.

WW (EDPS):

- The EC has negotiated a similar agmt with MS (framework contract for EUIs). EDPS raised some doubts about the contract.
- The DPIA made by the Dutch Gov't is convincing (and the underlying facts were confirmed by MS).
- You're welcome to contact the EDPS.

Participant: how can you negotiate with resellers instead of providers? If you ask them to have awareness sessions for example, those need to be done by the software provider and not by the reseller.

Participant: did any provider inform you of requests from authorities?

Participant: P&I pose a theoretical question → has anyone been faced with requests from authorities?

Participant: we do have experience with requests from government (Syrian government). Another participant: we prevailed when some of our data was requested by authorities to one of our contractors.

Panelist: clauses that are non-negotiable correspond to the provisions of GDPR regarding transfers to third party (e.g. not use data for any other purpose…).

Session 4 – Personal data transfers to IOs

Moderator: this topic has been gaining increasing attention.

Panelist ([redacted]: [redacted]project ([redacted]) and int'l data transfers.

- Actors:
    - There is a governing board
    - the work is overseen by the IO, which also analyses the data
    - the international contractors (mostly American; they are not Microsoft, etc. but they are large players in their field) organise the data collection and prepare the dataset
    - national centres: they collect the data in schools in their own country
- Student information are initially kept locally by the contractor, then it is transferred to the IO. Most countries do not share the specific list of schools and students but just an ID. Steps:
    - 1. National centres provide school info to contractor
        - Each student has an ID number + a name + a school + results of the test
        - Countries transfer only the ID numbers + the results (pseudonymised data).
        - The raw data are kept locally and are deleted before the publishing of the report. It's kept because there might be a need to check some things.
    - 2. Conractor administers test and creates data base
    - 3. IO analyses results and publishes report
- In 2018 the contract between IO and contractors was amended → the contrators agreed that the processing and transfer will be carried out in accordance with the IO principles, and provided assurance to participants subject to GDPR (…).
- Unresolved questions:
    - Transfer to contractors: contract amendments are insufficient; shall we envisage SCCs agmts between countries and contractors? Those data transfers would be covered. But not very elegant; not all EU countries would be able to do it; etc.
    - Transfer to IO: insufficient legal framework for allowing IO to receive data. Countries will still have the identified data. Public interest derogation? EU countries we spoke to told us they are not in the position to assess whether this works under the GDPR.
- Are there other solutions?

- Moderator: who are these contractors?
- Panelist: they can change from a cycle to another; there's a tender process; the ones we have now are US companies and are relatively big in the education assessment field. One of them is a non-for-profit and one is a for-profit company.
- Participant: who decided that your IO does not afford an adequate level of protection?
  - Panelist: no EU country has flagged issues on how we process data. It's not a technical question but a legal question.
- Participant: who would seek the derogation? Would it be requested by the IO / the country / the contractor?
  - Panelist: it's something to be decided by each country.
- Moderator: have concerns been raised by non-EU countries? > no.

Panelist ([redacted]:

- important to keep in mind that
  - the transfer between national countries and contractors is subject to the GDPR;
  - the transfer between the contractor and the OECD is not subject to the GDPR.
- The rules on international transfers have not been deeply changed under the GDPR as all the previous possibilities are stil in place.
- IOs are not per se subject to the GDPR. But entities transfering data to IOs are subject to the GDPR. When IOs collect personal data from an individual, this does not fall within the GDPR.
- Description of rules on data transfers under the GDPR.
  - Adequacy findings: so far only for countries.
  - SCCs
  - Tailor-made clauses: contracts / non-binding administrative arrangements (examples: The OLAF has used a model administrative arrangement that they agreed with many IOs; ESMA agreement). No need to copy-paste GDPR, need a core set of safeguards.
  - Statutory grounds (derogations): should be used for specific situations and not for systematic cooperation.

Moderator: will [redacted] issue some statement on this point to provide some clarity? When should we expect some public clarification? Some of your legal conclusions are open to challenge

Panelist ([redacted]: the DPAs are best placed to provide guidance. I don't know if EC will issue public statement. We have tried to engage with member states. We are working with them as much as possible.

Participant: I know of ongoing discussion between UN and EC, are there updates?

Panelist: still ongoing – several exchanges – the main update is the outreach we have been doing.

Participant: planned adequacy decision for IOs?

Panelist: the GDPR provides for this possibility, so we are open to explore that, but the adequacy assessment is very thorough, it takes time and some specificity of IOs may make it harder (e.g. independent oversight, redress mechanisms). It depends on specific situations.

Panelist n. 3:

- [redacted] established as a member of he ESFS

- Exchange of data between supervisors: needed for market manipulation investigation, for example, and in general to comply with our mandate.
- Previous transfers were based on non-binding Memorandum of Understanding. BUT The public derogation was declared to not be a viable option by European DPAs. So there was a shit from the public interest derogation to a multilateral Cooperation Arrangement.
- The work led to Administrative Arrangement for the transfer of personal data between EEA Authorities and non-EEA Authorities.
    - We managed to convey the message that data protection is a value to be treasured.
    - Transparency: it was a key challenge because enforcement actions require confidentiality. All signatories published a general privacy notice; etc.
    - Effective redress: top-up approach.
    - Oversight mechanism

Participant: questions – data subjects who don't access grievance procedure within IOs – can we expand DPO powers? What's a real practical equivalent of independent authority?

Panelist: could be that IO already has an inspection authority that is independent.

Participant: Using public interest for transfers: when a derogation is chosen, is this enough? Or do we still need to still sign an extra data protection annex, e.g. for onward transfers as per art. 44?

Panelist: the difference between derogations and the appropriate safeguards is precisely this. If all the conditions for using a derogation are fulfilled, there is no need to have other safeguards in place. But the GDPR might require a contract anyways (e.g. processors).

Participant: Regulation 2018/1725 – has the EDPS taken a position on transfers?

Panelist: we don't plan to create a special different way to transfer to IOs and third countries for EUIs. Chapter V of Reg 2018/1725 looks a lot like the GDPR. Some EUIs have a different regime (e.g. Europol transfers data based on ER). We didn't prepare any further guidance.

EDPB will publish guidelines on transfer between public authorities (art. 46).

Moderator: "important grounds of public interest" / "reasons of substantial public interest" / "important reasons of public interest" → the GDPR includes all these

Participant: if IO is the controller (…)?

Panelist: IO acting as a controller, using a processor subject to GDPR, does not bring the IO under the GDPR, but processor remains subject to GDPR.

Participant: we need guidance on how the IOs can apply all this. We are worried. Can the DPO or inspector general be really independent enough? They have a contract with the IO so how can they?

Panelist: an oversight mechanism is not always required, but when we want to rely on adequate safeguards there should be some form of it.

EDPS: Hard to imagine that EDPB / EDPS / EC will give guidance. The farthest we can go is to provide facilities and space. Among us, there are IOs whose supervisory authority has been recognised as qualified enough to be members of the International Conference. There won't be guidelines from EUIs because it's outside of our remit but there are good examples

Participant: we are working in an Expert Group in the EC – what is "public good"? What is "public interest"? Some of the qualifications of what is public interest are being taken from the SDGs (?). To qualify what kind of safeguards need to be applied (.....).

Participant: our IO deals with scientific and medical rsearch. A DPA told an entity that the personal data could be transferred to us based on adquacy decision. This blocked the project. We need to find sustainable solutions.

Participant: Indept oversight and individual redress: will the pillar assessment address it?

Panelist: this is different from transfers.

Participant: data protection pillar is one where auditor will issue comments and will come back to check if recommendations were implemented. If org does not get to 70% when checked , it will have an opportunity to be re-checked.

Moderator: very similar to what came out 15 years ago. Data protection has become very important.

Session 5.1 – Data inventory

- Challenges:
  - Think of all service providers and implementing partners (e.g. transfer data to airlines to get tickets)
- Questions:
  - Useful ?
  - Which entity is responsible?
  - How xtensive should the data mapping be?
- Very time consuming exercise
- There are useful tools to help
- Approaches to categorizing
- Helpful for the PIA
- Useful yet difficult exercise. Finding out what steps need to be taken.

Session 5.2 – Performing a risk assessment

- PIA software.
- DPO of a IO:
  - Risk assessment is also necessary under C108
  - Data protection office as independent internal officer → proposal submitted to them. Essential to be involved in early process.
  - Would be helpful to have a link between PIA and register of data processing operations
  - Not a static exercise. Should follow project throughout lifecycle.

Session 5.3 - Data subject rights / redress

- Individual redress mechanisms: our privacy policy says that each of our institutions adopts mechanisms to provide individuals with a method to obtain redess. Balancing with particular status of the IO.
- Who has the authority to decide first review and appeal?
  - Business / Privacy champions in the business / DPO / Escalation group

- What rights do we give the data subject?
    - Access?
    - Right to be forgotten
    - Right to restrict processing
    - Right of appeal
- What should the process actually look like?
- Difficult questions
    - Representatives or class requests allowed?
    - How to authenticate the data subject?
    - What reasonable limitations an conditions can be imposed?
    - Monetary compensation? How to view harm that is compensable?

WW: conclusion

- Icdppc
-
    -