



Privacy by Design Conference Report

March 7th - 8th, 2019

American International School of Zagreb

<https://intprivacy.org/>

EXECUTIVE SUMMARY

20 International Schools, one International Consultancy, 50 participants and three internationally renowned experts in the field of Data Protection, all with a mission to further understanding of the EU General Data Protection Regulation, to raise understanding, pose sector-specific questions, share experiences and create a blueprint for future collaboration in the field of Data Protection and Privacy within the education sector. Building on two previous informal events at the International School of Brussels, this one and a half day conference identified areas of significant growth and awareness concerning Data Protection within schools, whilst also highlighting gaps in knowledge, grey areas of legal interpretation and challenges ahead. Most notably it provided an ethos to ensure that all students have the same right to data privacy, regardless of a schools' access to resources and to present a 'critical mass' to industry partners and Data Protection Authorities alike. Why? In order to guarantee a Privacy by Design approach within schools that is workable, proportionate, and able to adapt to new technological developments, whilst preserving the rights and freedoms of all our data subjects.

GOALS FOR THE GDPR CONFERENCE

- To raise the bar in terms of GDPR training and awareness
- To identify and establish key policies for schools concerning GDPR
- To share experiences regarding the reality of GDPR on a daily basis within schools (DPO or no DPO?)
- To discuss and work towards a Privacy by Design culture within International Schools
- The signing of the Zagreb Declaration.

ATTENDANCE

Speakers

Mr. Leonardo Cervera Navas, Director of the European Data Protection Supervisor
Cosimo Mondo, Director of the European Centre on Privacy and CyberSecurity (NL)
Leena Kuusniemi of FIPRA (Finland)
Tash Whitaker of Whitaker Solutions Ltd (UK)
Cristina Hoyos, Data Protection Officer, European School, Uccle, Brussels (B)

Participants

Participants came from all over Europe– Paris, Prague, Brussels, Zagreb, Rome, Belgrade, Bavaria, Moscow, Zurich, Helsinki, Frankfurt, Kiev, Zug and Luzern, Sofia, The Hague, Vienna, Vienna again, Luxembourg, CEESA and Croatia.

	Schools	Participants
Western EU	9	23
CEESA – 8 from Central and Eastern EU, 3 from non-EU countries	11	19
Speakers and Other		9
TOTAL	20	51
Evaluation Response		45%

THE SESSIONS

Session 1 The foundations of data privacy.

Session 1 presented an introduction to the legal framework and historical context behind the GDPR, drawing parallels between the two fundamental EU rights of Privacy and Data Protection. Placing these fundamental rights within the context of our modern age, the session addressed the challenges we face as a result of developing technologies and the increasing data challenges we face in the wake of such new technologies.

1. What is personal data?
2. Differences between personal data and sensitive data
3. Accountability
4. Group Privacy
5. Change of data use over time and Toxic data

Session 2: Data processing in schools

“Consider consent as the last action” “It can be super dangerous if it doesn’t work”.

This session introduced the lawful basis for data processing within schools and addressed the complexity surrounding legitimate interests and consents. When considering the legal basis for the processing of personally identifiable information, consideration should always be given to the context of the processing. No article, paragraph or even an entire law lives in isolation.

Schools are recognised to be reliant on legitimate interests, vital interests, consent, and the performance of a contract. But what is the interplay between these different bases, and are schools relying on the appropriate legal basis at the appropriate times?

Session 3: To DPO or not to DPO?

“There should be shared accountability and broad organisational intelligence - the DPO should not be the only person to know how to comply with the GDPR. If they leave this should not have a significant impact on an organisation as an organisation should be well briefed and have good policies, systems, and procedures in place.”

This session investigated the differing approaches to the DPO position adopted by the International Schools present at the event. One full-time DPO was present at the event, while other schools had a Data Privacy Committee/ Task Force, a part-time DPO, and/ or were reliant on the services of an external consultancy as well as legal services. Collaboration is critical to the success of the DPO role - if they don't know what's going on, how can they defend you?

Session 4: Data Mapping and Data Subject Rights

“The Record of Processing Activities is about the how and the why, the ‘where’ is secondary”

- Oran Kiazim, Senior Data Protection Advisor UK, Bird and Bird.

Starting with a clarification on the role of Data Controller and Data Processors, this Session proceeded to invite delegates to consider who our data subjects are, what is the data we hold on them, why do we hold it, where do we hold it, who do we share it with, how is it protected, and what our lawful basis is for processing it in the first place.

Session 5: DPIAs, DPAs and Data Transfers

“Processing by a processor shall be governed by a contract or other legal act..” (Article 28, GDPR)

Providing the legal background behind when a DPIA should be undertaken, the aim of this session was to consider risk in relation to data processing activities and to introduce the what, when and why of Data Processing Agreements (DPAs).

Session 6: Data Breach and SAR

“You know when a lot of data breaches happen?..... Friday afternoons...”

While a school's first priority must be to continue to protect the security of the data of its data subjects, coordination and cooperation are the keys to a successful data breach response. With any data breach incident, follow-up must be agreed, including a post mortem of the event, why it happened, lessons learned, and what should be done to ensure the incident is not repeated in future.

Subject Access Request

“The multiple data entry systems in schools make SARS a challenging procedure”

The risk of a SAR was presented as most likely to come from existing or applicant parents and disgruntled staff and students. To understand what different procedures might look like in different schools delegates debated a series of case studies. This exercise raised the challenge of identifying the data subject, should a SAR be submitted, the difficulties in relation to proof of deletion, and the level of detail required within a SAR in order for it to be adequate, whilst also respecting the data privacy of third parties who may be mentioned within a SAR response.

NEXT STEPS IN COLLABORATION

RECOMMENDATION 1 – Build infrastructure to support ongoing collaboration

- Maintain Privacy by Design -- International website
- Establish a formal DPO group with enhanced communication protocols
- Plan for the next annual conference
- Plan for mini-workshops around specific content or knowledge needs
- Plan for guest speakers to repeat their sessions
- With permission, develop ways to use the video and audio of the conference, for training purposes
- Explore the use of podcasts as a professional development method
- Write articles to be posted in industry publications
- Create announcement-style newsletters
- Plan for school exchange visits
- Improve Hubspot, the third-party processor database
- Create a “lingo” glossary of the GDPR “words of art” that we either misunderstand or they have a different meaning under GDPR

RECOMMENDATION 2 – Intentionally expand the network of colleagues and resources for international schools

- Explore securing high-quality DPO training
- Develop a shared understanding of how education is different from other industries so can develop customized guidance
- Explore the idea of a working group that will develop specific guidance for schools
- Explore the idea of creating a working model of how schools can implement data privacy

RECOMMENDATION 3 – Embed privacy by design in international schools

- Expand privacy by design to include the entire school community in a meaningful way
- Plan for engaging teachers/staff in data privacy and digital ethics
- Plan for engaging students in data privacy and digital ethics
- Plan for engaging parents in data privacy and digital ethics
- Explore the idea to jointly plan and collaborate with international bodies, including the Council of International Schools, and the European Institutions to make digital ethics a sustainable priority in the classroom

CONCLUSION

In conclusion, the conference was a success on many levels, with more participants than originally expected and the highest calibre of speakers. Consideration was given to how much was already known about GDPR within the International Schools sector and how much work has already been undertaken to promote a culture of Privacy by Design. From this experience, a number of actions have been generated that can be taken to become more knowledgeable, more collaborative and to promote best practice in the field of Data Protection, with the cooperation and support of the European Data Protection Supervisor, the European Data Protection Board, and National Data Protection Authorities.

APPENDICES

To view the presentations, speeches and Zagreb Declaration, please scan below:

