Privacy by Design Conference Report
March 7th - 8th, 2019
American International School of Zagreb

https://intprivacy.org/

TABLE OF CONTENTS

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. This one and a half day event 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 opportunity to bring together international schools with an interest in moving forward collaboratively to overcome some of these challenges, as well as 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.

It is too easy to state that this is just the beginning. 89% (171) of global constitutions already explicitly address privacy (The Constitute Project, 2018) while Privacy as a value, has been established globally since the UN Universal Declaration of Human Rights (UN 1948, Resolution 217 A (III), Articles 3 & 12). Furthermore, since the adoption of the GDPR, a ripple effect of additional data protection legislation has made waves internationally with considerable implications for schools outside of the European Union. With the continued support of colleagues representing International Schools there is a current and potentially powerful momentum to make a significant impact on the global education sector and its commitment to Data Protection.

INTRODUCTION and BACKGROUND

On March 7 and 8, 2019, the third 'GDPR' conference in a series of conferences for international schools in Europe, was held in Zagreb, Croatia. This third event was remarkably different than the first two conferences and highlighted the tremendous progress that international schools in Europe have made toward implementing GDPR.

To back up for a moment, the first 'GDPR' conference was held in November of 2017, sponsored by the International School of Brussels, with the recognition that GDPR would enter into force in May of 2018. At this point in time the GDPR was poorly understood by many in the international school community and as such the coming together of schools was an opportunity to pool resources, share experiences and work towards a common approach. This work was also supported by 9ine, a UK consulting firm that has worked with ISB and many other schools across Europe to prepare for adherence to data protection legislation in their countries.

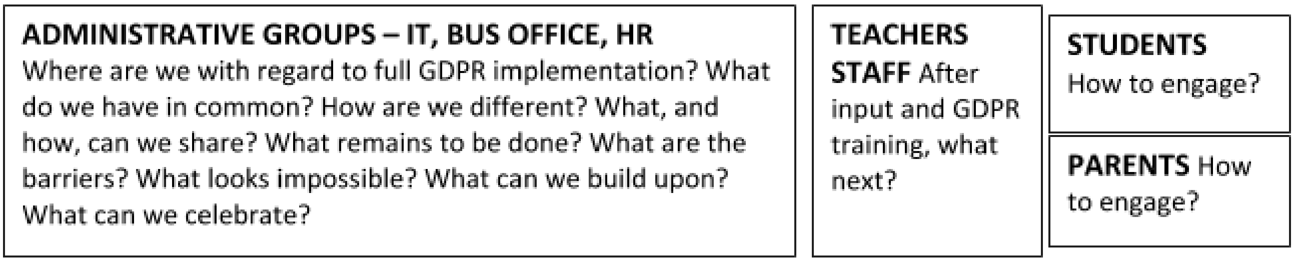
The conference participants came from schools in western/central/eastern EU and non-EU countries. CEESA (Central and Eastern European School Association) was a participant, acting as a regional entity that had taken a leadership role in assisting member schools with implementing GDPR.

Building on the foundation of the first two preparatory events, ISB and CEESA, co-hosted the third conference. Given the significant progress many schools had made in GDPR implementation since the first event, it was clear the Zagreb event needed to be different. With this in mind, the collaborative of international schools was ready to make a pivot and to enter the next phase of GDPR readiness. A conference ethos and set of goals were established to help drive the conversations forward and to provide this more knowledgeable group with nuanced examples and answers.

GOALS FOR THE GDPR CONFERENCE

Current GDPR Focus

As many schools have implemented Data Protection measures, they are aware of four major audiences in schools. The first phase of GDPR implementation has focused primarily on what needs to be done by the back office or administrative staff. Teachers have been involved primarily to provide input and to be trained on GDPR and school policies. Students have not been involved much in GDPR, nor have parents except being on the receiving end of new policies. As schools transition to the next phase, and in the spirit of privacy by design, our future focus is on the broader goals of data privacy.



ADMINISTRATIVE GROUPS – IT, BUS OFFICE, HR Where are we with regard to full GDPR implementation? What do we have in common? How are we different? What, and how, can we share? What remains to be done? What are the barriers? What looks impossible? What can we build upon? What can we celebrate?

TEACHERS STAFF After input and GDPR training, what next?

STUDENTS How to engage?

PARENTS How to engage?

Emerging Ethos

The purpose of GDPR, to demonstrate respect for an individual's right to privacy, aligns with international schools' existing commitment to child well-being and protection. We recognize that we can make greater progress with a collaborative approach that keeps the well-being of the student at the center. We believe that all students have the same right to data privacy, regardless of a schools' access to resources.

Key Questions:

Where are international schools in the privacy by design process? What challenges remain? What obstacles lie ahead? How can we work together collaboratively to navigate the future? What is the governance structure for GDPR within international schools?

Objectives:

- 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.

Attendees

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 a local Croatian company.

	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%**

PURPOSE OF THIS REPORT

The goal of this report is to communicate to a variety of audiences the content of the conference and planning for the future. The structure is to briefly summarize the individual sessions and reflect upon what we learned from the session. All of the sessions highlighted areas for follow up. Recommendations for how to move forward as a group is summarized in a separate section – Next Steps in Collaboration.

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.

Arising issues for schools and their corresponding questions:

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**

1. What is personal data?

Schools are now required to reconsider what can be defined as personal data as a result of the GDPR. Where in the past data flows of personal data within educational institutions may not have been mapped, such transfers of information must be recorded and considered in relation to the sensitivity of the data and risks associated with its processing. In order to do this successfully, schools must have a comprehensive understanding of what personal data is considered to be. Under the GDPR 'personal data' is considered to be "*any information relating to an identified or identifiable natural person*". Within the school environment this may include, but not be limited to:

- Demographic information
- Behavioural patterns and interests
- Travel history and location data
- Medical records
- Biometric data
- IP addresses
- Financial information etc.

2. Differences between personal data and sensitive data

“Consent is your best ally when done properly and your worst ally when not”

Schools have a responsibility to understand the difference between personal data and sensitive data, as well as contexts where sensitive data may be revealed, such as through the publication of photographs in print or via online resources. For the most part, sensitive data may only be processed by a school where explicit consent has been granted. With this in mind, explicit and freely-given consent is mandatory for the processing of any personal data which may reveal racial or ethnic origin, political opinions, religious or philosophical beliefs (including veganism) and trade union membership. This also includes genetic data, biometric data (where it is being processed with the purpose of identifying an individual), data concerning health, sex life or sexual orientation, and data related to criminal offences.

The notion of consent for schools in this context presents a number of challenges which will require further clarification in future, most notably in relation to the taking of photographs and videos, and their posting on school-managed and non-school managed social media accounts.

Schools would need to consider whether individuals can be identified by such images, and furthermore whether such images may reveal any sensitive data. This may be in relation to a data subject’s physical appearance, or in relation to the context in which the photograph was taken. Attendance at an event for example, may reveal an individual’s philosophy or political opinion, and as such, could reveal sensitive data.

In the absence of case-law, schools look to concrete examples from the Data Protection Authorities to demonstrate where consent may be required, and/ or instances where sensitive data is being processed.

This is important in relation to schools and their use of social media, particularly where such third party involvement also implies a controller-processor or joint controller relationship. Schools must be accountable for their role as a controller when posting personally identifiable information online, and for the responsibilities which accompany this role. Furthermore, they must also specify where controller accountability may shift directly from the school to individual faculty and staff members should individuals post photographs or videos of school activities on their own personal social media accounts.

In this regard, schools have a responsibility to educate staff on the difference between personal and sensitive data and in ensuring the appropriate consents have been granted.

In Belgium, the law regarding consent for photographs and videos has referred to whether an image is ‘targeted’ on an individual or small group of individuals and whether they can be identified via the image. If this is the case, consent is required. This approach is described below:

A " **targeted**" image is more striking as it depicts

- an image of an **individual** or
- an image in which **one or a few people are highlighted** during a group activity
- or when **posing for an image**. A good example of this is the classic class photographs or an individual photo

In the case of an " untargeted " image, it is more a matter of image material that reflects a **general, spontaneous and non-posed mood-recording instance without exposing one or a few persons.** A group photo of the class during a forest walk or sports activity is an example of this. For such images, it suffices that you inform the people/pupils concerned about the fact that such images will be taken, for what purpose you do that and what publication is concerned.

The concept of targeted vs non-targeted images poses difficulties for schools in terms of 'one or a few people' and what is 'posed' vs 'non-posed'. Furthermore, questions arise even in terms of non-targeted, non-posed photographs, should it still be possible to identify individuals within such images as a result of the context in which the image was taken.

This is an area which requires greater clarification and firm examples for schools, to ensure that they do not find themselves contravening the requirements of the GDPR. While the implications of a contravention point schools towards a fine from the relevant Data Protection Authority, the damage to an organisation's brand is potentially more significant with far-reaching implications for its sustainability and long-term profile.

3. Accountability: No surprises!

"I've learned that data is everywhere and the idea that we can contain it is impossible so we have to focus on managing it. We need to see data as valuable."

Clarity around group privacy and accountability for schools were referred to in relation to Articles 5 (2) and 24 (1) of the GDPR.

Controllers must be responsible and answerable in terms of demonstrating their compliance and be transparent about their data processing. To support this approach, the highest levels of management should be committed to the successful adoption of privacy by design procedures within schools, including data mapping, effective privacy policies, education and training, internal oversight, auditing, transparency and mechanisms for remediation and responding to external requests.

Schools are recommended to work on the concept of transparency to guarantee that all data processing is conducted lawfully and fairly. There should be no surprises for the data subject in relation to any personal data that is processed about them, what it contains, where it is stored, who can access it, and how long it is stored for.

4. Group Privacy

“The main issue is not writing protocol for schools, it's having staff follow the protocol - keep it simple and pertinent!”

Group Privacy relates to the accountability measures that a school introduces to ensure that any member of the ‘group’ who is able to access data about an individual is only able to view or process what is relevant to their particular role. The requirement falls to a school to educate staff on the concept of shared responsibility in terms of what happens to personal data as it flows through their department.

This shared approach and understanding of the different responsibilities of the different members of the group are critical in protecting an organisation against the risk of interference and ensuring that an organisation adheres to the principles of data minimisation, accuracy, storage limitation, integrity, and confidentiality.

It is essential for schools and their faculty/staff body to have a broad understanding of group privacy and what that means in terms of shared responsibility for anyone who processes data within a school.

Future consideration may be given to the use of pseudonymised data within schools, or default settings within school systems to ensure that personally identifiable data is not unnecessarily processed by default and to uphold the notion of privacy by design, however, such risk mitigation strategies are not without restrictions.

5. Change of data use over time - How to prevent Toxic Data?

‘It’s all about the WHY?’

Why was the data gathered in the first place? Care should be taken to ensure that the processing of personally identifiable data is compatible with the original purpose for which it was collected. Should schools be unsure whether this is the case, a compatibility test can be undertaken.

If data is found to be processed in a way that is incompatible with the original purpose for which it was collected, it becomes ‘toxic data’. This change of purpose should be communicated to the data subjects and recorded in the data mapping. Guidance for schools may be needed in terms of how to best to do this, particularly with regards to data subjects whose data was collected pre-gdpr.

In terms of Alumni, schools noted the potential migration of student records into alumni. This would be a different processing operation from the original purpose for which the data was collected, and as such, would render such data ‘toxic’. Organisations may need to consider ways to ensure the migration of data into alumni is appropriately informed and mapped, for example through listing this activity at the beginning of a student’s journey through school.

Going forward, schools should take care to ensure that any potential change of use should be communicated to the data subjects in advance. A strong system for data protection by design and default within schools would help to support this process and would minimise the possibility of an unlawful change of data use occurring in the future.

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?

Legitimate Interest - Would the organisation still function if this data were not being collected?

This is the fundamental question when relying on legitimate interest as a legal basis. Legitimate Interests (or LI) is not a 'magic bullet' for organisations to process the data they want, rather it is an exception to be used when no other legal basis may be doable, but when the processing of such data is nonetheless essential to the functioning of the organisation.

When relying on LI, organisations should be certain that such Legitimate Interests will not override the 'interests and fundamental rights and freedoms' of the data subject, in particular where the data subject is a child. Should any uncertainty exist, the balancing test should be applied.

Schools may need to carry out a balancing test to ascertain whether a particular processing activity does fall under LI, and a written analysis with solid reasoning must be in place to demonstrate why the activity would not override a data subject's fundamental rights.

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.

While some EU countries are requiring their public schools to appoint DPOs either externally or internally, this does not appear to be a consistently applied procedure within the international schools' sector. Nonetheless, schools reported on their experiences of using the GDPR-International group as a helpful resource as well as in seeking external consultancy support, particularly in relation to Data Mapping. Helpful online resources were cited such as Iubenda and national data protection authorities including the ICO (UK) and CNIL (France).

In spite of a standardised approach to the DPO position within schools, there was consistency in relation to collaboration, with schools incorporating working groups and cross-campus support into their data protection methodologies. The importance of Leadership team support was noted to promote a culture of privacy within the school community, as well as encouraging staff and faculty 'buy-in'.

Furthermore, some schools noted the involvement of Board Members within their structures, either as members of the Data Privacy working group or as a body to report to when a data breach occurs. As the culture of Data Privacy in schools evolves, it may be worth considering how the composition of such groups may change and adapt to fully represent the broader school community.

Such Privacy committees, whether led by a formally appointed DPO or not, are acknowledged as having a crucial role to play in mapping data processing activities, supporting shared accountability, implementing privacy by design systems and processes, and developing staff training and awareness. 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.

Referring back to the concept of legitimate interests under Session 2, schools were invited to consider whether the lawful bases being applied were accurate, and in reference to Session 1 whether special category data was being processed appropriately. This consideration fed into the question of Data Subject Rights of which organisations must be mindful when processing personal data, notably:

- Right to be informed
- Right to Access
- Erasure if data is no longer needed for the purpose it was collected for
- Right to rectification
- Right to object to processing for marketing purposes
- Right to object to automated decision making or profiling
- Right to complain to the DPA.

Furthermore, the Session stressed the importance of a granular approach to Data Mapping, making sure that every activity is included, described and updated as required.

Data Mapping was cited as a means of protecting an organisation allowing them to keep track of the data they process as well as flagging any access controls that may be required or highlighting instances where pseudonymisation, anonymisation, encryption could be applied as risk mitigation measures.

Schools reported the value of consultancy feedback in the provision of a Data Mapping template, with the recognition that this could be enhanced in future with further staff training to assist them in completing and constantly updating data mapping templates. One school reported that the Data Mapping process led to an audit of the tools they use and the creation of a Data Retention Schedule.

The mapping process revealed the scale of data collected as well as highlighted data collection practices that required further action or restriction, for example, faculty use of free online teaching resources, or a lack of school guidance to parents on the taking and sharing of photographs.

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).

Organisations noted the significant amount of DPAs required within the education sector due to the number of third-party processors contracted by schools and the sensitive data of much of the personally identifiable information involved. Schools were advised to prioritise areas of highest risk first, which would be made evident through the DPIA procedure.

To overcome the enormity of acquiring all DPAs as quickly and efficiently as possible, schools were encouraged to seek a collaborative approach towards DPAs with third-party processors or joint controllers where such third parties are used by a wide number of schools, for example, Powerschool, NWEA, Follett. A consistent approach may also help to ensure that the DPAs schools sign with such parties contains all required aspects of a DPA, including obligations pertaining to sub-processors.

Furthermore, this approach may be even more advantageous where third-party processors or joint controllers are considered to have a base outside of the EU, given that the transfer of data to non-EEA bodies is only permitted under the following criteria:

- There is an adequacy agreement
- Binding Corporate Rules
- EU Standard Clauses
- Contract Derogation
- Explicit Consent
- Legal Claim
- Vital Interest
- Public Register
- Public Authority
- Compelling one-off vital interest.

Consideration was given to US-based data processors and controllers which are not required to comply with GDPR, but which provide services to international schools required to comply with the Regulation. Discussions also took place concerning Brexit and the potential implications on contracts with UK-based organisations, which may in the future, find themselves outside of the EU.

Session 6: Data Breach and SAR

Session 6 engaged in the practical steps required to respond to a Data Breach and Subject Access Request.

Data Breach

"*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.

In preparation for a potential breach, schools must be prepared to have a data breach procedure which includes mechanisms for the following immediate actions:

- Communication with IT, Legal, Communications and Management teams
- Organisational review, or review of contract with the third party responsible
- Contact with the third party responsible
- Contact with other representatives likely to be affected, for example, other schools if the breach is via a third party and those schools are known also to have a contract with the same organisation
- Agreed single point of contact and porte parole for external communications
- Agreed to means of giving information regarding the breach via the school website or any other means appropriate
- Agree on steps to define width and depth of breach notification for DPA (if needed)
- Available Data Breach procedure guidelines for all staff to ensure a consistent approach

During the event, schools shared experiences of potential (low risk) breaches that had occurred, as well as mitigating actions and their own data breach procedures. This included the integration of Data Breach recording within the school's IT system, thereby facilitating the reporting process and ensuring an effective organisational literacy for understanding the school's reporting procedure.

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.

Finally, discussions around Subject Access Requests also addressed potential difficulties in identifying a clear line between objective and subjective data. This is not yet defined and represents challenges in relation to confidential references (where nationally implemented laws may differ) as well as student reporting or counsellor notes.

The debate broached a broader question in relation to the rights of students aged 13 and over, whose parents have a contract with the school, but who are themselves deemed old enough under national law (at least in Belgium) to determine for themselves how their personal data may be processed. The legal representation in the room confirmed that while the school has a contract with the student's parents, this would not override the student's rights and freedoms to data privacy, and as such, the student has a right to dictate access and ownership over their own data. In a practical sense, this was applied to a situation where a student may not wish for a parent to see their school report. It was determined that the student had the right to make such a decision, while the right of the parent would simply be to see whether their child had ‘passed’ or not.

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
- Pla 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: