Centre for Advanced Research in Management and Applied Ethics

ETHICS and COMPLIANCE ACADEMY

Privacy & Data Protection for Education

Two Basic Issues

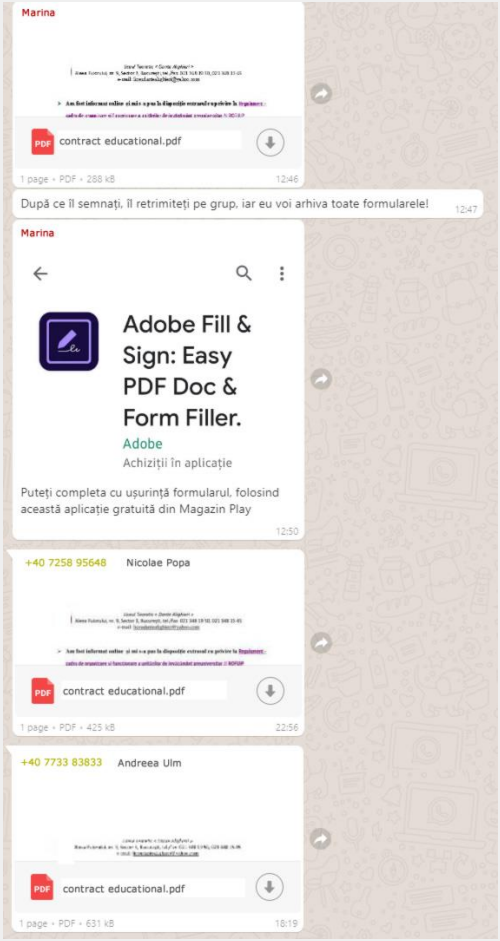
Risky Apps, Risky Communication Practices

Marina is the leading teacher for a 4-grade class of Romanian students. Her job includes a close communication with the parents of her students. In the previous years, this used to be sporadic, with parents mainly meeting her after the daily schedule. She was also used to send short messages to parents via WhatsApp, but, during the pandemic, when face-to-face meetings were no longer possible, this took over all the communication.

Due to this situation, at the beginning of the school year, Marina sent the educational agreement and some other official documents, including medical consent, that parents have to sign in order to ensure compliance with school regulation. She explained how the PDF file can be filled in with the required information and electronically signed by the parents.

All those documents contained not only the names of the parents and students, and their home/official addresses, but also their personal identification number and some data regarding the medical situation of the kids (allergies, chronic illnesses, medical treatment etc.). Generally, this kind of information does not lead to any kind of discrimination, but, in one particular situation, there is an element that might be used in this way. One of the students suffers from a hearing deficiency that parents want to keep it undisclosed because of previous experience with bullying at a different school.

All the parents sent the PDF documents via the same Whatsapp group.



Personal Data

1

‘Personal data’ does not include only data about an identified individual, but also data about a person that can be used at some point to identify it.

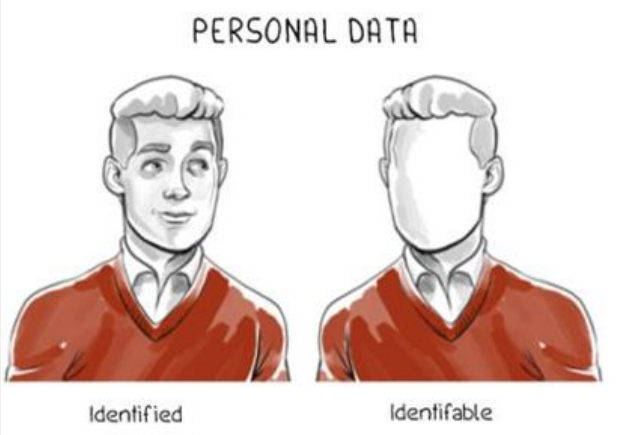


Illustration by Daniel Solove
https://twitter.com/DanielSolove/status/948943917193531398/photo/1

Personal Data

2 What does count as ‘personal data’?

General information

- Name, age, job title,
- Personal email address (including those hosted by public services like Google)
- Personal phone number
- Home address
- **Economic, cultural, political or social identity of a person** (e.g. economic status, ethnicity, sexual preferences, political opinions)

Travel & Location data

- Travel history
- Location logs

Financial data

- General bank information (e.g. bank account)
- Transaction history
- Credits and insurance history

Connectivity data

- Network & computer ID data (IPs, MACs)
- Device information
- Online behavior
- Online group membership

Biometric data

- Facial recognition data
- Fingerprints
- Voice recognition data
- Iris and retina recognition data
- Palmprint
- Ear shape recognition data

Health data

- Patient medical history
- Information about disabilities
- Medical diagnosis, opinion, etc.
- Medical treatment
- Genetic data

Personal Data

3

What does not count as ‘personal data’?

- **School email address**
- Information about school budget and other administrative issues
- **Data related to school activities (class calendar, etc.)**
- Statistical data related to no. of students, absentees, etc.

An Unprepared School

Turgheniev High-School from Budapest, Hungary, just installed a complex digital system that holds both the school data (teachers and students data) and the security system, which includes biometric data. Every person working for this institution or studying there received, based on historic paper-based documents, a new electronic profile.

All the data is hosted both on a local server and in the cloud, with support from specialized IT company that ensure the safety and security of the electronic system.

In order to ensure compliance with GDPR, the system allocates a random number to each individual account and provides an anonymization key for making anonymous processing possible. Consequently, the biometric data of a teacher are connected to the teacher's personal account, but not directly: another key is used to configure the connection between the biometric security system and the personal account identified by the number assigned to the teacher.

The personal accounts of teachers include not only educational activity and logs related to their presence in school, but also administrative and financial history, as well as various documents regarding medical history, disciplinary actions, etc. Similarly, for students, the personal accounts include not only the educational activity (grades, school calendar, regular evaluation letters etc.), but also data regarding physical and psychological evaluations done at school by specialized personnel, medical history, etc.

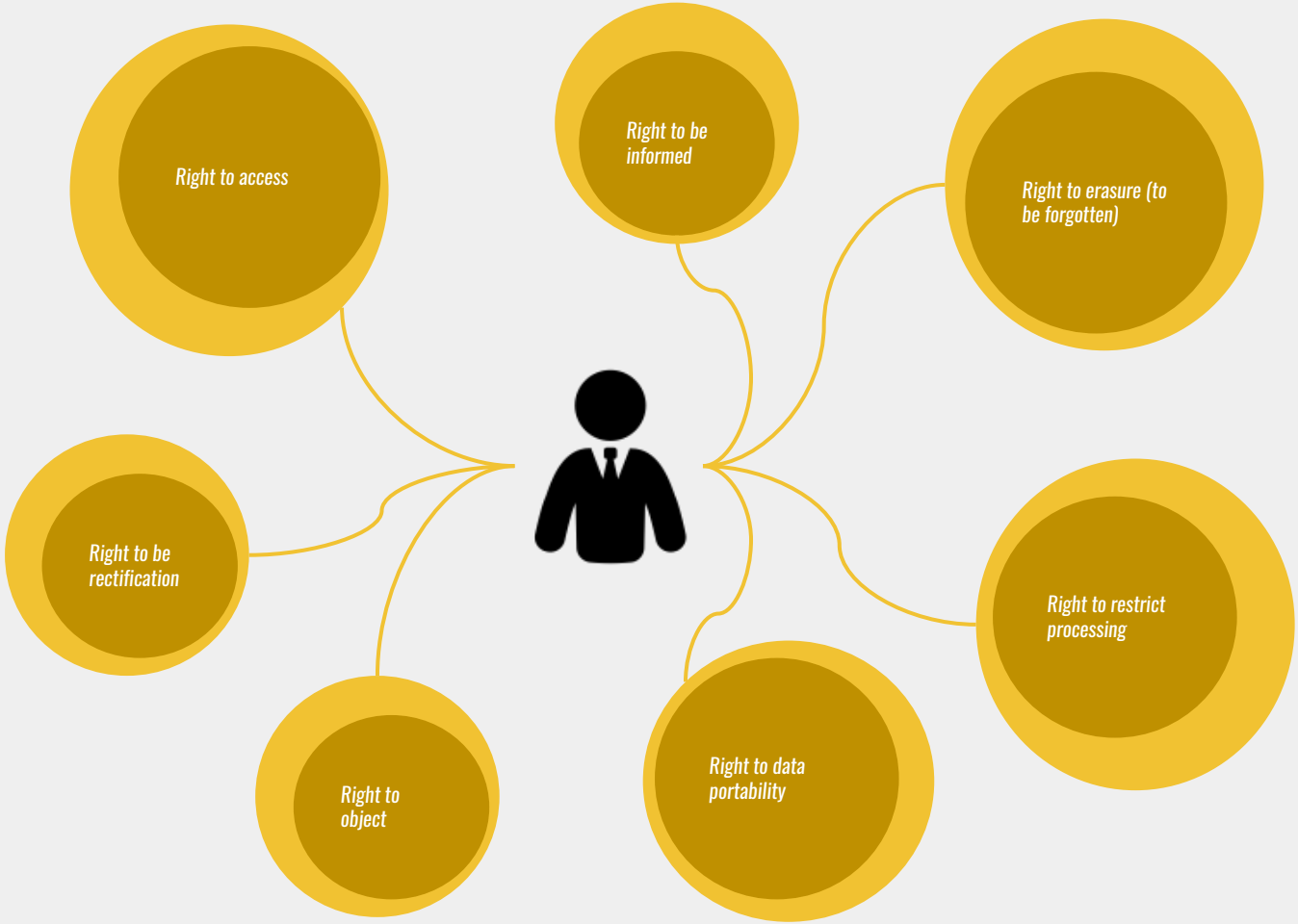
As soon as the system was installed, everybody could enter the school only if the system recognized them. A guard was announced every time an unknown person entered the school and that person was identified in a special electronic registry.

When the system was up and running, the Headmaster gathered together every member of the school and informed them about the new electronic platform and what it involves. It made clear that the system is secure and a specialized company is making sure the data is safe and secure. That was the only time the school management discussed the new system. The teachers themselves carried this message to the parents and students, explaining them how it works and what it involves from them. For this, the teachers received 3 hours of self-paced online training from the producer of the system.

After four months, some unknown hackers penetrated the security layer of the system and extracted all data available at that moment. In total, around 1TB of data, including the access logs.

The school management tried to hide the incident for over 5 months, but, at a certain point, an anonymous message placed on the Facebook page of the school revealed the entire situation.

RIGHTS OF DATA SUBJECTS



THE 7 PRINCIPLES OF GDPR

Art. 5(1)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)

Art. 5(2)

- Accountability

1. The user has given you **consent** to do so.
2. You must do it to make good on **a contract**.
3. It's necessary to **fulfill a legal obligation**.
4. For **protection of vital interests of a natural person**.
5. It's a public task done in **public interest**.
6. You can prove you have **legitimate interest**, and it's not overridden by data subject's rights and interests.

Thank you!

Cristian Ducu, *Phd*

Senior Expert - Governance, Ethics & Compliance, Anti-Corruption, Sustainability

Centre for Advanced Research in Management and Applied Ethics
www.etica-aplicata.ro

European Ethics & Compliance Association
www.ethicscompliance.eu

cristian.ducu@etica-aplicata.ro
+4 072 251 6889