INTERNATIONAL CONFERENCE OF PRIVACY AND DATA PROTECTION COMMISSIONERS

* * *

Personal Data Protection Competency Framework for School Students

Intended to help Educators

October 2016

October 2016

Personal Data Protection Competency Framework for School Students

Intended to help Educators

Introduction and Acknowledgements

Why an international framework on data protection training?

In the digital age, responsible, ethical and civic-minded education in the use of new technologies is a priority for action, particularly for young people in school.

A key component of digital education is highlighting privacy and personal data protection. Educators have a key role to play in this digital education of citizens.

Acquiring critical knowledge and understanding of digital rights and responsibilities, developing critical thinking skills in young people towards the uses of personal data, raising awareness of risks, and teaching practices to enable people to navigate the digital environment with confidence, lucidity and respect for the rights of everyone – these are the learning objectives to be attained.

To assist educators, data protection authorities—with their expertise in this field—thought it necessary to design a training framework for students specifically dedicated to data protection, for use in official school programs and in training courses for educators, regardless of the particular discipline taught.

Although it can certainly be adapted to address specific educational purposes, laws and data protection approaches relevant to each country, the framework has been deliberately designed to have an international dimension.

Why? Because this is a major issue that concerns all countries without distinction; because it aims to create **a common base of concrete and operational competences about personal data protection** that can be used by everyone; and because its purpose is to address the world of education as a whole.

That is why this framework, designed on the initiative of the International Digital Education Working Group coordinated by the National Commission on Information Technology and Liberties (CNIL), was adopted by all the data protection authorities at the 38th International Data Protection and Privacy Commissioners' conference in October 2016[1].

About the Framework

The purpose of this set of learning principles is to provide all students the knowledge, competencies and skills identified in the common base of concrete and operational competences of the competency framework on data protection.

This framework presented here has nine ***foundational principles***; knowledge and understanding of these is a priority.

[1] Resolution of 18 October 2016 for the adoption of an international Competency Framework on Privacy Education.

A block of stand-alone general competencies is identified for each principle. They are juxtaposed and linked so that they achieve a progressive thematic balance. Nevertheless, educators will be able to use them, either by following the progression suggested in the document or in a modular manner, as part of their instruction.

Each of the principles was analyzed in terms of **knowledge** and **skills**, with the acquisition of the knowledge or skill affecting the student's ability to say "*I know*" and/or "*I can*." These **descriptors**, as well as what the terms "knowledge" and "skill" cover, are defined in the proposed terminology appended to this document.

The agreement reached on ***a common base of concrete knowledge and skills*** is the first step in disseminating and promoting the protection of personal data and privacy in education programs.

Other steps and action items are important to successfully achieve digital education efforts, which are:

- How educators implement these teaching principles in the classroom setting;
- The identification, **based on the age group considered**, of the degree of depth needed for each knowledge and skill element; and
- The availability of **training and education resources** to professionals and their students.

Further information at digitaleducation@icdppc.org

Acknowledgements to the contributors:

This framework has been designed by the French data protection authority, the National Commission of Information Technology and Liberties (CNIL), with the invaluable assistance of the data protection authorities belonging to the International Digital Education Group. It has also benefitted from the knowledgeable advice of education specialists and experts with the Educational Services of the Council of Europe.

Summary

[1/9] Personal data

Purpose: Understanding the concept of **personal data** is essential. The notions of **pseudonymity and masking one's identity** and **metadata** are also explained. The student is also taught that **certain personal data can be considered particularly sensitive,** because of the intimate nature of private life and/or the data could be the source of possible discrimination or they refer to minors. Finally, understanding the terms of data collection and processing is necessary to understand the concept of personal data.

KNOWLEDGE outcomes

- I understand what is involved in the concept of **personal data**, defined as any data—whether or not it was made public—about an identifiable individual;
- I know and understand the concept of **pseudonymity and masking one's identity**;
- I know that, **depending on how it is processed**, data may allow the identification of individuals;
- I know some **technical data** can assist in the identification of individuals; that scanned documents and images have embedded **metadata** that describe their contents and that online activity may leave **traces** (cookies, browsing history, etc.) which can contain personal data;
- I know that there are data **which can be considered as particularly sensitive, according to countries, and** which, for example, contain information regarding **minors, people's origins, political and/or religious opinions or affiliations, biometric or genetic profile, health and/or sex lives.**

SKILLS outcomes

- I can give examples of personal data that can directly identify individuals (civil status, photo of a student in the class, etc.) and technical data that can monitor the activities of a person and identify them (cookies, geolocation data, etc.);
- I can give examples of sensitive personal data (e.g., health, genetic profile, sex lives…).

[2/9] Privacy, civil liberties and protection of personal data

Purpose: The right to the protection of personal data is founded in **human rights, civil liberties, democratic values and citizenship**. It is also an important guarantee of **respect for privacy.**

KNOWLEDGE outcomes

- I know what human rights and civil liberties are and can recite them;
- I know these principles and democratic values are exercised as much in the real world as in the virtual world;
- I understand the concept of privacy, the right to privacy, and the need to have them recognized and protected;
- I understand how my actions may affect the privacy of others;
- I understand how the protection of privacy is not just about everyone's private life, but can also be applied in the public space, particularly on the Internet;

SKILLS outcomes

- I can give examples of situations pertaining to private life (e.g., medical consultations, parental separation);
- I evaluate what information I can and cannot disclose about myself and others (e.g., my home address, illness of a relative, etc.);
- I can give examples of situations in which digital media use has enhanced the expression of civil liberties and/or, *on the contrary*, curtailed them.

[3/9] Understanding the digital environment – technical aspects

Purpose: To protect his/her privacy, the student must understand the digital environment and must be able to navigate it independently. To do so, it is necessary to understand the **hardware** and **technical infrastructure of information systems** that support deployment.

KNOWLEDGE outcomes

- I know the difference between hardware, software and applications; I understand how **software and hardware components** make up computer systems;
- I know what the **Internet and its services** are (social networks, mobile applications, the cloud, etc.);
- I understand how digital space is structured (physical networks, browser, IP addresses and URLs, search engines, etc.);
- I am aware of the concept of information **architecture**, and the **collection**, **structure** and **processing** of information;
- I know the key **IT risks;** I know what **digital security** includes and understand the need to ensure the physical and logical security of a digital environment.

SKILLS outcomes

- I assess my practices and develop **problem-solving** and **learning** reflexes— namely about security—by identifying resources (user communities and forums, tutorials, etc.);
- I can identify malfunctions and solve simple problems by following established procedures; if necessary, I know how to actively seek solutions online, particularly when it comes to ensuring the security of my digital environment.

[4/9] Understanding the digital environment - economic aspects

Purpose: Understanding the digital environment and navigating it independently require **understanding it as an *ecosystem*** and **understanding its underlying logic**; this involves knowledge and competencies: the economics and ***value*** of personal data, key players and services, and economic models.

KNOWLEDGE outcomes

- I know who the key players in the digital economy are (e.g., ISPs, service providers, developers, curators, etc.);
- I understand the systems used to market products and offer **free services** (loyalty cards, targeted advertising *via* cookies, setting up user accounts, subscribing to newsletters, etc.), for the purpose of establishing **personalized user profiles**;
- I understand that the majority of such offers of services entail collecting and using personal data as well as storing this information in a database;
- I know what **data** are collected and stored when I use the Internet, a social network or a service.

SKILLS outcomes

- I can give examples of the types of technical data likely to be collected when I am online (e.g., browser type, contacts list, geolocation data, private messages, etc.).
- On any given website, I can find the **terms and conditions of use** of my personal data (Terms and Conditions of Use, legal information, privacy policy, etc.).
- I can give examples of digital services whose economic model involves—or does not involve—the collection of personal data.

[5/9] Understanding personal data regulations and legislation

Purpose: Knowledge of **data protection systems and institutions** is covered in this competency principle: *regulation principles*, applicable legal texts, Data Protection Authorities (DPAs). The student understands that i**n a *number of countries*, personal data is protected by laws and regulations**, which means that individuals or **organisations** are not free to use it as they please.

KNOWLEDGE outcomes

- I know that personal data cannot be used for just any purpose and that regulations exist;
- I know and understand **the key rules relative to data protection:**
  - Personal data is processed or used for specific purposes and must be relevant to or consistent with the activity in question (e.g. finality, proportionality);
  - Some particularly sensitive data can be, in certain countries, be regulated in a specific way (e.g. data from minors, people's origin);
  - Personal data should not be retained for longer than is necessary and must then be archived or deleted (retention period) when appropriate according to countries's Privacy laws ;
  - People have rights regarding their personal data (e.g. access, correction, , refusal, consent);
  - Personal data is collected and processed or used under conditions that ensure privacy;
- I know that public and private organizations that collect and process or use personal data must comply with these rules and that violations can lead to **sanctions, according to countries**;
- I know of the existence, role and powers of **Data Protection Authorities**;
- I know that people about whom personal data is collected must be **informed** on their rights and of the use to which their data will be put and to whom it may be shared.

SKILLS outcomes

- I can give examples of digital practices that I think **comply** with and/or **violate** data protection regulations;
- I can name the Data Protection Authority in my country (of my area) or give an example of a Data Protection Authority, and I can cite examples of actions or decisions made by the authority;
- If a Data Protection Authority exists in my country, I can contact it for information and advice.

[6/9] Understanding personal data regulations: Controlling the use of personal information

Purpose: The student is taught that **the controlled use of his/her personal data** is both necessary and legitimate, based on the context in which it is used in daily life (as a student, team member, member of a family, etc.). The way that the student identifies him/herself and/or makes him/herself known to others in the digital world can vary depending on the situation and lead them to reveal more or less information about themselves. This is learning to manage one's "digital identities." Students are also introduced to the fact that they have rights and duties, particularly towards others.

KNOWLEDGE outcomes

- I understand the need and purpose of providing or not providing personal information, depending on the context and the end use of the information;
- To this end, I know how to set up and use pseudonyms and more than one email address, account and/or profile **depending on how I intend to use them**.
- I know that it is necessary to regularly monitor what is said about me online (my e-reputation);
- I know that posting involves **responsibility on my part** and that of my parents / legal guardians.

SKILLS outcomes

- I am careful to only share the personal data that is absolutely necessary to register for a service;
- I can express myself online while taking into account the **nature of the space** in which I am posting (private, public, related to school, family, friends, etc.);
- I am **vigilant about what I publish online**, even under a **pseudonym**;
- I can participate in an online debate with **respect for others**: I do not share information and photos of third parties without their knowledge and that can harm their privacy or reputation;
- I use tools to regularly monitor content and information about me that is seen by others on social networks.

[7/9] Managing my data: Learning to exercise my rights

Purpose: Here we learn about the range of actions available to me as a child/teenager *when it comes to consenting to or refusing the collection of my personal data,* **alerting**, **reporting** and protecting myself—through **intervention by a responsible adult**, when appropriate (*)—to deal with situations experienced and/or identified as breaching the privacy and/or the integrity of persons, or which constitute a violation of the law.

(*) By introducing the concept of **intervention** by a responsible adult and/or legal guardian, the authors take into consideration the specifics of national legislation, services offered, age group, child's level of autonomy and identified practices.

KNOWLEDGE outcomes

- I know that, to use certain online services, the consent of myself or my parents/legal guardians **is required**;
- I know that I have **rights regarding my personal data (e.g. access, correction, refusal, consent, delisting, erasure)** and that I can exercise these rights or have them exercised on my behalf by contacting the service in question according to domestic procedures and, in the event of a refusal or any problems, by contacting the Data Protection Authority if it exists, a judge, according to countries and/or the relevant national/sub-national authorities, or advocacy groups.

SKILLS outcomes

- I can update or request updates to data concerning me which appears to be **outdated, inaccurate or incomplete**, if necessary.
- I can request the deletion of my personal data online;
- I am able to check with the service in question whether or not personal data have been **collected and stored in a database**. If necessary, I can obtain this information from the service in question and exercise - or have exercised on my behalf - my other rights regarding said service;
- I am able to unsubscribe from a service and/or delete an account that I have created.

[8/9] Managing my data: Learning to protect myself online

Purpose: This competency principle covers the solutions used to **ensure the technical protection** and **security of personal data**. These solutions are the subject of **learning processes** experienced within the collective framework of school and school-related environments. Students must know how to use technical devices to identify and authenticate themselves online, authorize - or not - the collection of personal data, and set up an account and/or profile in accordance with data protection rules.

KNOWLEDGE outcomes

- I know that there are **ways to protect myself online**: in particular, I am familiar with the different ways to **identify and authenticate** myself; I am aware of data encryption solutions;
- I understand **the terms and conditions** of use relative to online services (allow or refuse geolocation, allow or refuse applications access to my contacts, photos, etc.);
- I know that I can **manage the settings** of the online applications and services that I use.

SKILLS outcomes

- I use procedures available **to protect my personal data**: for my accounts and profiles I can create strong passwords, or passphrases, and change them regularly; I can examine documents and images that I share online and if necessary, I can use tools to delete metadata; and data encryption solutions;
- I can manage the **security and privacy settings** of the accounts, profiles and devices that I use; **I regularly check** these settings and **adjust them**.

[9/9] The digital world: Becoming a digital citizen

Purpose: Students are to develop a critical and ethical approach to navigate the digital environment with **confidence and clarity** and act accordingly. Exercising their rights, using digital services while respecting the protection of personal data, identifying service offerings that may affect privacy or freedoms, reporting, and mobilizing: all actions which define a digital citizen, responsible for their own data and respectful of the data of others.

KNOWLEDGE outcomes

- I can compare information and **assess whether or not it is reliable**;
- I can **analyze and critically assess** a situation related to the use of digital media (e.g., the spread of false information and/or rumours);
- I can identify inappropriate or illegal content and behaviour;
- I can recognize situations involving **reputational damage** or **cyber-bullying**.

SKILLS outcomes

- In the situations described above, I can, directly or through an adult, **notify the relevant authorities and/or advocacy associations**;
- I am able to foster positive outcomes (complaints likely to influence major Internet players, mediation to ensure that inappropriate behaviour stops, development of codes of conduct, etc.);
- I am able to judge whether it is **appropriate** to publish such information **in a given context**; I can analyze and foresee the potential consequences of sharing it online.

Glossary (coming)