State-of-the-art report on teaching privacy and personal data protection at schools in the European Union
Gonzalez Fuster, Gloria; De Hert, Paul; Kloza, Dariusz

Publication date: 2015

Document Version: Final published version

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.
ARCADES

Introducing dAta pRoteCtion AnD privacy issuEs at schoolS in the European Union

http://www.arcades-project.eu/

CALL: JUST/2013/FRC/AG
AGREEMENT NUMBER: JUST/2013/FRAC/AG/6132

Workstream 1: Preparing the two-day seminar for teachers.

Deliverable 1.1: State-of-the-art report on teaching privacy and personal data protection at schools in the European Union

Prepared for the European Commission
Directorate General Justice
Co-funding by the Fundamental Rights & Citizenship Programme

Brussels, March 2015

Disclaimer: the contents of the paper do not necessarily reflect the views of the European Commission
State-of-the-art report
on teaching privacy and personal data protection at schools
in the European Union

Responsible partner:
Research Group on Law, Science, Technology and Society (LSTS), Vrije Universiteit Brussel (VUB)

Authors:
Gloria González Fuster (VUB-LSTS), Paul De Hert (VUB-LSTS) and Dariusz Kloza (VUB-LSTS)

Delivery date:
31 March 2015

Status:
Version to be submitted to the European Commission.

Revision history:

<table>
<thead>
<tr>
<th>Rev.</th>
<th>Date</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1</td>
<td>18 March 2015</td>
<td>VUB</td>
<td>First draft for partners’ consultation</td>
</tr>
<tr>
<td>V2</td>
<td>31 March 2015</td>
<td>VUB</td>
<td>Final version, changes following feedback by GIODO, NAIH and IC Slovenia</td>
</tr>
</tbody>
</table>
# Table of contents

Introduction ........................................................................................................................................... 5

1. EU privacy and personal data protection for minors ................................................................. 6
   1.1. Current landscape .................................................................................................................. 6
   1.2. The proposed General Data Protection Regulation ............................................................ 7
   1.3. Rights of the children ......................................................................................................... 10
   1.4. Privacy and personal data protection culture .................................................................... 10
   1.5. Compendium of key issues ............................................................................................... 11

2. General background ....................................................................................................................... 12
   2.1. Council of Europe ............................................................................................................. 12
      2.1.1. Building a Europe for and with children ................................................................. 12
      2.1.2. Human rights education ............................................................................................ 13
      2.2. European Union ............................................................................................................ 14
         2.2.1. Promoting the EU Charter and privacy and personal data protection ................. 14
         2.2.2. Promoting children rights ....................................................................................... 15
         2.2.3. Strategy for a Better Internet for Children ............................................................. 15
         2.2.4. Other EU policies .................................................................................................. 16
   2.3. International cooperation of Data Protection Authorities ................................................. 17

3. A variety of practices ................................................................................................................... 18
   3.1. Privacy and data protection in official curricula ................................................................. 18
   3.2. Classification of available materials and relevant activities .............................................. 19
      3.2.1. Materials and activities by data protection authorities ............................................ 20
         a) Data protection authorities targeting schools ......................................................... 20
         b) Other data protection authorities activities targeting minors .............................. 25
         b) Other data protection authorities’ activities revolving about the protection of minors ................................................................. 29
      3.2.2. Materials and activities by other organisations ........................................................ 30
         a) Developed in the context of the Safer Internet / Better Internet for Kids Programme ......................................................................................................................... 30
         c) Other ........................................................................................................................................ 31

4. Analysis of teaching materials .................................................................................................. 32
   4.1. Aims .................................................................................................................................... 32
   4.2. Tools .................................................................................................................................... 33
      4.2.1. Lesson plans ............................................................................................................... 33
      4.2.2. Other elements .......................................................................................................... 33
      Videos ....................................................................................................................................... 33
      Test and quizzes ............................................................................................................................... 34
   4.3. Target audiences .................................................................................................................. 34
   4.4. Content .................................................................................................................................. 35
      4.4.1. Introducing privacy and personal data protection ................................................... 35
         a) The significance of privacy and personal data protection ...................................... 35
         b) Surveillance .................................................................................................................... 36
      4.4.2. What is privacy .......................................................................................................... 37
      4.4.3. What is personal data protection ............................................................................ 37
      4.4.4. Protect your data ....................................................................................................... 38
      4.4.5. Decide, and decide wisely ......................................................................................... 39
         a) How to consent genuinely ............................................................................................ 40
         b) Consent can be revoked .............................................................................................. 41
      4.4.6. Do not share without consent ................................................................................... 41
      4.4.7. Internet does not forget… yet? .................................................................................. 42
      4.4.8. Parents ....................................................................................................................... 43
a) Surveillance by parents ................................................................. 43
b) Over-sharing parents ................................................................. 44
4.4.9 Schools .................................................................................... 45
4.2.10. Take action (if necessary) .................................................. 45
   a) Use your personal data protection powers ................................ 45
   b) Know how to react in case of serious problem .................... 46
   c) Do not fall into blackmail ......................................................... 46
4.2.11. Meet your data protection authority ................................. 47

5. Concluding remarks ...................................................................... 47

Bibliography ................................................................................... 47
Introduction

This report offers a state-of-the-art review of materials available for teaching privacy and personal data protection at schools in the European Union (EU), assessing prior knowledge in this area. It has been produced in the context of the Introducing Data Protection and Privacy Issues in the European Union (ARCADES) project, co-funded by the EU, which aims to elaborate new materials to be used for the wider promotion of school education about privacy and personal data protection across EU Member States, targeting children aged between 6 and 18. Concretely, ARCADES focuses on the preparation of educational materials that will help shaping informed and responsible attitudes towards personal data protection and privacy.

The purpose of this report is to provide relevant insights able to guide the ARCADES consortium in that direction. It does not have the ambition of delivering an exhaustive account of all past and existing initiatives in the area of European privacy and personal data protection education, which are numerous, and which have already been surveyed in other settings. The mapping put forward here is primarily directed to document major trends and common (as well as best) practices, and to open up a discussion on the requirements that upcoming materials in this area should meet.

The ARCADES project targets the development of documentation and approaches that are relevant all over the EU. This notably implies that, in the end, the project’s objective is to offer materials that are not country specific, but potentially pertinent in any Member State – even if they might inevitably require some flexibility to ensure their practical and direct relevance in each local context. ARCADES’ focus on EU-level relevance implies also that the project’s goal is not to work towards solutions that are necessarily globally fitting. Teaching privacy and personal data protection at EU schools requires embracing the peculiarities of the European position in this field, which cannot be neglected.

The report’s first section focuses precisely on the basic features of the EU privacy and personal data protection legal framework, insofar as it relates to minors. To this purpose, the first section maps pertinent privacy and personal data protection legal instruments, but also considers children’s rights, and how they can be relevant for European children’s personal data protection and privacy. Additionally, the first section introduces the notion of ‘privacy and personal data protection culture’ as a notion that allows to grasp the different dimensions that are at stake in individuals’ relation with privacy and personal data protection.

The second section describes the general background of the support of privacy and personal data protection school education internationally and in the EU. It introduces the main actors involved, and reviews their goals and main actions.

1 http://www.arcades-project.eu/
2 These ages indicate the prime references for the targeted audience; in practice, children and youngsters of other ages might also be reached. It must be noted that in some Member States such as Poland school education formally targets youngsters of up to 19 years.
3 Most notably, by the Working Group of Data Protection Authorities on Digital Education, an international group of data protection authorities collaborating on digital education issues (see: Working Group of Data Protection Authorities on Digital Education (2014), Table of results and fact findings from the questionnaire on digital education: Overview of the resources provided by 36 contributions to the 3 questions – classified by regions and main topics, 1 September 2014). The authors of this report are extremely thankful to the Working Group for the input provided in the context of this research.
The third section documents the variety of relevant practices currently in place in Europe, by providing a profusion of examples. It advances information and knowledge emanating from the data protection authorities (DPAs) participating in the ARCADES project, but also from non-participating DPAs. It primarily focuses on EU initiatives, but also considers instances from non-EU countries with related privacy and personal data protection frameworks, such as Norway.

The report’s fourth section enters into a deeper analysis of currently available materials. It discusses what are the tools currently used, the audiences targeted, and which are the main topics of existing European privacy and personal data protection education materials. Finally, a concluding section describes the following steps of the ARCADES project.

1. EU privacy and personal data protection for minors

The regulation of privacy and personal data protection in EU Member States involves three basic legal orders: the national level, the EU-level and the level of the Council of Europe. These three basic layers of protection are substantially intertwined. National regulation in Member States results to a great extent from the implementation of EU personal data protection law, which is directly inspired by Council of Europe’s instruments, which in their turn are also relevant nationally. The purpose of the ARCADES project being to produce materials with relevance across the EU, in the context of this report it is appropriate to focus on applicable privacy and personal data protection provisions from the prism of EU law.

1.1. Current landscape

In EU law, the starting point for privacy and personal data protection are Articles 7 and 8 of the Charter of Fundamental Rights of the EU. The Charter’s Article 7 sets out a right to privacy, corresponding to the right to respect for private life of Article 8 of the European Convention on Human Rights (ECHR). Article 8 of the Charter enshrines as a distinct right, the right to the protection of personal data. The coexistence of two fundamental rights, one about privacy and the other about personal data protection, can be regarded as one of the main particularities of EU law. Although some EU Member States also recognise internally two distinct and autonomous rights, it is not always the case. In the context of the Council of Europe, additionally, personal data protection safeguards are typically conceived of as a manifestation of the right to respect for private life.

Another key provision of EU law on personal data protection is Article 16 of the Treaty on Functioning of the European Union (TFEU). The first paragraph of Article 16 of the TFEU restates the existence in EU law of a right to personal data protection. Article 16’s second paragraph imposes a mandate on the European Parliament and the Council to lay down rules in this area.

Currently, the most important EU legal instrument on personal data protection is Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and

---

4 The EU Charter is legally binding since the entry into force of the Lisbon Treaty in December 2009 (see Article 6(1) of the Treaty on European Union (TEU)). The EU Charter was originally solemnly proclaimed by Parliament, the Council and the Commission in Nice on 7 December 2000. On 12 December 2007 the Presidents of Parliament, the Council and the European Commission signed and once again solemnly proclaimed a revised version.

5 On this right, see notably: Gloria González Fuster (2014), The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer, Dordrecht.
on the free movement of such data (generally known as the ‘Data Protection Directive’). This Directive delineates the general applicable framework, developed notably also by other instruments of EU secondary law such as Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive).

The principles set out by the Data Protection Directive ‘give substance to and amplify’ those of Council of Europe’s 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (‘Convention 108’), which has been ratified by all EU Member States.

At the level of the Council of Europe, the key provision is Article 8 of the ECHR, already mentioned, which guarantees everybody’s right to the respect for private life. Over the years, the European Court of Human Rights has been built a solid case law on this provision, integrating in it safeguards related to the processing of information about individuals, making explicit references to Convention 108.

All EU Member States are members of the Council of Europe and must respect ECHR’s Article 8. Member States are also bound by the EU Charter of Fundamental Rights when implementing EU law, and all of them have transposed Directive 95/46/EC as well as Directive 2002/58/EC in their own legal order.

Directive 95/46/EC applies generally to personal data relating to identified or identifiable natural persons, and thus also to data relating to minors. It does not include, however, any specific provision dealing with them. Some Member States, nevertheless, have adopted national instruments that do adapt some of the provisions of the Data Protection Directive to the protection of minors, for instance imposing different obligations in terms of consent. Differences can notably concern the age until which parental consent shall be required, and how to obtain verifiable parental consent.

### 1.2. The proposed General Data Protection Regulation

In 2012, the European Commission launched the review of the current EU data protection legal landscape with the introduction of a legislative package that notably included a proposal for a General Data Protection Regulation, currently still under negotiation by the EU Commission.
The proposed Regulation was specifically designed to replace Directive 95/46/EC, reinforcing the level of harmonisation across EU Member States.

The European Commission incorporated into the proposed General Data Protection Regulation explicit references to children. In this sense, the preamble of the proposed draft declares that "[c]hildren deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data". It then adds that, in order to determine when an individual is a child, should be taken over the definition laid down by the UN Convention on the Rights of the Child.

The proposed draft offers indeed a definition of a ‘child’ based on the United Nation’s (UN) Convention on the Rights of the Child. According to Article 4(18) of the proposed text, ‘child’ shall mean any person below the age of 18 years.

The main provision about the protection of personal data of children in the proposed General Data Protection Regulation is Article 8, titled ‘Processing of personal data of a child’, and which sets out special conditions for the lawfulness of the processing of personal data of children in relation to information society services offered directly to them. By virtue of this article, which is only applicable to the offering of information society services directly to a child, in order to ground the processing of personal data of a child below the age of 13 on consent it is necessary to obtain consent authorised by the child’s parent or custodian. Concretely, Article 18(1) states: ‘For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child’s parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology’.

It must be underlined that although the title of Article 8 refers generally to the processing of personal data of children, which are defined as any person below 18 years, in practice the requirement of needing consent by the parent or custodian is only applicable to children below 13 years. As a result, it must be deduced that minors aged between 13 and 18, who are officially still falling under the category of ‘child’, can nevertheless consent on their own to the processing of their personal data. The draft also foresees the possible adoption by the European Commission of delegated acts and standard forms relevant for the application of these provisions, which could for instance provide concrete rules on how to obtain verifiable parental consent.

The issue of the protection of children also pops up in other provisions of the submitted proposal for a General Data Protection Regulation. Article 6 of the draft, on ‘Lawfulness of processing’, indicates that special consideration is to be given to the fact that interests of children might be at stake. Article 11, on ‘Transparent information and communication’, establishes that information must be adapted to the data subjects, especially if they are

---

12 For a sound analysis of the proposed provisions, see notably: María Belén Andreu Martínez (2013), *La protección de datos personales de los menores de edad*, Thomson Reuters, (Cizur Menor.


14 Idem.

15 Adopted and opened for signature, ratification and accession by the UN General Assembly resolution 44/25 of 20.11.1989.


18 See also Recital (38) of the proposed General Data Protection Regulation: ‘The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection’.
children. Article 33, on ‘Data protection impact assessment’, sets out that ‘personal data in large scale filing systems on children’ shall be considered as presenting specific risks. Article 38, on ‘Codes of conduct’, determines that codes of conduct shall take into account the specific features of the various data processing sectors, in particular in relation to ‘information and protection of children’.

One of the objectives of the proposed General Data Protection Regulation is to further harmonise the duties of DPAs in the different Member States. It thus describes with particular detail the authorities’ duties, and explicitly foresees they ‘shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data’. Furthermore, it adds that ‘activities addressed specifically to children shall receive specific attention’, which is a particularly important clause in the context of the ARCADES project.

In addition, the proposed General Data Protection Regulation vindicates the existence of a link between the ‘right to be forgotten’ and the protection of children. Indeed, the European Commission proposal includes a provision on the ‘Right to be forgotten and to erasure’, Article 17, according to which the right is granted ‘especially in relation to personal data which are made available by the data subject while he or she was a child’. Recital 53 clarifies that the right is ‘particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet’. The coherence between this idea and the proposed Article 8(1) is debatable, as on the one hand the proposed Regulation prohibits obtaining consent from children, and on the other it claims that the right to be forgotten is especially relevant for the cases in which consent has been obtained from children. A possible way to reconcile the two ideas is to think that Article 17 refers to children that are aged 13 or more (that is, able to give consent but still under 18).

After the introduction of the proposal of the European Commission, the EU Court of Justice asserted that the current EU legal framework on personal data protection, interpreted in the light of Article 7 and Article 8 of the EU Charter, already provides for the possibility for individuals to request that some pieces of information are not shown in the results displayed by search engine providers when searches using the individual’s name are made. Although the EU Court of Justice did not refer to this possibility as the existence of a ‘right to be forgotten’, the judgment answered a request for preliminary ruling submitted in the context of proceedings where the parties discussed the existence and applicability of such a right.

The proposed Regulation might not be adopted in the form put forward by the European Commission. It is nonetheless of high interest in the context of the ARCADES project.

---

19 See also Recital (46) of the proposed General Data Protection Regulation: ‘The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose. Given that children deserve specific protection, any information and communication, where processing is addressed specifically to a child, should be in such a clear and plain language that the child can easily understand’.

20 Article 52(2) of the proposed General Data Protection Regulation, COM(2012) 11 final, p. 78.


22 For a discussion of the conceptual weaknesses of protection of children in the context of the review of the EU personal data protection framework, see: Gloria González Fuster (2014), ‘How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection’, IDP Revista de Internet, Derecho y Política, N° 19, November 2014, p. 98.

23 Judgment of the Court (Grand Chamber) of 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12.
especially as it repeatedly stresses that children deserve ‘specific protection’. This notion of ‘specific’ protection is primarily declared as reinforced protection, that is, not a different type of protection, but manifesting in stricter rules. And, by alluding to the UN Convention on the Rights of the Child, the proposed draft signals the existence of a bridge between EU personal data protection law and children’s rights.

1.3. Rights of the children

The UN Convention on the Rights of the Child, of 1989, attests of a direct relationship between children’s rights and the protection of privacy. The Convention’s Article 16(1), indeed, establishes that ‘No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation’. Article 16(2) adds that ‘The child has the right to the protection of the law against such interference or attacks’.

These are not, however, the only provisions that might be significant in the context of children education on privacy and the protection of personal data. In this sense, the Convention on the Rights of the Child also sets down two particularly pertinent principles: the child’s best interest, and the respect for the views of the child. By virtue of the principle of the child’s best interest, the determining factor in all actions dealing with children should be their best interest, to take thus precedence over the interests of the adults concerned — although there is no clear consensus on how to determine in each case what is the best interest of each child. By virtue of the principle of respect for child’s views, children have the right to express an opinion and to have that opinion taken into account in any matter affecting them.

These two principles are echoed by the EU Charter of Fundamental Rights. Article 24(1) of the Charter establishes indeed that children ‘may express their views freely’, and that their views ‘shall be taken into consideration on matters which concern them in accordance with their age and maturity’. Furthermore, by virtue of Article 24(2), in all actions relating to children ‘the child’s best interests must be a primary consideration’.

1.4. Privacy and personal data protection culture

The described legal norms about privacy and personal data protection need to be put into the context of available information on how people perceive them, what they know about them and whether they actually use the rights they are granted and respect the obligations imposed of them.

For this purpose, the notion of ‘privacy and personal data protection culture’ is particularly useful.24 This notion stresses that individuals’ relationship with privacy and personal data protection is composed of different dimensions, which include: a cognitive dimension, related to what individuals know about privacy and personal data protection; an attitudinal dimension, regarding how they perceive those issues, and which are their feelings about them, and a behavioural dimension, concerning real practices, that is, what people actually do and do not do.

These three dimensions are intertwined and affect each other. For example, by changing the level of knowledge of individuals about privacy and personal data protection, it should be

24 On this concept, see notably: José Félix Muñoz Soro and Daniel Oliver-Lalana (2012), Derecho y cultura de protección de datos: Un estudio sobre la privacidad en Aragón, Dykinson, Madrid.
possible to alter their practices, but these will also depend on the image that individuals have about those issues.

All in all, it ensues that in order to reinforce somebody’s privacy and personal data protection it is not enough to provide them with more information. It might also be necessary to reorient their attitudes towards those issues, and to encourage them to undertake concrete actions. In line with this assessment, ARCADES aims to offer educational content contributing to the shaping of both informed and responsible attitudes towards personal data protection and privacy.

1.5. Compendium of key issues

The analysis of the described legal sources, read in the light of the need to support a multidimensional privacy and personal data protection culture, allows identifying which are the main points that should be conveyed to school pupils. The information to be transferred does not need to be limited to information that is directly applicable to them, but might also comprise general knowledge on privacy and personal data protection and their role in society. This can have an impact on the way in which they perceive those concepts. Furthermore, attention should be given to concrete actions that are in the hands of children.

The following table shows some of the key points that can be derived from an analysis of the legal framework:

<table>
<thead>
<tr>
<th>Key points</th>
<th>Legal references</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have a general right to privacy</td>
<td>Art. 7 EU Charter, Art. 8 ECHR</td>
</tr>
<tr>
<td>You have a right to the protection of your personal data</td>
<td>Art. 8 EU Charter</td>
</tr>
<tr>
<td>This right protects your personal data online, but also offline</td>
<td>Art. 8 EU Charter, Art. 3(1) of Directive 95/46/EC</td>
</tr>
<tr>
<td>The rights to privacy and to personal data protection are fundamental</td>
<td>Art. 7 and 8 EU Charter</td>
</tr>
<tr>
<td>Personal data are, for instance, your name, your telephone number, a picture of you</td>
<td>Art. 2(a) of Directive 95/46/EC</td>
</tr>
<tr>
<td>You have the right to know who is collecting and using data about you</td>
<td>Arts. 10 and 11 of Directive 95/46/EC</td>
</tr>
<tr>
<td>You have the right to know which data they have</td>
<td>Art. 12 of Directive 95/46/EC</td>
</tr>
<tr>
<td>You have the right to rectify the data if they are inaccurate</td>
<td>Art. 12(b) of Directive 95/46/EC</td>
</tr>
<tr>
<td>You have the right to refuse some usages of your data</td>
<td>Art. 14 of Directive 95/46/EC</td>
</tr>
<tr>
<td>When you accept to give data to somebody for a specific purpose, they cannot use them for something completely unrelated</td>
<td>Art. 6(1)(b) of Directive 95/46/EC</td>
</tr>
<tr>
<td>You cannot share personal data of other people without their consent</td>
<td>Art. 7(a) of Directive 95/46/EC</td>
</tr>
<tr>
<td>Data about your health, your sex life, your ethnic origin and your beliefs deserve special protection</td>
<td>Art. 8(1) of Directive 95/46/EC</td>
</tr>
<tr>
<td>You have the right to request that some results are not shown by search engines when somebody looks up your name</td>
<td>EU Court of Justice, Google Spain and Google, C-131/12</td>
</tr>
</tbody>
</table>
Your views must be taken into consideration on matters that concern you, in accordance with your age and maturity. Art. 24(1) of the EU Charter

In case of doubt, you can contact your data protection authority, or ask an adult to do it. Art. 28 of Directive 95/46/EC

Table 1 - EU privacy and personal data protection for children

2. General background

This section delineates the general landscape of European privacy and personal data protection education in schools, to help understanding some of the conditions and circumstances surrounding its deployment.

Although this report is centred on EU initiatives, it must nonetheless be mentioned that the interest for raising awareness among children and youngsters on privacy issues is also present beyond European borders. The United States (US), for instance, was one of the first countries to regulate online privacy protection, with the adoption in 1998 of the Children's Online Privacy Protection Act (COPPA),25 applying to websites that collect information from children under the age of 13. The US Federal Trade Commission (FTC) manages the website Online OnGuard,26 on safe Internet use, and also launched the website Admongo,27 aiming to educate children of ages between 8 to 12 about advertising.28

A particularly rich source of educational materials, including several presentation packages for teachers and parents, is the Office of the Privacy Commissioner of Canada’s youth privacy section.29 In Mexico, the Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) published in collaboration with the Canadian International Cooperation Agency the Montevideo Memorandum, on the protection of personal data in online social media, giving particular attention to children and youngsters.30 The IFAI has also a full website devoted to children and youngsters, Clic seguro.31

2.1. Council of Europe

Privacy and personal data protection of minors, as well as specifically privacy and personal data protection school education, has surfaced in different areas of action of the Council of Europe.

2.1.1. Building a Europe for and with children

The Council of Europe has developed a number of strategies focusing on children. In 2006, it launched the transversal programme ‘Building a Europe for and with children’. More concretely, the Council of Europe’s Strategy for the Rights of the Child 2012-15 aimed to help the organisation to fulfil its role as a catalyst for the implementation of the UN Convention on the Rights of the Child in Europe.

28 https://www.beesecure.lu.
29 https://www.priv.gc.ca/youth-jeunes/index_e.asp.
31 http://clicseguro.sep.gob.mx/.
Privacy and personal data protection appear however to have benefited only in a limited way from those efforts. A review of the achievements of the 2012-2015 Strategy pointed out that the Council of Europe’s Programme ‘Building a Europe for and with children’ had failed to deliver sufficient initiatives on ‘some of the more demanding issues such as children and the Internet, children’s use of newer information and communication technologies enabling them to better manage their privacy and personal data’.32

2.1.2. Human rights education

The Council of Europe has encouraged human rights education by actively supporting the production of relevant materials. It is also a key partner of other institutions granting much importance to human rights education such as the UN and the UN Educational, Scientific and Cultural Organization (UNESCO).33

In 2000, on the occasion of the 50th anniversary of the ECHR, the Human Rights Education Youth Programme of the Directorate of Youth and Sport of the Council of Europe launched COMPASS,34 a tool pursuing the development of human rights knowledge, skills and attitudes. One of the themes developed in COMPASS are the rights of children. In this context, much emphasis is put on the idea that children ‘can be exposed to a wide range of risks when they use the Internet’, and that this requires individuals to take action whenever they encounter illegal or dangerous material, but also more generally to work towards the empowerment of children and parents.35

COMPASS was accompanied by COMPASITO,36 a manual on human rights education for children aged from 6 to 13 years. One of the themes developed in COMPASITO is ‘Media and the Internet’, under which it is stressed that interactive media such as the Internet and mobile phones ‘produce additional dangers for children’ because ‘children may provide personal data that may be used for unwanted advertising and provide room for online predators’.37 COMPASITO also notes that children sometimes use ‘the unsupervised online environment’ for sending cruel messages and degrading photographs aimed at other kids, in cyberbullying practices that can be especially harmful because of online anonymity.38

In 2007 was first published Council of Europe’s Internet Literacy Handbook,39 now in its third edition. The Internet Literacy Handbook is a guide for teachers, parents and students on the Internet and online privacy. It is composed of a series of ‘Fact Sheets’. Fact Sheet Number 15 is specifically about ‘Privacy’, which it defines as ‘the degree of control that a person has concerning access to and use of personal information’. The Fact Sheet warns that privacy is eroding, and blames youngsters for this phenomenon:

34 http://www.eycb.coe.int/compass.
35 See Chapter 5 ‘Background Information on the Global Themes’, Section 5.1 ‘Children’ of COMPASS.
36 http://www.eycb.coe.int/compasito/.
37 Chapter V ‘Themes’, Section 9 ‘Media and the Internet’ of COMPASITO.
38 Idem.
‘Privacy is being increasingly undermined by the rapidity and ease with which youngsters can publish and/or stream digital images on Internet through Web 2.0 applications and via camera and mms facilities on mobile phones. A simple rule of thumb for youngsters: never publish anything you don’t want your teachers or parents to see!’

Fact Sheet Number 15 includes a set of ‘ideas for classroom work’, such as discussing the significance of privacy, learning how to create strong passwords, or exploring and comparing privacy settings in social networks sites.

The Council of Europe has also backed up the creation of an online game, *Through the Wild Web Woods*, designed to help children learn basic Internet safety rules. The game, which has been translated into more than 20 languages, targets children aged between 7 and 10.

### 2.2. European Union

Privacy and personal data protection are at the crossroads of different policy areas of EU action. Some of EU’s institutions’ commitments in this direction emanate directly from the Charter of Fundamental Rights of the EU.

#### 2.2.1. Promoting the EU Charter and privacy and personal data protection

As the right to privacy and the right to personal data protection are both rights enshrined in the EU Charter of Fundamental Rights, they both fall under the scope of the EU institutions commitments to the EU Charter.

The European Commission’s 2010 strategy for the effective implementation of the EU Charter of Fundamental Rights highlighted among its objectives to improve EU citizens' understanding of fundamental rights protection within the EU. In this sense, the European Commission stressed that it was particularly important to provide information on means of redress related to the rights of the child, as young people often express they do not know how defend their rights or who to turn to.

Surveys indicate that knowledge in EU Member States about existing personal data protection legislation is limited. According to a 2011 Eurobarometer survey, the majority of Europeans have not heard of their national data protection authority. In 2014, the Fundamental Rights Agency (FRA) of the EU published the results of a study on access to data protection remedies in EU Member States, which concluded that the general public needs to know more about data protection violations, existing remedies and support.

---

40 Fact Sheet # 15 of the Internet Literacy Handbook (Third edition).
41 ‘Create a basic knowledge framework for privacy with your class. Define concepts, both technical and social, and identify prejudices and myths for discussion’ (ibid.).
44 Ibid., p. 10.
45 Ibid., p. 11.
2.2.2. Promoting children rights

The Treaty of Lisbon introduced in 2009 as an objective of the EU the promotion of children's rights. Inside the European Commission, the Directorate General (DG) Justice acts as the children's rights coordinator of the different European Commission’s services dealing with related issues.

In its 2011 Communication An EU Agenda for the Rights of the Child, the European Commission expressed its commitment to the principle of ensuring that all EU actions are exemplary in the respect of the EU Charter and of the UN Convention on the Rights of the Child. As part of this agenda, it set up a child-friendly section of the EU website, the Kids' Corner online, and launched the European website on the rights of the child.

The 2011 EU Agenda for the Rights of the Child also stated that the European Commission ‘aims at achieving a high level of protection of children in the digital space, including of their personal data’, explicitly referring in this context to the review of the EU personal data protection legal framework, and noting that efforts to protect and empower children online are coordinated through the Safer Internet Programme.

2.2.3. Strategy for a Better Internet for Children

In 2012, the European Commission published its Strategy for a Better Internet for Children. This strategy is articulated around four main ‘pillars’: stimulating quality content online for young people; stepping up awareness and empowerment; creating a safe environment for children online; and fighting against child sexual abuse and child sexual exploitation. The responsible DG for this Strategy inside the European Commission is the DG Communications Networks, Content & Technology (DG Connect).

In the context of the pillar ‘Stepping up awareness and empowerment’, the European Commission’s Strategy noted that ‘[c]hildren, their parents, carers and teachers need to be aware of the risks children can encounter online as well as of the tools and strategies to protect themselves or cope with such risks’. The Strategy also pointed out that digital and media literacy and skills are crucial to the children’s use of the Internet, and that ‘it is necessary for online safety education to start in early childhood’. Observing that online safety as a specific topic was included in the school curriculum of more than 20 education systems across Europe, the European Commission stated that ‘[s]chools are best placed for reaching the majority of children, regardless of age, income or background, as well as other key recipients of internet safety messages, such as teachers and (indirectly) parents’.

According to the Strategy for a Better Internet for Children Member States should step up the inclusion of teaching online safety in school curricula by 2013, reinforce informal education about online safety and provide for ‘online safety’ policies in schools and adequate teacher

---

50 http://ec.europa.eu/.
52 Ibid., p. 2.
53 Ibid., p. 8.
54 Idem.
55 Idem.
training, as well as support public-private partnerships to reach these goals. The industry, in its turn, should engage in such private-public partnerships to support the development of interactive tools and platforms providing educational and awareness materials for teachers and children, building on existing initiatives. The European Commission specifically committed to support the identification and exchange of best practices among Member States in the areas of formal and informal education on online safety and to promote the creation of relevant educational content, and to back up public-private partnerships aimed at reaching out to children, parents, teachers and carers.

Under the pillar ‘Creating a safe environment for children online’, the Strategy for a Better Internet for Children explicitly referred to the review of the EU personal data protection legal framework, indicating that the European Commission’s proposal for a General Data Protection Regulation would take specific account of children’s privacy and introduce the ‘right to be forgotten’.

The Strategy for a Better Internet for Children is the follow up of the Safer Internet Programme, launched in 1999. Under this programme saw the light INHOPE, an International Association of Internet Hotlines, and the Insafe network. The Insafe network was founded in 2006, and brings together more than 30 national awareness centres, including, in addition to EU Member States, Iceland, Norway, Russia and Serbia. Every centre is entrusted to implement awareness and educational campaigns and run a helpline. The mission of the Insafe cooperation network is to empower children and young people to use the internet, as well as other online and mobile technologies, positively, safely and effectively. The Insafe Network eventually took up the Safer Internet Day campaign, an annual initiative initially launched by the European Commission, currently celebrated in more than 100 countries worldwide and supported also by the Council of Europe.

Insafe is coordinated by the European Schoolnet, a not-for-profit organisation networking more than 30 European Ministries of Education. European Schoolnet has set up also the eSafety Label, a European-wide accreditation and support service for schools aiming to develop and maintain high standards of e-Safety in schools across Europe. Its services include a system of accreditation, self-assessment, and personalised action plan, resources on e-Safety advice and guidance, and an online community.

In the context of EU’s support for a Better Internet for Children was also backed up the multinational research network EU Kids Online, seeking to enhance knowledge of European children’s online opportunities, risks and safety.

2.2.4. Other EU policies

EU action in other areas can also translate into the promotion of privacy and personal data protection education in schools.

---

56 To illustrate this, was given the example of Teach Today, [http://www.teachtoday.de/en/140_Home.htm](http://www.teachtoday.de/en/140_Home.htm).
57 [http://www.saferinternet.org/](http://www.saferinternet.org/). It must pointed out that the transition between the two programmes is on-going, and as a result the two names tend to coexist.
58 [http://www.inhope.org/gns/home.aspx](http://www.inhope.org/gns/home.aspx). This collaborative network brings together 51 hotlines in 45 countries worldwide, dealing with illegal content online and committed to stamping out child sexual abuse from the Internet.
59 [http://www.eun.org/home](http://www.eun.org/home).
60 [http://www.esafetylabel.eu](http://www.esafetylabel.eu).
61 [http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx).
The Directorate for Personal Data Protection of the Republic of Macedonia, DZLP, for instance, developed between March 2013 and March 2014 the project Sustainable system for continuous primary and secondary education for principles of personal data protection, co-funded by the EU in the context of its Programme for Macedonia. In the context of this project, the Macedonian Directorate for Data Protection organised on the for the Data Protection Day of 2014 an arts competition for primary school pupils under the motto ‘Privacy is mine, although I am a child’, and the Director of the Directorate for Personal Data Protection contacted Macedonia’s Minister of Education and Science with the aim of planning methodological units in primary and secondary education on privacy and the protection of personal data.\(^{62}\) The project resulted in the elaboration of materials for teachers of primary and secondary schools.\(^{63}\)

### 2.3. International cooperation of Data Protection Authorities

Other international initiatives have emerged in the context of coordination and cooperation between privacy and data protection authorities.

In 2009, the 1st Euro-Ibero-American Seminar of Data Protection devoted a full thematic area to the protection of minors, and included a panel on education of minors in privacy and personal data protection issues.\(^{64}\)

In 2013, the 35th International Conference of Privacy and Data Protection Commissions celebrated in Warsaw adopted a Resolution on Digital Education for All.\(^{65}\) The resolution was submitted by the French data protection authority, the CNIL.\(^{66}\) It recalls previous resolutions of the International Conference of Data Protection and Privacy Commissioners, and in particular a 2008 resolution, Children’s Online Privacy, which had been proposed by Canada’s Privacy Commissioner.\(^{67}\) The 2008 Resolution encouraged the Commissioners to develop digital education, especially for the youngest, noting that children and young people are often ‘unaware of their own legal rights’.\(^{68}\) It expressed support for ‘the development of education-based approaches to improving the state of online privacy, both locally and globally’, and encouraged educators ‘to recognize privacy education as fundamental to a child’s education and to include privacy education in their curricula’.\(^{69}\)

In Warsaw, the Commissioners agreed on adopting a common programme on digital education, based on five principles: 1) specific protection should be provided to minors with respect to digital technology; 2) lifelong training on digital technology should be fostered; 3) appropriate balance between the opportunities and the risks of digital technology should be looked for; 4) the development of good customs should be fostered and respect for other users should be promoted, and 5) critical thinking regarding the risks and benefits of digital technology should be fostered. The adopted common programme on digital education is to


\(^{63}\) Borivoj Kos, Nada Molerovic, and Ljubica Pendaroska (2013), *Прирачник За Наставници За Изучување На Заштитата На Личните Податоци (За Основно И Средно Образование)*, Sustainable System for Continuous Primary and Secondary Education for Principles of Personal Data Protection.


\(^{65}\) 35th International Conference on Data Protection and Privacy Commissioners, *Resolution on Digital Education for All*, Warsaw, 26 September 2013.


\(^{68}\) Idem.

\(^{69}\) Idem.
pursue four operational objectives: 1) promoting privacy education as part of digital literacy programs; 2) playing a part in training relay persons by organising or contributing towards ‘training of trainers’ on data protection and privacy; 3) promoting digital technology professions by promoting innovative sectors, especially sectors developing ‘privacy by design’; and 4) formulating recommendations and good practices on the use of new technologies for the concerned public.

As a follow up to the Resolution *Digital Education for All*, the CNIL proposed the creation of an International Working Group on Digital Education. This International Working Group is currently responsible for putting into effect the described operational objectives.

At EU level, the Article 29 Working Party, bringing together representatives of the data protection authorities of all EU Member States, has also been considering the issue of the protection of personal data of minors. It notably published in 2009 its *Opinion 2/2009 on the protection of children’s personal data (General Guidelines and the special case of schools)*, where it stressed that school comprises a significant part of children’s daily activities. The Opinion reviews applicable fundamental principles such as the already mentioned ‘best interest of the child’, observing that the child’s representatives should always apply it but that, in case of conflict between the interests of children and their legal representatives, the courts or, where appropriate, national data protection authorities, should decide. The document also emphasises that all children have a right to privacy and that this right and the right to personal data protection belong to children, and not to their legal representatives, who merely exercise them in certain circumstances.

3. A variety of practices

This section outlines existing initiatives in school education on privacy and personal data protection in the EU. First, it puts forward the heterogeneous panorama of national curricula. Second, it traces out national practices, presented using a typology that is not centred on national profiles, but rather on the different kinds of activities and materials that are developed in Europe.

3.1. Privacy and data protection in official curricula

Privacy and personal data protection are part of the official curricula in some EU Member States, but not in all of them. The following examples illustrate the heterogeneity of approaches.

- **In Poland**, knowledge about privacy and personal data protection, as well as the rules concerning safe use of the Internet, is an essential component of formal education. According to the Ordinance of the Minister of Education of 27 August 2012 on the core curriculum of pre-school education and general education in particular types of schools,
kindergarten children must know that all persons have equal rights, and higher levels of education must develop pupils’ attitudes determining effective and responsible functioning in the modern world. During Computer courses, students graduating from the 3rd class of primary school (8-9 years) should be made aware of the risks related to computer and Internet use; students from 4th to 6th class (9-11 years) must learn that while using a computer and ICT they should respect the privacy of others. Students of middle school (12-15 years) and high school (16-19 years) must be able to use efficiently modern information and communication technologies; at middle school level they are taught what are the human rights, while at the high school they should know human rights, recognise cases of violations of human rights and know how to protect them. These contents are transferred during Civic Education course. Computer lessons at middle school level cover more detailed knowledge on the social aspects of information processing, and on related legal standards.

- **In Slovenia,** consideration and respect for privacy and intimacy is already specified in the curriculum for kindergarten. Privacy and data protection are also substantially included in the elementary school curriculum. The contents are offered in the compulsory courses Civics and Ethics, where pupils learn about the right to privacy in the context of ‘The problems of modern society’, and optional elective courses Computer science and Media education. In the Computer science course, students notably have as a goal to recognise the importance of personal data protection. The Media education course includes discussing how journalists should respect personal privacy. At the level of secondary school, the geography curriculum for gymnasiums also encompasses digital competences, including the protection of privacy and respect for cultural differences, as well as developing willingness to respect the values and privacy of others. The sociology curriculum for gymnasium includes topics such as: the development of information science and technology and its impact on privacy, data protection, human rights and control. The information science curriculum for gymnasium contains the social aspect of information science in which students are asked to explain and evaluate the importance of security and data protection and privacy.

- **In Hungary,** personal data protection does not appear as independent subject in the national core curriculum, but are be incorporated into informatics and media awareness subjects, and privacy issues can also surface in history, social and civic competence, visual culture, and ethics.

- **In England, Northern Ireland and Wales,** personal data protection is a key element of the study of the Information and Communications Technology (ICT) legal framework, in the context of the General Certificate of Secondary Education (GCSE), a qualification taken by 15 and 16 year olds to mark their graduation from the Key Stage 4 phase of secondary education. As a component of this syllabus, students must study the UK Data Protection Act.

### 3.2. Classification of available materials and relevant activities

Existing materials and on-going activities related to privacy and personal data protection education in schools can be classified depending on the type of organisation responsible for them, and subsequently sub-divided in different groups depending on whether they have been

---

75 These details have been provided by the Slovenian Data Protection Officer in the context of the ARCADES project (December 2014).
76 In the 7th and 8th grade of elementary school.
77 Computer science is in the elementary school curriculum for the 4th, 5th and 6th grade.
78 These details have been provided by NAIH in the context of the ARCADES project (December 2014).
specifically designed for schools or are more widely created to be made available for children, youngsters, educators or parents through other means such as online distribution, or depending on their form.

The following section offers examples of the different types of materials and activities that can be encountered in the EU. It does not aim at being exhaustive, but rather to illustrate the current state (and diversity) of practices. Even if it focuses on EU cases, exceptionally it encompasses European but non-EU examples.

3.2.1. Materials and activities by data protection authorities

Many EU data protection authorities openly endorse an educational function, despite the fact that Directive 95/46/EC does not impose any obligation in this sense.

a) Data protection authorities targeting schools

In some cases, the direct focus of the activities of data protection authorities for (or at) schools are minors themselves. In other cases, the authorities’ efforts target primarily teachers, who will later reach the pupils. In other cases still, data protection authorities aim to influence school education professionals at a higher level, or responsible decision makers.

Focusing on pupils

- According to the French data protection authority, the Commission nationale de l'informatique et des libertés (CNIL), the right to privacy is one of the subjects most requested by pupils in French schools in the context of education on children rights. In 2013, the CNIL organised 291 visits to schools, reaching more than 30,000 children and youngsters.  

- The Greek data protection authority, HDPA, has organised since January 2005 awareness-raising seminars on the protection of personal data and Internet safety at primary and secondary schools.

- The Data Protection Commissioner of Rhineland Palatinate, Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz, has promoted since 2010 free workshops for schools. It is assisted in all its training activities by pedagogues.

- Activities primarily targeting pupils usually take place at schools, but in some cases pupils might be asked to attend special classes or workshops elsewhere.

- The Croatian Personal Data Protection Agency, AZOP, organised the initiative ‘Young personal data protection officer’, consisting of a series of workshops (with lectures, quizzes and educative games) taking place in public libraries, targeting primary school pupils. Children received an oath to sign in order to commit to keep the personal data of others safe.

---

80 www.dpa.gr/.
82 Ibid., p. 24.
The Polish data protection authority, Inspector General for Personal Data Protection (GIODO) organised in 2015 in cooperation with the Warsaw City Council classes for children entitled ‘My Data, My Treasure’, within the action ‘Winter in the City’, in Warsaw. GIDO representatives conducted 2-hours long workshops, during which pupils of Warsaw primary schools learnt about the importance of the protection of personal data and the respect for the right to privacy. The classes were also an opportunity to reflect on how to safely use modern technologies and how to consciously avoid online threats.

The Slovenian Information Commissioner published a brochure titled *Samoj ti odločaš* (‘Just for you to decide’) aimed at raising awareness of privacy and personal data protection issues among young people.86

Directed to teachers

The UK’s Information Commissioner’s Office (ICO) offers through its website a set of resources for schools.87 These resources include lesson plans developed by teachers and tailored to specific areas of the curriculum. There are three lesson plans for primary schools, titled ‘What is personal information?’, ‘Who needs to know? Why?’, and ‘Opting out’.88 And there are four plan lessons for secondary schools: ‘Strictly private? What is personal data?’, ‘Private versus public’, ‘Is there something I should know? Exercising your rights’ and ‘No secrets? Freedom of information’.89

The French data protection authority, CNIL, devotes a whole section of its website to teachers and education professionals.90 The section offers: two special interactive versions of *L’actu*, a journal targeting teenagers, but in special issues addressed to teachers (one is about geo-localisation and private life, the other is about privacy protection online); twelve ‘methodological sheets’ with essential information about a series of subjects (*Create a blog or a site*, *Share pictures*, *Register in a social network*, *Surf safely*, etc.);91 and thirteen ‘pedagogical sheets’ with teaching suggestions on different subjects: ‘The CNIL, what is it?’,92 ‘Internet, a new tool’,93 ‘Personal data’,94 ‘Intimacy and community’,95 ‘What is a friend on a social network?’,96 ‘Cyber-bullying or cyber-harassment’,97 ‘Mobile phones, geo-localisation and targeted advertising’,98 ‘Teen-marketing’,99 ‘Spam’,100 ‘School and privacy’,101 ‘Geo-localisation or the tracking of individuals’,102 ‘On-line reputation or e-reputation’,103 ‘Identity theft on the Internet’.104

---

86 The brochure can be downloaded from this link: [https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosura_koncna_otroci_CMYK.pdf](https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosura_koncna_otroci_CMYK.pdf)
87 [https://ico.org.uk/for-organisations/resources-for-schools/](https://ico.org.uk/for-organisations/resources-for-schools/)
88 [https://ico.org.uk/for-organisations/resources-for-schools/primary-school-lesson-plans/](https://ico.org.uk/for-organisations/resources-for-schools/primary-school-lesson-plans/)
89 [https://ico.org.uk/for-organisations/resources-for-schools/secondary-school-lesson-plans/](https://ico.org.uk/for-organisations/resources-for-schools/secondary-school-lesson-plans/)
90 [Surfer, ça s'apprend !](http://www.jeunes.cnil.fr/enseignants/).
- The Irish Data Protection Commissioner, in conjunction with the Curriculum Development Unit of the Department of Education and Science in Ireland, developed a resource for the Civic, Social and Political Education (CSPE) programme for Junior Certificate Students. The Junior Certificate is an educational qualification awarded to students who successfully complete the junior cycle of secondary education, and the CSPE programme aims to enable students to become active, aware and responsible citizens. The developed booklet, titled *Sign Up, Log In, Opt Out: Protecting your Privacy & Controlling your Data*,105 was distributed to all Irish secondary schools and is accessible via the website of the Irish Data Protection Commissioner.106 The booklet has four sections: ‘What is privacy?’, ‘Privacy as a Human Right’, ‘Rights and Responsibilities’, and ‘Technology’. Each section describes relevant aims, concepts, attitudes, knowledge and skills, and puts forward possible activities as optional exercises: these include ‘Follow-up Activities’ and ‘Ideas for Action’.107

- The Spanish Data Protection Agency, Agencia Española de Protección de Datos (AEPD), has made available to teachers an ad-hoc section on its website for minors, targeting also interested parents.108 The website turns around the campaign ‘The Pandi’, which follows everyday stories related to a group of friends, presented in the form of a comic. According to the AEPD, comics are a particularly suited medium for teaching in this area because they are attractive to minors and favour reflexion and critical thinking.109 The website offers six educational brochures, on the following subjects: personal data and privacy, rights and obligations and main risks online; digital identity and online reputation, social networks; pictures in web 2.0 services; email, chats and instant messaging; advertisement, shopping and online entertainment; and identity theft, cyber-bulling, grooming and sexting.110 Each brochure presents basic knowledge on the issues, references for further information, and suggested activities, typically aiming to generate a dialogue between pupils and teachers.

- In the Czech Republic, the Office for Personal Data Protection is responsible for an educational program titled ‘Protection of Personal Data in Education’,111 aiming at preparing teachers at elementary and secondary schools for topics in the area of personal data protection and enable their incorporation in the educational programs of individual schools.112 This program includes four lessons: one on the right to personal data protection within the framework of human rights and the Czech legislation, another on the subject of personal data protection in schools, and two on the possibilities of applying protection of personal data and privacy in the framework of specific subject. Its main

---

107 This booklet was later translated into Spanish with the support of the Spanish data protection authorities; the Spanish version is accessible here: [http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/menores/common/guia-educativa.pdf](http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/menores/common/guia-educativa.pdf).
target are teachers of Czech language and literature, basics of social sciences, history, mathematics, information and computer technology, and biology.

- In Belgium, the company Paco Producties, active in the area of educational theatre, has developed an education package for teachers on Internet safety and privacy, called ‘Net op het Net’. It targets children and teenagers between 10 and 12 years. Its core element is a play where three actors play the roles of people sharing experiences in a youth centre in an informal way. The package is available via the website of the Belgian data protection authority.

- The Hungarian National Authority for Data Protection and Freedom of Information (NAIH), is responsible for performing teaching activities in schools, and has also joined as observer to other teaching initiatives.

- The Polish data protection authority, GIODO, in cooperation with the Ministry of Administration and Digitization developed an educational set of materials for teachers called ‘How to discover cyber world safely’, destined for teachers. The developed educational and informational package outlines the most important issues regarding personal data and privacy protection and safe use of the Internet by children. The brochure comprises 7 themes: personal data protection, the right to online privacy, social networking sites, digital footprints, online communication, undesirable online actions and games.

- The Slovenian Information Commissioner published a brochure titled Vodič po varstvu osebnih podatkov za starše in učitelje (‘Guide to the protection of personal information for parents and teachers’) aimed at raising awareness of privacy and personal data protection issues among teachers.

Addressing education professionals in general

- In France, the French data protection authority, CNIL, led the setting up in 2013 of EDUCNUM, a collective for digital education bringing together 60 partners from the field of education, research, digital economy, civil society and political institutions. EDUCNUM notably delivers prizes celebrating works that raise awareness on safe use of

113 Specific educational goal: ‘ability to perceive the concept of privacy and personal data protection in various time periods on the basis of a literary text or a work of art’.
114 Specific educational goal: ‘personal data protection and protection of privacy in the context of human rights, law and psychology’.
115 Specific educational goal: ‘development of opinions on human privacy, its value and establishment of personal data protection in various time periods within the development of the European civilization, influence of totalitarian regimes on the perception of protection of privacy’.
116 Specific educational goal: ‘protection of personal data, their securing in automated processing – security within the Internet, principles of administration of computer technology with respect to data protection, danger of identity theft, modern equipment in personal data protection (tapping, RFID, database systems), principle of electronic signature’.
117 Specific educational goal: ‘possibilities of taking DNA samples, their subsequent processing for verification or identification purposes, different approaches to DNA databases in other countries, creation of databases of fingerprints and other personal identifiers, sensitive data in health care; human privacy – privacy of animals’.
118 www.pacoproducties.be.
122 The brochure can be downloaded from this link: https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/Brosura_učitelji_koncna_CMYK.pdf.
123 http://www.educnum.fr/.
the Internet. It has delivered prizes, such a Grand Prix du Jury prize to the video Les aventures croustillantes du Prince Chip, targeting children between 6 and 10 years; and a Prix Spécial du Jury for Data Fiction, a game for the 12-18 range.

- Catalonia’s data protection authority, Autoritat Catalana de Protecció de Dades (APDCAT), celebrates each year since 2009 an event on personal data protection and Internet safety of minors, co-organised with the Catalan Department of Education. The event targets school directors and education professionals in general, who are invited to discuss issues related to personal data protection in schools.

Reaching decision makers

- In France, the French data protection authority, CNIL, launched a campaign, together with other organisations, asking for ‘digital education’ to be recognised official as a French ‘great national cause’.

- The Hungarian data protection authority, NAIH, contributes to the National Cyber Security Coordinative Committee, Working Group for the Protection of Children Rights set up in 2013 by the Hungarian government. A subgroup of this Working Group is fully devoted to discussing education matters.

- Outside the EU, the National Centre for Personal Data Protection of the Republic of Moldova signed in December 2013 a cooperation agreement with the Moldovan Ministry of Education, with the view combining efforts aimed at a sustainable system of continuous training of students and education personnel regarding personal data protection. The Act signed by both parties strives for mutual exchange of information, the gradual implementation of training programs for teachers, and the integration of personal data protection in the national pre-university curriculum.

- Also outside the EU, in Albania, the Commissioner for Personal Data Protection signed in 2011 a cooperation agreement with the Minister of Education to raise awareness on personal data protection among children, students, teachers and parents.

- The Polish data protection authority, GIODO, in cooperation with the Centre for Education Development (public teacher training institution run by the Minister of National Education) is currently developing a publication titled ‘Personal data protection: Guide for the principal of the school’, which will constitute the basis of professional preparation of the school principals in the field of personal data protection. The guide will present the key issues related to the data controller’s role and proper personal data processing in schools as an element of good management of the institution.

Targeting parents

Some activities of data protection authorities aim to raise awareness on privacy and personal data protection issues among parents.

124 https://racontr.com/projects/les-aventures-croustillantes-de-prince-chip/
125 http://www.thomas-thibault.fr/portfolio/datafiction/.
- The French data protection authority, CNIL, has collaborated with an organisation representing families, UNAF, and an NGO for the protection of youth, Action Innocence. Jointly they launched a study on practices of minors aged between 8 and 17, and published in 2011 an informative brochure for parents.\textsuperscript{131}

**Targeting multiple actors**

The mentioned sub-divisions of categories of activities and materials for schools are not always clearly distinguishable.

- In 2008, the Portuguese data protection authority, Comissão Nacional de Protecção de Dados, launched the DADUS project to introduce data protection into school curricula, following an Agreement with the Ministry of Education and the Education Regional Authorities for Azores and Madeira.\textsuperscript{132} It targeted children from 10 to 15 years old, and was supported by a dedicated site hosting a manual for teachers and supporting materials.\textsuperscript{133}

- The Polish data protection authority, GIODO, organises yearly (and since 2009) a two-day seminar for teachers in the context of the educational programme ‘Your data – Your concern: Effective protection of personal data. Educational activity addressed to students and teachers’, often with the collaboration of local authorities and stakeholders. The main objective of the programme is to involve in initiatives increasing awareness on the need of personal data protection school communities and local communities such as media and public institutions. Special activities take place to celebrate the Data Protection Day, under the responsibility of participating institutions but with the support of GIODO. Activities of the programme ‘Your data – Your concern’ target teachers but also parents, as well as students.

Catalonia’s data protection authority, Autoritat Catalana de Protecció de Dades (APDCAT), has launched the project ‘Menors, Internet i Tecnologies’.\textsuperscript{134} This project unfolds in two phases. The first phase takes place in a number of selected schools, to which are provided materials to work with pupils. Data protection experts and APDCAT collaborators take care of a first information session directed to pupils. On the same day, but later, another information session welcomes families and teachers to give them more information on the details provided to the pupils, and to answer their questions. In a second phase, a congress will bring together involved pupils and experts.

**b) Other data protection authorities activities targeting minors**

Data protection authorities efforts to raise the awareness of minors on privacy and personal data protection issues sometimes take paths different than those of school education.

**Online resources**

Data protection authorities sometimes devote part of their online presence to targeting minors. In some cases, the resources are recommended not only for the personal use of children and youngsters, but also for their use in an educational context.

\textsuperscript{132} Article 29 Working Party (2009), Twelfth Annual Report, p. 81.
\textsuperscript{133} The DADUS website is currently undergoing maintenance: http://www.cnpd.pt/bin/dadus/dadus.html.
\textsuperscript{134} http://www.menorsiprivacitat.cat/.
Although surfaced outside the EU, the Norwegian initiative Du Bestemmer (‘You Decide’) has been particularly popular across Europe. Du Bestemmer was launched in 2007 and is a collaboration between the Norwegian data protection authority, the Norwegian Centre for ICT in Education and the Norwegian Board of Technology. You Decide is also supported by the Norwegian Directorate for Education and Training. You Decide consists of a website, dubestemmer.no, which contains factual information, practical examples, discussion exercises and videos, as well as physical booklets and posters. It is available in Bokmål, Nynorsk, Sami and English. Booklets for the youngest age group are translated into Urdu, Somali and Arabic. Materials prepared in the context of You Decide have reached many EU countries, as well as non EU-countries. Part of its material was translated in 2009 by Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein; The Finnish National Board of Education created web pages in Finnish and Swedish.

Belgium designed a campaign indirectly inspired in the Norwegian You Decide, under the Flemish and French names of ‘Je décide’ and ‘Ik beslis’. This campaign, supported by the Belgian data protection authority, centres on a website with four different tracks for different target audiences: a) thematic pages for children (on mobile phones, advertisement, Internet, social media) with a survey and a quiz; b) thematic pages for youngsters (on mobile phones, advertisement, Internet, social media and images), with a quiz; c) thematic pages for teachers (text on CCTV, e-ID, mobile phones, privacy at schools, Internet, advertisement, social media), and shorter texts on different subjects by Dr Buzz (‘a very funny scientist’) and Miss P@otte (‘a trendy auntie’), and d) thematic pages for parents: the same subjects, with a slightly different content.

In Finland, the Finish data protection authority contributes to the Safer Internet Day activities, which in that Member State last for one week and take the shape of a Media Literacy Week. Every year, new content is developed for the Media Literacy Week by all participating institutions. Materials include for instance documentation for teachers to teach children about the online use of pictures, including practical exercises.

In Germany, the Federal and Länder Data Protection Commissioners shared a youth portal, Young Data. The site includes information about personal data protection targeting youngsters. The website refers children to the Datenschutz section of the Internet ABC portal, where can be found material targeting children.

The French data protection authority, the CNIL, has put online an interactive video titled ‘Share the party’. In this video, viewers enter a party and are invited to take a series of decisions on whether to share or not to share online some of the images they see. If they chose to share them, they will see a final scene where the persons involved are arguing, in distress, and even, in one case, taken away by the police. If they chose not to share anything, they will receive some negative comments by a friend. The video aims to raise awareness about the importance of protecti

---

135 Translation into German of the booklet for Ages 13-17, available here (pdf).
136 Sinä päätät.
137 Du bestämmer.
138 Je décide.
139 Ik beslis.
140 Dr Buzz page.
141 Miss P@otte page.
143 http://www.mediataitokoulu.fi/mediataitoviikko-3/.
144 http://www.youngdata.de/.
146 http://www.jeunes.cnil.fr/jeunes/share-the-party/.
awareness among teenagers between 13 and 18 of the potential negative consequences of sharing some pictures.

- The Spanish data protection agency, AEPD, has a website specially targeting minors, *Tú decides en Internet* (‘You decide on Internet’).\(^{147}\) The website revolves around a comic strip about a group of friends using different information technologies, *The Pandi*.\(^{148}\) It includes a test evaluating general knowledge about good personal data protection practices,\(^{149}\) and links to pedagogical material for teachers.\(^{150}\) The basic message of this website is that minors must decide by themselves how they behave online, but that they must do so knowing the consequences of their decisions: ‘*Es tu mundo. Tú decides en él*’ (‘It is your world. You decide’).\(^{151}\)

- Catalonia’s data protection authority, Autoritat Catalana de Protecció de Dades (APDCAT), launched in 2011 the campaign ‘A Internet, controles?’.\(^{152}\) The campaign consisted of four basic elements: a guide for minors on the Internet (*La Guia de menors a Internet*), a manual on good practice online, a set of informative sheets, and a video (in short and long versions). The APDCAT also offers an online test for children to evaluate their knowledge to ‘navigate safely’ through the Internet,\(^{153}\) and another on personal data,\(^{154}\) and has a section for children and youngsters, called ‘Privacy for the young’.\(^{155}\)

- In Greece, the Greek data protection authority (HDPA) created in 2011 a special section of its website devoted to teaching privacy and personal data protection issues to children and youngsters.\(^{156}\)

- The website of the Hungarian data protection authority, NAIH, has a page devoted to children and youth.\(^{157}\)

- The Polish data protection authority, GIODO, takes active part each year in the celebration of the Safer Internet Day organised in Poland by the Research and Academic Computer Network by participating in special fairs and in the scientific conference. During the fairs, GIODO makes available educational materials devoted, *inter alia*, to safe use of the Internet, such as special leaflets for children or brochures from a series named ‘ABC of personal data protection’.

Sometimes the ‘minors’ section of data protection authorities’ websites are however not targeting children and youngsters directly, but rather just summarising efforts undertaken in that direction.\(^{158}\)


\(^{149}\) [http://www.tudecideseninternet.es/menores/?q=node/212](http://www.tudecideseninternet.es/menores/?q=node/212).


\(^{155}\) The section is formally accessible in English, Spanish and Catalan, but only the Catalan version offers full content.

\(^{156}\) [http://www.dpa.gr/portal/page?_pageid=33,96295,33_96308|33_96321&_dad=portal&_schema=PORTAL](http://www.dpa.gr/portal/page?_pageid=33,96295,33_96308|33_96321&_dad=portal&_schema=PORTAL).


Media campaigns

- In Hungary, the Hungarian National Authority for Data Protection and Freedom of Information, NAIH, rolled out in spring 2014 a media campaign turning around a song and video by a popular Hungarian singer, Tamás Vastag.159 The song is called ‘Egy biztos hely’, which means ‘A safe place’, and aims to warn youngsters of the dangers of an unlimited and wary Internet use.160 NAIH’s media campaign was followed by a TV spot161 and a radio advertisement162 calling attention to the facts and dangers of online activities and the importance of data protection settings.

Competitions

A special type of awareness-raising initiatives are competitions on the subject of privacy and personal data protection. They can involve children and youngsters directly, or through their schools. They might be organised online or offline.

- The Irish Data Protection Commissioner organised in 2008 and 2009 video competitions on privacy issues, in the context of the Data Protection Day.163 The 2008 competition was about 'Privacy In The 21st Century', and the 2009 one was titled ‘Private I, Public Eye’.

- In Italy, the Italian Garante per la Protezione dei Dati Personali awarded on the 2012 Data Protection Day to videos prepared by pupils on the subject of privacy. The competition was open to pupils of the third and fourth grades (teenagers).164 For the 2010 Data Protection Day, the Garante organised the projection of four privacy-related to films.165

- The Bulgarian Commission for Personal Data Protection organised a competition titled ‘Me and Internet’ through a popular children portal. Children aged between 4 and 17 contributed with pictures, essays and poems.166

- Within the framework of the programme Your Data – Your Concern, the Polish data protection authority, GIODO, awards each year prizes to participants who have shown special commitment in the competitions. Two competitions are organised: one for pupils aimed at encouraging them to become interested in this issue and to present their thoughts thereon in a creative way in the form of info-graphics, and another for institutions, aimed at granting distinctions and awards to schools and teacher training institutions which undertake the most interesting activities for the benefit of dissemination of knowledge on personal data protection among pupils and teachers.167 GIODO has also conducted three editions of a fine art contest for students: ‘Privacy around me’, ‘Privacy protection in the world without borders – Schengen’, and ‘Personal data protection in contemporary world’.

160 The video is accessible on YouTube: https://www.youtube.com/watch?v=gc8s581LJws.
164 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1804368.
166 Working Group of Data Protection Authorities on Digital Education (2014), pp. 11-12.
167 More information on the competition can be found at http://www.giodo.gov.pl/1520208/id_art/8539/j/pl/.
Other awareness-raising activities

- The Belgian Commission for the Protection of Privacy sent in 2012 posters and postcards aiming to raise privacy awareness among young people to public libraries.\(^{168}\)

- Catalonia’s data protection authority, APDCAT, is present at events for children and youngsters, such as children and youth fairs.\(^{169}\)

- The Commission for Personal Data Protection of Bulgaria printed two educational leaflets containing advice and guidelines for children and parents related to safe Internet behaviour. Copies of these leaflets were distributed to the Ministry of Education and to regional education inspectorates.\(^{170}\)

- The Croatian Personal Data Protection Agency, AZOP,\(^{171}\) made public in May 2014 an educational poster on hate-speech, elaborated in collaboration with private companies.\(^{172}\)

- The Italian data protection authority, the Garante per la Protezione dei Dati personali, published on the occasion of the 2014 Data Protection Day a report on institutional communication campaigns.\(^{173}\)

b) Other data protection authorities’ activities revolving about the protection of minors

Data protection authorities also engage in other reflexive or exploratory activities on the subject on privacy and personal data protection and minors, including research efforts.

- The Croatian Personal Data Protection Agency, AZOP, participated in a study launched in 2010 to analyse the perception of privacy and personal data protection by children and youth,\(^{174}\) in the framework of the EU’s Leonardo da Vinci programme.

- The Hungarian data protection authority, NAIH, carried out a study on the safe and conscious Internet use of children (‘Key to the world of the net! Promoting legally conscious internet use of children by means of fundamental rights protection measures’), which was published in 2013\(^{175}\) and included materials targeting minors. Also with the name ‘Key to the world of the net!’, NAIH initiated in 2013 a long term programme focusing on children’s rights from a privacy and data protection perspective.\(^{176}\)

- In 2010, the Polish data protection authority, GIODO, has been selected to realise a study visit co-funded with EU funds within the framework of the Study Visits Programme, part of the Lifelong Learning Programme. The objective of the visit was the exchange of information and experience related to the ways and methods of providing knowledge on

\(^{168}\) Ibid., p. 10.

\(^{169}\) Ibid., p. 12.

\(^{170}\) Ibid., p. 29.


\(^{174}\) http://www.azop.hr/cpage.aspx?page=print.aspx&PageID=139. The study was set in motion together with the Hungarian and Polish data protection authorities.


\(^{176}\) http://www.naih.hu/key-to-the-world-of-the-net-.html.
personal data protection addressed to children and youth. Moreover, during the meeting the possibility to introduce educational programmes in primary-, middle- and high schools was analysed, and the most effective form of education in this field was discussed.

3.2.2. Materials and activities by other organisations

In addition to the initiatives led by data protection authorities, there are also relevant practices.

a) Developed in the context of the Safer Internet / Better Internet for Kids Programme

Much work has been developed with the support of Insafe, the European network of awareness centres promoting safe, responsible use of the Internet and mobile devices to young people. Although the prime objective of Insafe is not specifically to educate on privacy and personal data protection, its activities touch upon many related issues. Sometimes, Insafe national centres and data protection authorities work together.

- Saferinternet.at, the information and coordination centre for safer Internet use and media competence in Austria, develops free school resources and booklets. An example is the 2011 report *Schutz der Privatsphäre im Internet. Erst denken, dann klicken. Unterrichtsmaterialien*. This is an extensive document (82 pages), primarily targets teachers and students of Austrian secondary education. It includes a FAQ section on data protection at schools, a chapter on the significance of privacy, a chapter on the Internet, a chapter on rights and obligations, a chapter on tips on how to protect privacy, exercises and a final selection of ten key recommendations. Saferinternet.at is led by the Austrian Institute of Applied Telecommunications (OIAT) in cooperation with the association of Internet Service Providers Austria (ISPA).

- In Luxembourg, Safer Internet activities are coordinate by the BEE SECURE initiative. A representative of the data protection authority of Luxembourg, la Commission Nationale de la Protection des Données (CNPD), stands on BEE SECURE advisory committee. They produced together a leaflet on online personal data protection for youngsters.

- In Slovenia, the Center for Safer Internet Safe.si is responsible for website with educative content and workshops for primary school and high school children and their parents. On the safe.si website are published ten ‘golden rules’ aimed at young people for the safe use of the Internet, and e-learning materials for teenagers. The website has a special section on ‘My identity and privacy on the Internet’.

- At EU level, the European Schoolnet has published *The Web We Want: Teachers online – Handbook for educators*, a handbook supported by Insafe, two private companies

---

177 [https://www.saferinternet.at/](https://www.saferinternet.at/)
178 [Saferinternet.at (2011), Schutz der Privatsphäre im Internet. Erst denken, dann klicken. Unterrichtsmaterialien (Mit Übungen für den Unterricht), Österreichisches Institut für angewandte Telekommunikation (ÖIAT).](https://www.saferinternet.at/)
180 [http://safe.si/](http://safe.si/)
(Google and Liberty Global) as well as the European Commission.\textsuperscript{182} The document presents lesson plans on different Internet-related issues, prepared by teachers for teachers.\textsuperscript{183}

c) Other

- In Belgium, the Kenniscentrum Mediawijsheid\textsuperscript{184} brings together partners working on tools and initiatives to enhance media literacy in Flanders. One of its partners, MIOS,\textsuperscript{185} a research group within the Department of Communication Studies at the Faculty of Political and Social Sciences of the University of Antwerp, develops tools to inform and sensitize parents, teachers and youth workers on different issues such as privacy and online contact risks. In April 2014, MIOS researchers authored a guide for parents, teachers and other adults involved in the education of young people entitled ‘Mediawijs Online’.

- In Slovenia, Amnesty International Slovenia published in 2009 a guide to teach human rights containing model lessons that are applicable to all rights, and which includes the right to privacy. Additionally, the project ‘My rights’ was devoted to the promotion of knowledge and education on children’s rights (including the right to privacy), based on the long-term and systematic coordination of governmental and non-governmental organizations School for Peace, Amnesty International, Slovenian Association of Friends of Youth, the National Education Institute of the Republic of Slovenia and the Human Rights Ombudsman of the Republic of Slovenia. The project targeted pupils aged between 6 and 15, and was implemented by teachers in elementary schools. Another relevant project is Education as a Strategic Method Against the Illegal Use of Internet (ESMAIUI), undertaken by the company B2 and the National School of Leadership in Education, Institut ISA: this project, about the education and training of children, parents and teachers on the safe use of information and communication technologies, runs the so-called Internet self-defense school\textsuperscript{186} and has conducted lectures and workshops touching upon personal data protection.

- In Hungary, the Hungarian National Authority for Data Protection and Freedom of Information, NAIH, has several times joined as observer teaching activities in schools organised in the context of the Okosdigitális Programme.\textsuperscript{187}

- In Spain, the NGO Padres 2.0 is responsible for educational campaigns on online safety including privacy and personal data protection issues.\textsuperscript{188} The Spanish association of privacy professionals, Asociación Profesional Española de Privacidad (APEP), has launched a guide on minors for parents and educators.\textsuperscript{189}

\textsuperscript{182} The document is available here: http://www.webwewant.eu/web/guest/handbook-for-educators;jsessionid=FDD36B50EF8673BFCC11053688EA17D2.
\textsuperscript{183} It was preceded by The Web We Want: Young and Online – Activities by young people for young people, also by the European Schoolnet, available here: http://www.webwewant.eu/documents/10180/18685/Handbo ok_for_web+lght.pdf/11922503-f1c3-45a4-817d-0795cf0b199.
\textsuperscript{184} http://mediawijs.be/.
\textsuperscript{186} http://www.internetna-samoobramba.si/izvedba-izobrazevanja/.
\textsuperscript{187} http://okosdigitalis.hu/.
\textsuperscript{188} http://padres20.org/.
\textsuperscript{189} María Arias Pou et al. (2015), Cuestiones y recomendaciones básicas para padres y educadores sobre el uso de redes sociales e Internet por los menores, Guías APEP nº 1, Asociación Profesional Española de Privacidad (APEP), http://www.apep.es/presentacion-de-la-gui a-de-menores-apep-para-padres-y-educadores/.
4. Analysis of teaching materials

This section enters into the analysis of available materials. This examination aims to facilitate the preparation of ARCADES documents, that is, two sets of lesson-based materials. To do so, it looks for commonalities in existing practices but also pursues the identification of aspects in which there might be discrepancies, or a diversity of approaches.

This analysis first discusses the material’s aims, afterwards examines their formal features, and finally addresses the content.

4.1. Aims

A common feature of existing materials is that they generally do not simply aim to transfer knowledge to minors, but rather to support learning and reflection, in order to promote a reflexive, responsible use of new technologies – and in particular of the Internet. The Norwegian initiative Du Bestemmer, for example, self-describes as a resource about privacy and ‘digital responsibility’.

Not all initiatives related to privacy and personal data protection education are primarily concerned with these two issues. In some cases, these are issues that emerge in the context of teaching about concomitant subjects, such as online safety. When this occurs, the information related to privacy and personal data protection might be affected by the emphasis put on online safety.

Privacy and personal data protection, on the one hand, and online safety, on the other, are subjects that partially overlap, but are not fully coincidental. In this sense, it is true that being prudent online is important to guarantee the protection of children’s privacy and personal data, as it is also unquestionable that being aware of privacy and personal data protection will contribute to the online safety of minors. Having said that, to a certain extent the conceptual grounds on which some online safety education is based clearly differ from the European legal notions of privacy and personal data protection.

In the field of online safety, the mere sharing of personal data is sometimes envisioned and presented as a risk. From the perspective of privacy and personal data protection law, however, the processing of personal data is in principle not a problem in itself (except in special cases, for instance when sensitive data is at stake), but rather the trigger of the applicability of a series of obligations for data controllers, and what will prompt the coming into being of a series of subjective rights. Therefore, unlike in the online safety discourse, data subjects are supposed to be in a position of trust, rather than of general distrust.

In many cases, emphasis is put on teaching pupils how to reinforce their own (personal) privacy and personal data protection, as data subjects. Teaching materials do not always attempt to provide pupils a complete picture of what privacy and personal data protection entail, for instance by entering the issue of what are the obligations of data controllers. This, however, can also occur. The UK’s ICO resources for schools openly aim to help children

---

190 See, for instance, the tutorial made available online by the Spanish data protection agency, AEPD, http://www.tudecideseninternet.es/educadores/introduccion0.
191 See, for instance: Sonia Livingstone and Leslie Haddon (2009), EU Kids Online: Final Report (EC Safer Internet Plus Programme Deliverable D6.5), The London School of Economics and Political Science, p. 1: ‘Giving out personal information is the most common risky behaviour’.
192 https://ico.org.uk/for-organisations/resources-for-schools/.
and young people better understand the value and importance of their personal information, know how to look after it, and understand the obligations that organisations have.

4.2. Tools

Only some of available materials pursue the provision of full lesson plans for teaching about privacy and personal data protection. Often, educational materials made available might consist in elements that can be integrated into lessons, such as comics, brochures, posters or videos, for instance. Other components might be a glossary, practical examples, or key legislation.

4.2.1. Lesson plans

Lesson plans typically accommodate different types of documentation, and different kinds of activities. Activities might include general information, practical examples, discussion exercises, individual exercises, or suggestions for homework.

The materials offered by UK’s ICO, for instance, are designed to allow teachers flexibility in their approach and to encourage active learning, with opportunities for student talk, discussion and questioning.

The lesson plans might integrate special background information for the teachers, but this knowledge can also be provided through other resources such as online resources.

4.2.2. Other elements

Materials such as videos, quizzes, or comics can be directly integrated into lessons plans, or made available to teachers in case they consider it appropriate to integrate them. These types of materials have the key advantage of being in principle more attractive for minors than plain text. They might have also, however, some drawbacks. In general terms, audio-visual materials might rapidly start to look out of fashion, or not in full concordance with the technological realities that surround minors, which change particularly quickly.

Videos

An important number of videos have been developed over the years with the aim to illustrate the risks of Internet or mobile use, showing to children or youngsters what could happen due to the misuse of their personal data. Videos seem to be used primarily to trigger emotional reactions by pupils, but might not always allow conveying concrete information about which uses of personal data are legitimate, and which are not.

The video for the song ‘Egy biztos hely’, by Tamás Vastag, promoted by the Hungarian data protection authority, NAIH, shows at the beginning some happy teenagers enjoying life. Two girls discuss, using their mobile phones, and one of them posts her phone number to a social media platform. After this, a man starts harassing her, and will later assault her. In parallel, a boy takes a selfie in front of his new car. Before the end of the video, he is violently attacked and his car is stolen. In a similar vein, a video titled ‘The Postman’, made available online through the Du Bestemmer, a Norwegian initiative, tells the story of a girl

193 Idem.
194 https://www.youtube.com/watch?v=gc8s581LJws
who, just before leaving school, posts an online message to a friend telling her she is feeling unwell and will stay home in the evening. The message is read by a man, who is able to obtain the girls’ address through a public directory. In the evening, the man goes to the girls’ house to sexually assault her. 195 This kind of material can certainly have an impact on the perceptions of the minors on the importance of privacy and personal data protection, but should be accompanied with information as to what practices are problematic and which are legitimate.

Test and quizzes

Test and quizzes are also relatively popular tools. They can be used to motivate pupils to pay attention to the subject and learn more, or as pedagogical devices, which allow pupils to learn while they play. When this is the purpose, it is key for the test to make sure that the minors’ misconceptions are timely tackled, as otherwise they will not be able to understand what is wrong.

An online test offered by the Spanish data protection agency, AEPD, for example, consists of six questions that need to be answered consecutively before arriving to the results. 196 Users only discover at the end whether they answers were wrong, and even then they are not systematically granted an explanation as to why they were wrong, or on which was the correct answer.

The Hungarian data protection authority, NAIH, uses a quiz 197 with 15 questions, which aims to call children’s attention to privacy issues. The quiz has been elaborated within the ‘Key to the world of the net!’ programme, and the study 198, that includes it. NAIH introduces the quiz during teaching in schools and other programmes, where its representatives can also explain the data protection relevance and meaning behind each questions.

4.3. Target audiences

The purpose of ARCADES is to deliver two distinct sets of materials, one targeting pupils aged 6 to 13, and the other minors above 13. To mark the distinction between these two basic groups, a possibility is to refer to the first group as ‘children’ or ‘kids’, and to describe the second as ‘teenagers’. In practice, it is quite common for existing educational materials in this area to be divided similarly in two different groups, also on the basis of the targeted audience, but generally the two main audiences are referred to as ‘children’, on the one hand, and ‘youngsters’, on the other.

In its 2/2009 Opinion, nonetheless, the Article 29 Working Party stressed that ‘according to the criteria in most relevant international instruments’, a child is someone under the age of 18, but only unless they have acquired legal adulthood before that age. 199

In the initiatives that have different tracks for different ages, tracks generally share common features. The Du Bestemmer resources, for example, target minors aged 9-18 years; one of its tracks addresses ages 9 to 13 years, covering the subjects ‘Privacy’, ‘Social Media’,

---

‘Cyberbulling’ and ‘Source Criticism’, and the other focuses on ages 13 to 17 years, covering ‘Privacy’, ‘Social Media’, ‘Cyberbulling’ and ‘Digital Trails’. Materials should always be generally adapted to the target group they are aiming to reach.

4.4. Content

The content presented in available materials can envisaged as a series of issues falling under a set of general subjects. This section reviews these subjects and issues providing concrete examples that illustrate how they are presented, including extensive quotes from some of the resources available in English. Not all EU materials address each and every subject listed here, but most of these are undoubtedly recurrent.

It is important to note that a great number of available materials do not explicitly distinguish privacy and personal data protection. Often they use the term privacy to also refer to personal data protection.

4.4.1. Introducing privacy and personal data protection

Privacy and personal data protection can be introduced to pupils in many different ways. The Irish booklet Sign Up, Log In, Opt Out, intended as an introduction to the general idea of privacy, starts addressing privacy in a home environment and then moves on to other settings such as Big Brother and the relationships between celebrity and privacy. That section is followed by a second on how privacy became enshrined as a human right, a third on data protection legislation within a national and global context, and a last one where the focus switches to technology and the implications of innovation for privacy. This structure aims specifically to allow the ‘[d]evelopment of a sense of why privacy is important and why it should be respected’ and an ‘awareness of rights’. In terms of knowledge, pupils are expected to learn ‘How privacy can be defined’, ‘Dangers of interference or violation of a person’s right to privacy’, ‘How removing privacy can affect those otherwise materially privileged’, and the fact that ‘Privacy is a human right’.

a) The significance of privacy and personal data protection

The Sign Up, Log In, Opt Out booklet devotes special attention to explaining why privacy is nowadays enshrined as a human right. It explains that the emergence of this right is partly a reaction against Hitler’s Nazi regime, and that data was used by the Nazis to create sophisticated population identification systems. This is connected to a discussion of population of census and of identity cards. After an excerpt of Anne Frank’s diary, the booklet notes that eventually ‘[p]eople saw the destructive power that information could have in the hands of an evil government and how information gathered for one purpose could be re-used for a wide range of sinister purposes’, which led to the recognition of the right to privacy.

201 Sign Up, Log In, Opt Out, p. 3.
202 Idem.
203 Sign Up, Log In, Opt Out, p. 21.
204 Ibid., p. 24.
Similarly, materials supported by Saferinternet.at draw pupils’ attention to the fact that the protection of privacy plays an important role for the functioning of democracy.\textsuperscript{205} And the \textit{Du Bestemmer} resources stress the link between privacy and personal data protection and freedom:

‘This is about freedom. If someone was monitoring and following your every move, or if someone could see everything that was stored about you, perhaps you would change the way you behave. Or?’ \textsuperscript{206}

Reflections on the importance of privacy and personal data protection can also be linked to reflections on the significance of the Internet or of social media in modern societies. For instance, the \textit{Du Bestemmer} initiative proposes the following ‘Discussion’ exercise:

‘Some people think that children should not belong to social networking sites.
- What do you think?
- What are the advantages of belonging to a social networking site?
- Are there any disadvantages?
- Should an age limit apply to social networking sites and why?
- Some large social networking sites apply an age limit of 13. What do you think about this?’\textsuperscript{207}

Discussion exercises can also engage with the question of the importance of privacy. For instance:

‘Adults and children, individuals and famous people all have a right to privacy.
- Why do you think privacy is so important?
- Are there places or situations where we have a greater need to be left in peace? What are they?’\textsuperscript{208}

Or see the following example of ‘individual exercise’:

‘Privacy is a right that is important to respect.
- Do you tell everyone you know about what you think and feel, or are there some people you tell more than others?
- What do you tell different people and why do you tell some more than others?
- Do you think that you and the other pupils in your class have different limits for what you share with others? If this is the case, what are the differences, and why do you think this is the case?
- In what situations do you think privacy is even more important? What information do you think is important to keep to yourself?’\textsuperscript{209}

\textit{b) Surveillance}

As an element of the introduction or concluding a lesson or lesson plan, pupils can be invited to think about the erosion of privacy, and the dangers of surveillance.

The \textit{Du Bestemmer} resources invite pupils to reflect on CCTV:

\textsuperscript{205} Saferinternet.at (2011), p. 11.
\textsuperscript{206} Du Bestemmer online resources, ages 13-17, Privacy track. \url{http://www.dubestemmer.no/en/13-17-ar/privacy}.
\textsuperscript{207} Du Bestemmer online resources, ages 9-13, Social Media track. \url{http://www.dubestemmer.no/en/9-13-ar/social-media}.
\textsuperscript{208} Du Bestemmer online resources, ages 9-13, Privacy track. \url{http://www.dubestemmer.no/en/9-13-ar/privacy}.
\textsuperscript{209} Du Bestemmer online resources, ages 9-13, Privacy track. \url{http://www.dubestemmer.no/en/9-13-ar/privacy}.
‘Camera surveillance is increasing, both in private and public places.
- Would you behave differently if you knew that you were being filmed?
- Do you think it is OK that someone is always watching what you do?
- Give five examples of when camera surveillance would be OK/not OK.’ ²¹⁰

The Irish booklet Sign Up, Log In, Opt Out devotes a section to Big Brother, aiming to ‘provoke students into thinking about ways in which the government in a different type of society or state could curtail individual freedoms including the right to privacy’. ²¹¹ It introduces George Orwell’s 1949 Nineteen Eighty-Four book and suggests an activity where students have to rate different ‘orwellian’ conditions according to their severity, on a scale of 1-10. These conditions include ‘You are forbidden to keep a diary’, ‘A flat-screen TV in your living room broadcasts government propaganda 24 X 7. You can lower the volume slightly but you can never turn the TV off or change channel’, or ‘It is a crime to fall in love’. ²¹²

4.4.2. What is privacy

‘Privacy is the right to be left alone and to live one’s life with the minimum of interference’, summarises the booklet Sign Up, Log In, Opt Out. This basic idea is supported in the document by some reflections on three aspects of privacy: ‘the right to be let alone’ (or the privacy of the home), ²¹³ ‘personal documents’ ²¹⁴ and ‘personal belongings’. ²¹⁵ The make pupils think about the notion of private spaces, teachers are invited to compare intrusions in the private space with the damage caused by burglars. ²¹⁶

The Du Bestemmer materials offer this definition of privacy:

‘We all have things we don’t want to share with others. Not because they are illegal or because there is something we need to hide, but simply because they are private. Privacy means that you have a right to a private life.’ ²¹⁷

Privacy, however, is often presented as mainly related to information, and more specifically about the control of personal information online.

4.4.3. What is personal data protection

The Du Bestemmer resources offer this summary of what is personal data protection about:

‘The more digitalised our everyday lives become and the more information about us that is stored, the more important it becomes for us to know what is stored, who can see the

²¹¹ Sign Up, Log In, Opt Out, p. 9.
²¹² Ibid., p. 10.
²¹³ ‘As the evening draws in, we draw the curtains in our homes. We block out the approaching darkness and turn on the lights’, Sign Up, Log In, Opt Out, p. 4.
²¹⁴ ‘We also like to keep some of our personal documents private’, idem.
²¹⁵ ‘Other items in our possession are of sentimental value’, idem.
²¹⁶ ‘Burglars enter houses and take physical belongings or damage items. However intruding on someone’s privacy and becoming aware of their habits, monitoring their activities and listening to their conversations can be just as damaging in the long run’ (Sign Up, Log In, Opt Out, p. 5).
information and how it is used. You have a right to know what information is stored about you and why.\(^{218}\)

Personal data are described this way:

‘What are personal data? Personal data are data that can be associated with a particular individual. This means, for example, that your name, address and telephone number are your personal data. Pictures where you can be recognised are also personal data.\(^{219}\)

The section on data protection of the Irish booklet *Sign Up, Log In, Opt Out* starts with an ‘Activity’ for students where they are asked to divide into groups of five and think together about what type of information is held by different institutions relating to an individual, and why. Concretely, they must complete a questionnaire indicating which information could hold (and why) organisations such as a phone company, a bank, a supermarket, the school, the chemist, the Department of Education and Science, or the Department of Health and Children.\(^{220}\) Teachers are provided a completed questionnaire listing which type of information is held by each organisation.\(^{221}\)

There exist a very limited number of resources highlighting that the right to personal data protection has currently the status of fundamental right in EU law. The European Schoolnet’s *The Web We Want: Teachers online – Handbook for educators* includes a Worksheet inviting students to read the whole Charter of Fundamental Rights of the EU and identify important rights for the use of Internet. Right after that, the Worksheet lists three rights of the EU Charter that deserve particular attention, and asks students to revise the booklet in their light: human dignity as enshrined in Article 1, respect for private life as in Article 7, and freedom of expression as in Article 11.\(^{222}\) There is, however, no mention of Article 8, on the protection of personal data.

### 4.4.4. Protect your data

A key message in many available resources is that children and youngsters must take steps in order to keep their personal data safe. For instance:

‘Look after your information: Mobile phones, tablets and computers store a lot of personal information about you and your friends. If unauthorised persons obtain your information, they can use it in ways that could be very unfortunate for you. It is therefore very important that you look after your devices and information as best you can.’\(^ {223}\)

This general recommendation can be accompanied by more concrete advice such as:

‘Tips for securing your mobile:
- Use a lock on your screen (password, privacy pattern, PIN code or similar)
- Use a SIM card code that has to be entered every time the phone is switched on
- Ask an adult before you install new apps. They can help you check the app

---


\(^{220}\) *Sign Up, Log In, Opt Out*, p. 32.

\(^{221}\) Ibid., p. 33 and 34.


- Never leave your phone or other devices unattended without locking the screen
- Never share your passwords or codes with anyone. 224

Another issue often tackled is privacy settings in social media. 225

Also in relation to social media the issue of the use of pseudonyms typically surfaces. In this context, materials generally recommend the use of a nickname in some circumstances, but take the opportunity to remind minors that other Internet users might also not be using their real name. Additionally, minors might be advised to use a ‘good’ nickname when using one – that is, a nickname that does not reveal any personal information. 226

The Du Bestemmer materials propose the following ‘discussion’ exercise:

‘In many situations on the Internet you can use a nickname instead of your full name.
- How many in the class have online profiles where you use your own name and how many have profiles where you use a nickname?
- Discuss the consequences of having a nickname.
- Do you think you behave differently when you use a nickname than you do if you write something under your full name? Why/why not?
- In what situations might it be better to use a nickname and in what situations might it be better to use your full name?’ 227

In some cases, recommended practices appear to go beyond normal usages. Resources supported by the Belgian Privacy Commission, for instance, advise minors to create two email addresses and use each of them for distinct functions, for example one for games, and the other only for school purposes. 228

Some available resources discourage the use of cloud computing services to store certain types of data. For instance, a ‘practical example’ from the Du Bestemmer materials reads as follows:

‘Cloud accounts hacked: A right-wing politician circulated naked pictures of young girls on the Internet. He had obtained the pictures from the girls’ iCloud accounts. They didn’t even know that the pictures had been stolen and published. This shows that you cannot trust that your personal data is secure when stored in a cloud.’ 229

4.4.5. Decide, and decide wisely

A message very frequently stressed in available materials is that children and youngsters should think carefully whenever they decide to share or allow access to personal data. Here, the main point is that many decisions are in the hands of minors, who shall act as responsibly as they can.

For instance, in the words of the Du Bestemmer resources:

224 Ibid.
‘We are all responsible for safeguarding our own information to the best of our abilities. It is important that you take control of your own information and don't share it indiscriminately. You should think about what you share, and with whom, and you should never share other people's personal data without asking their permission first. Ask questions when someone wants your personal data. Why do they want it and what are they going to use it for?’

Taking bad decisions can have negative repercussions. This ‘practical example’ is provided:

‘Contacted by unknown adults: Ambre (14) had an unpleasant experience when she was nine years old and visited a website for children. She posted her phone number although she knew she should not. She was then contacted by several unknown men who both phoned her and sent messages. Ambre found this really unpleasant and at first she didn't dare to tell her parents. She was afraid that they would get angry because she had posted her phone number - which she wasn't allowed to do. Luckily her father discovered what was happening and could help her. Since then, she has been much more careful about what information she posts about herself.”

a) How to consent genuinely

Resources insist that, in many cases, individuals can consent to or refuse the processing of their personal data. They also provide information on when can minors give consent, and when the responsible adult must give consent. For instance:

[In Norway] ‘From the age of 15 you can agree that your personal data can be collected and used. If you are under 15, those who wish to use your personal data must normally have permission from your parents. If it concerns personal data of a ‘sensitive’ nature (for example criminality, health, sexuality, etc.) your parents' permission is usually required until you are 18.”

Some resources explain that children cannot decide on their own whether to give or not to give some personal data because they are too young, and thus incapable of evaluating what represents a risk and what does not. Children should thus always consult their parents.

The Du Bestemmer materials note that even when consent is not to be provided by the minor, but by the parents, the parents should explore and consider the minor’s views.

‘An explicit yes: A person who wishes to post pictures and other information about you online, must first have your permission. If you are under 15, your parents have to give permission. You should therefore discuss with them what they think that others should be able to share about you online and what should not be shared.’

This seems particularly consistent with the guidance provided by the Article 29 Working Party on personal data protection and children. According to the Working Party, for consent ‘the solution can progress from mere consultation of the child, to a parallel consent of the child and the legal representative, and even to the sole consent of the child if he or she is

---

234 Idem.
already mature’. This is asserted on the basis that children gradually become capable of contributing to decisions made about them, and that as they grow they should participate more regularly to the exercise of their rights.237

b) Consent can be revoked

Some available materials underline that the fact that consent to personal data processing has been given does not mean that the consent cannot be revoked. For instance:

‘If you or your parents change your minds afterwards, you just have to say so. The person who posted the picture or information is then required to remove it immediately.’238

4.4.6. Do not share without consent

Teaching materials often stress that privacy and personal data protection law oblige children and youngsters to respect some obligations, and notably to ask for other people’s consent before sharing online personal information about them.

For instance, the Du Bestemmer materials state:

‘Online files: If you would like to post pictures of your friends online you need to ask them first. If you have a picture of a friend on your mobile and wish to share it with others, you also have to ask first. Because even if you think the picture is funny and innocent your friend might not think so. And your friends also have a right to privacy.’ 239

Similarly:

‘When you have an online account, you are responsible for the information you post on it. You are responsible for what you may and may not publish about others, and you are also responsible for what you should and should not publish. Something that might seem OK to you to publish, might not seem OK to someone else. If you would like to post pictures of your friends online you need to ask them first. If you have a picture of someone on your mobile and wish to send it to someone else, you also have to ask first. Because even if you think that the picture is funny and innocent your friend might not think so. This also applies to information about other people. You cannot write anything you want about other people, even if you have a blog etc.’240

To further stress this point, it is suggested to carry out the following ‘individual exercise’:

‘It has become very easy to share pictures, both online and by using your mobile and various applications.
- Has anyone ever published a picture of you on the Internet?
- Did you think that was OK? Why/why not?
- Did they ask you first?
- Could you imagine situations where someone would not like or should not have pictures and other information about themselves published on the Internet?’ 241

---

237 Idem.
239 Idem.
4.4.7. Internet does not forget... yet?

Much emphasis is placed by available materials on the idea that once information is shared online it is difficult to take it down, or even to control who else will use it.

For instance:

‘If you belong to a sports team or theatre group or something similar, it is possible that pictures of you have been posted online. Perhaps you are so good that you have been interviewed by a newspaper and the article has been posted online. Many schools also post pictures online. And perhaps you have a blog or something similar? It is important to understand that any information that has been posted about you online can be downloaded by others and stored in various places.’ 242

More concretely, often the attention of pupils is brought to the fact that much data can be made quickly accessible to anyone searching for their names. For example:

‘If someone searches your name on Google, they can form a picture of who you are as a person on the basis of the results they get. In a way you can say that in time everyone will have their own file online.’ 243

An exercise often recommended for children and youngsters to check which results are obtained when a search is made using their name. In this sense:

‘Many are surprised about how much information is available about them on the Internet.
- Google your own name. Did you get any hits?
- If so, did you know that this information about you had been published?
- Was it you or someone else who published the information?
- Did they ask your permission first?
- Do you think the information gives a correct impression of you?
- Did you find anything you did not like and that you wish could be deleted?’ 244

The exercise ‘Ich im Netz” proposed by Saferinternet.at aims to help pupils recognise the importance of Internet privacy and of avoiding undesired online content, as well as to get a sense of how quick and easily can be obtained personal information on the Internet. It has two phases: first, pupils are invited to imagine that they have an internship at a company and that they have been asked to play the role of personnel managers and have to obtain as much information as possible doing searches based on their name; in this context, they should also note the results that actually concern other people with the same name. In a second phase, they should get together in small groups and discuss how easy it was to obtain data, whether they have found any unexpected information, the possible impact of the available data, and how to avoid negative implications. As a possible variant it is suggested that the teachers could give their names as fictional candidates, but only if they have previously checked the information available online. Possible related homework could be to write an essay on digital traces on the Internet. 245

The majority of resources available were elaborated before the Court of Justice of the EU ruled in May 2014 that EU law allows data subjects to require search engines not to show certain results when searches using their names are carried out. The prerogatives asserted in

242 Idem.
243 Idem.
244 Du Bestemmer online resources, ages 13-17, Privacy track, http://www.dubestemmer.no/en/13-17-ar/privacy.
that judgment, regarding the removal of links with data that is inadequate, irrelevant or no longer relevant, appear to be however of the greatest significance for children. In this sense, the Article 29 Working Party has noted that as children are ‘developing’, the data relating to them change, ‘can quickly become outdated and irrelevant to the original purpose of collection’, and should be deleted when this happens.  

4.4.8. Parents

Parents are generally there to help pupils protect their privacy and personal data protection. They can also, nevertheless, play an active role in undermining their children’s rights and freedoms. This might notably occur if they monitor their children too closely, or if they share too easily personal data related to their sons or daughters. Discussing these issues with pupils has the key advantage of touching upon a subject that is close to their daily lives, and which can be of direct interest.

The Norwegian Du Bestemmer resources place particular emphasis on the need for children to be heard, also by parents. For instance, it can be read:

“When you are born, your parents have control over information about you and how it is used, but as you grow up they should listen to your own views on privacy.”

Control upon personal information is described as increasing with age:

“Privacy means that you should have the right to decide about information about you. The decision about what information to share and with whom to share it should be yours to an increasing extent as you grow up. According to the UN Convention on the Rights of the Child, all children have a right to privacy. The older you are, the more your opinion should count.”

a) Surveillance by parents

The level of acceptable interference of parents into the private life of children can nevertheless change depending on the circumstances, and some practices that are deemed intrusive in some contexts might not be regarded as such in others. There is, in this sense, room for debate, which can be encouraged:

‘Good to check up on you? Some parents check their children's computer logs and browser history to see what websites they have visited. Some also ask to see their children's mobiles to read messages that the children have sent or received. Many parents say they do this because they don't want their children to experience things they might find unpleasant. Other parents do not think it is appropriate to check their children's computers or mobile phones. What do you think?’

The Du Bestemmer resources illustrate this subject with practical examples such as the following:

‘Monitoring children's Internet use: There is software that helps parents monitor their children's Internet use. A filter can be installed on your PC that lets your parents see everything you do on the Internet, including what websites you visit. The Ombudsman for

248 Idem.
Children is sceptical about this and feels that this would be the same as reading your children's diaries. Children have a right to privacy and it is better to use discussion and dialogue to teach them about safe behaviour on the Internet.  

‘My mum and dad store my chat logs! I don't like it. Because when I talk to boys and hope it might lead to something, I don't really dare write that I like this boy, since my mum and dad will notice that he and I are flirting. It would be really embarrassing if my mum and dad read 'Oh, I love you SOOOO much' or 'You're hot and I'm not' and things like that. It is really embarrassing. Do you think it is OK that my parents store my msn chat logs? Regards from a 12-year-old girl’.  

‘Monitors daughter’s spending: A mother has explained that she gives her daughter pocket money which she puts into her account. She then checks her daughter's statements from the bank regularly and knows exactly when and where her daughter has used the money.’  

Discussion activities and individual exercises are proposed to explore pupils’ views on these subjects and whether they have agreed any rules with their parents.

Some available resources, however, take a different approach by unambiguously asserting that parents have a general right to read any text messages on the mobile phones of their children. In this sense, material supported by the Belgian Privacy Commission argues that children cannot refuse their parents full access to their phones, adding that this is not about controlling them but about caring for them. Resources targeting teachers and parents might emphasise that parents are generally responsible for the actions of their children in the terms described by law, not only offline but also in relation to their online activities.  

**b) Over-sharing parents**

A specific problem that children might have with their parents relates to overexposure in social media of children’s pictures or videos, which the later might find embarrassing or inappropriate. The *Du Bestemmer* resources emphasise that in these cases parents should not decide on their own whether the pictures can be shared, but should take into account the children’s views, even if they are minors:

‘The UN Convention on the Rights of the Child states that all children have a right to respect for their privacy, family, home and correspondence. It also states that you have a right to express your views and to be heard. This means that children's and young persons' views on privacy are important. For example, if you don't want your parents to publish pictures of you on social networking sites, they should respect this.’

The following fact is provided as an example to generate reflection and discussion:

‘2-year old had her own Instagram profile: One of Norway’s best known bloggers created an Instagram profile for her 2-year old daughter. In March 2014 the profile had 26,000 followers.’

---

250 Idem.
251 Idem.
256 Idem.
Additional arguments are provided in reference to national legislation:

‘In Norway we also have a Children's Act which gives children the right of co-determination as they grow up. This means that children shall be taken seriously and that their parents shall listen to their opinion, for example when they wish to publish information or pictures of the child on the Internet. Your opinion is important, even if you are a child.’

The message that parents’ sharing of personal data is to be controlled is certainly consistent with other subjects such as reminding children that it is extremely difficult to exercise control on personal data shared online.

4.4.9 Schools

Addressing privacy and personal data protection issues related to the school also provides a concrete setting for pupils to locate these issues. The Du Bestemmer materials tackles the question of what practices are permissible at schools:

‘What are schools allowed to check? Schools are normally not allowed to monitor pupils' use of the Internet. However, the school can use the logs to check unwanted activities on their network. Activity of this kind does not have to be illegal. It could be that someone uses too much of the school's resources to download music or other files that use up a lot of memory.’

They observe that information is a key issue:

‘Schools should limit their surveillance of the pupils and should inform them and their parents about what information they record and why.’

In this sense, the following activity is suggested:

‘Find out what rules apply at your school. Do you agree with these rules? Propose your own rules and present them to the head teacher.’

4.2.10. Take action (if necessary)

Available resources typically observe that in some cases children and youngsters might be entitled to take action in name of their rights to privacy and personal data protection.

a) Use your personal data protection powers

The Irish booklet Sign Up, Log In, Opt Out offers a chart of ‘rights and responsibilities’ related to personal data protection, followed by an ‘Activity’ where students are confronted with eight imaginary scenarios involving personal data processing. For each scenario,

---

258 Idem.
260 For instance: ‘Brian attends an outdoor concert and avails of a free call card offering €15 worth of mobile calls. He fills out a few details about himself on a card in order to receive the free credit. He is now receiving texts about all sorts of offers and holiday deals’, Sign Up, Log In, Opt Out, p. 48.
students are invited to decide whether any further action is required or not, and whether any enquiries or objections might be appropriate. The introduction to the exercise points out that ‘[t]here is no definitive answer for any of these scenarios as not all the facts are known’, but nevertheless the teacher is expected to talk through the answers.\footnote{Ibid., p. 47.}

Some teaching materials detail how to use the right to access, and how, if necessary, contact the data protection authority for assistance.\footnote{Saferinternet.at (2011), p. 27.}

\textit{b) Know how to react in case of serious problem}

Resources generally grant much attention to the possibility that minors realise that some particularly embarrassing or problematic data has been posted online. In that case, it is essential that they know they can ask somebody for help, and that they know whom to turn to.

The \textit{Du Bestemmer} resources observe:

‘Ask for help: If someone has posted information about you online without your permission, or information that you don't want to be public, you can tell the person who has published it. If that person does not remove the information, or if you feel uncomfortable about contacting this person yourself, you should talk to an adult (parent, teacher, nurse, etc.) about it. You have a right to have the information removed. If you don't like it, you should say so, even if it was your parents or your school that published the pictures of you. If you don't know any adults who can help you, there are others who can. For example Slettmeg.no\footnote{Slettmeg.no (‘deleteme.no’) is a service from the Norwegian Centre for Information Security (NorSIS) to help people who experience privacy violations online. It offers advice and guidance to people of all ages who find offending material about them on the Internet. Offending material might be photos published without permission, fake profiles on different Internet services, incorrect personal information or harassment.} can help and advise you how to remove unwanted information from the Internet.’\footnote{Du Bestemmer online resources, ages 9-13, Privacy track, \url{http://www.dubestemmer.no/en/9-13-ar/privacy}.}

The possibility to call the police is also explicitly mentioned:

‘If you feel that the information that has been published about you is so extreme that it must be removed quickly, you should contact the police where you live. Take a screen shot. Report the situation!’\footnote{Du Bestemmer online resources, ages 13-17, Privacy track, \url{http://www.dubestemmer.no/en/13-17-ar/privacy}.}

This approach contrasts with other cases where emphasis is placed on the idea that online information is there to stay, and no concrete advice is given on how to request the removal of data. For instance, material supported by the Belgian data protection authority offers a fatalistic view on the possibility of actually removing data that has been shared, presumably to invite minors to think carefully before they share it.\footnote{Je décide, Jeunes (Youngsters), social media thematic section, \url{http://jeunes.jedecide.be/jeunes-qu-on-m-enleve-ca}.}

\textit{c) Do not fall into blackmail}

The possibility of being blackmailed is openly discussed in some available materials. For example:

\begin{itemize}
\item \textit{Du Bestemmer} online resources, ages 9-13, Privacy track, \url{http://www.dubestemmer.no/en/9-13-ar/privacy}. \footnote{\textit{Du Bestemmer} online resources, ages 9-13, Privacy track, \url{http://www.dubestemmer.no/en/9-13-ar/privacy}.}
\item \textit{Du Bestemmer} online resources, ages 13-17, Privacy track, \url{http://www.dubestemmer.no/en/13-17-ar/privacy}. \footnote{\textit{Du Bestemmer} online resources, ages 13-17, Privacy track, \url{http://www.dubestemmer.no/en/13-17-ar/privacy}.}
\item \textit{Je décide}, Jeunes (Youngsters), social media thematic section, \url{http://jeunes.jedecide.be/jeunes-qu-on-m-enleve-ca}. \footnote{\textit{Je décide}, Jeunes (Youngsters), social media thematic section, \url{http://jeunes.jedecide.be/jeunes-qu-on-m-enleve-ca}.}
\end{itemize}
Online blackmail: An increasing number of people are being blackmailed to avoid pictures or videos of them being published online. The most common situation is where someone has been tricked into taking their clothes off on Skype. That person then gets blackmailed by someone who threatens to post the video from the call on YouTube or other social media sites unless the person pays up, takes more pictures or undresses in front of the camera. If this happens to you, the best thing is to contact an adult, for example a parent, teacher, nurse or the police, as quickly as possible, even if it feels embarrassing. Paying usually doesn't stop the blackmail so ask for help immediately before it gets worse!  

4.2.11. Meet your data protection authority

Some materials introduce to pupils the relevant data protection authority, describing its main functions and what it can do for them.

5. Concluding remarks

The value of privacy and personal data protection education has been recognised in many policy areas and at various policy levels. Taking privacy and personal data protection education to schools offers many advantages. It most notably allows reaching out a large number of minors, including those that might be less familiar with new technologies or with their rights and freedoms, and thus more vulnerable.

Data protection authorities can play a crucial role in ensuring that information that is provided at schools is in full accordance with applicable legal provisions. The aim of ARCADES is, on the grounds of the present state-of-the-art report and through the cooperation of data protection authorities, to produce fully legally compliant and effective educational materials with EU-wide relevance. On the basis of the gathered knowledge, the consortium will prepare a set of materials that will be tested in a series of seminars with teachers.

Bibliography

30th International Conference on Data Protection and Privacy Commissioners, Resolution on Children’s Online Privacy, Strasbourg, 17 October 2008.

35th International Conference on Data Protection and Privacy Commissioners, Resolution on Digital Education for All, Warsaw, 26 September 2013.

Andreu Martínez, María Belén (2013), La protección de datos personales de los menores de edad, Thomson Reuters, Cizur Menor.

Arias Pou, María et al. (2015), Cuestiones y recomendaciones básicas para padres y educadores sobre el uso de redes sociales e Internet por los menores, Guías APEP nº I, Asociación Profesional Española de Privacidad (APEP).


268 Du Bestemmer online resources, ages 9-13, Social Media track.
269 For instance, introducing the Austrian data protection authority: Saferinternet.at (2011), p. 29.


Kos, Borivoj, Nada Molerovic, and Ljubica Pendaroska (2013), Прирачник За Наставници За Изучување На Защитата На Личните Податоци (За Основно И Средно Образование), Sustainable System for Continuous Primary And Secondary Education For Principles Of Personal Data Protection.


EU Fundamental Rights Agency (2014), Access to data protection remedies in EU Member States, Vienna.


Livingstone, Sonia and Leslie Haddon (2009), EU Kids Online: Final Report (EC Safer Internet Plus Programme Deliverable D6.5), The London School of Economics and Political Science.

Muñoz Soro, José Félix and Daniel Oliver-Lalana (2012), Derecho y cultura de protección de datos: Un estudio sobre la privacidad en Aragón, Dykinson, Madrid.


TNS Opinion & Social (2011), *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, European Commission,

Working Group of Data Protection Authorities on Digital Education (2014), *Table of results and fact findings from the questionnaire on digital education: Overview of the resources provided by 36 contributions to the 3 questions – classified by regions and main topics*, 1 September 2014.