Gloria González Fuster and Dariusz Kloza (eds.)

The European Handbook for Teaching Privacy and Data Protection at Schools

EAP

THE EUROPEAN HANDBOOK FOR TEACHING PRIVACY AND DATA PROTECTION AT SCHOOLS

THE EUROPEAN HANDBOOK FOR TEACHING PRIVACY AND DATA PROTECTION AT SCHOOLS

Edited by

Gloria González Fuster
Dariusz Kloza

EAP

This book was prepared in the context of the project Introducing Data Protection and Privacy Issues at Schools in the European Union (ARCADES, www.arcades-project.eu/) running between November 2014 and May 2015 and co-funded by the Fundamental Rights and Citizenship Programme of the European Union, managed by the Directorate General Justice and Consumers of the European Commission (grant agreement JUST/2013/FRAC/AG/6132).

Disclaimer: The contents of this book do not necessarily reflect the views of the European Commission.

ISBN 978-1-78068-423-9
D/2016/7849/110
NUR 822

Cover illustration by Femke Vanhellemont © 2016, based on a photo taken by Nina Jelen © 2016. Illustrations: p. 79: Tomasz Soczyński – p. 92 and 93: Anže Novak

British Library Cataloguing in Publication Data. A catalogue record for this book is available from the British Library.

ACKNOWLEDGEMENTS

This book is indebted to the numerous teachers, education specialists, external privacy and data protection experts and professionals, privacy activists, policy makers, children and youngsters, who have provided support and encouragement during the unfolding of the ARCADES project.

In particular, we are extremely grateful to the members of the International Data Protection Working Group on Digital Education, coordinated by Pascale Serrier (*Commission Nationale de l'Informatique et des Libertés* (CNIL)), the Polish Gliwice Education Centre (*Gliwicki Ośrodek Metodyczny*), and Kirsten Fiedler (European Digital Rights (EDRi)) for their precious feedback on the Teacher's Manual. For their invaluable contribution to the ARCADES Final Conference, we are indebted to the *Autoritat Catalana de Protecció de Dades* (APDCAT) and Eticas Research & Consulting. For their help at various stages of the project, we would also like to thank European Schoolnet, Aída Barquero and the Centre for IT Education and Computer Applications in Warsaw (*Ośrodek Edukacji Informatycznej i Zastosowań Komputerów* (OEIiZK)).

Last but not least, we would like to express our sincere gratitude to all the pupils and teachers who participated in the lesson plan competitions – only a few could win, but they were all inspiring.

The ARCADES team

CONTENTS

PART I.
THE PRIVACY AND DATA PROTECTION EDUCATION LANDSCAPE

PART II.
THE TEACHER'S MANUAL

LIST OF ABBREVIATIONS

ARCADES	Introducing Data Protection and Privacy Issues at Schools in the European Union
CNIL	Commission Nationale de l'Informatique et des Libertés
DG	Directorate General
DPA	Data Protection Authority
EU	European Union
GDPR	General Data Protection Regulation
GIODO	Generalny Inspektor Ochrony Danych Osobowych
IP RS	Republika Slovenija Informacijski pooblaščenec
IT	Information Technologies
LSTS	Research Group on Law, Science, Technology and Society
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság
NGO	Non-Governmental Organisation
OEIiZK	Ośrodek Edukacji Informatycznej i Zastosowań Komputerów
VUB	Vrije Universiteit Brussel

FOREWORD
WHY ARCADES?

Wojciech Rafał Wiewiórowski*

There is no doubt that technology has an enormous impact on today's society and on economic development. There is no doubt either that the new generations of young people feel much more comfortable in the new Information Technologies (IT) world than their parents and grandparents. The increasing use of mobile, 'smart' devices and apps to collect information at an intensive rate and the substantial imbalance between providers of such devices and apps, on the one hand, and the consumer, on the other, are both part of the same story. These trends define a scenario where social benefits combine with significant risks for the individual's rights to privacy and data protection, and where knowledge on information management and digital skills are the core demands of the young generation. Bearing this in mind, the mission of data protection authorities is to ensure that young people are adequately prepared for the challenge, while society as a whole reaps the benefits of technology.

The concept of the ARCADES project was based on a 2009 Polish nation-wide programme for schools entitled *Your data – your concern* and the relatively high interest expressed by teachers in Poland for this programme, which inspired the Polish Data Protection Authority to transfer the idea to the European level. The project team believes that schools should teach pupils about privacy and personal data protection. The topics related to the protection of personal data can be incorporated in the curricula of various schools' subjects. They are part of digital skills which form the background for the 21st century knowledge and which are *conditio sine qua non* for the development of modern citizens. It is rightly stressed that the democratic society needs young people to use their digital activity both as a human right and as a tool to change the world. Digital skills enable social activity and help to develop entrepreneurship, art and innovation. Any young person who wants to use digital technologies practically and effectively must be aware that while data is the fuel of the new

[*] European Data Protection Assistant Supervisor.

economy, the user who is not aware of data processing's privacy concerns may become a 'product' in the industry chain.

European data protection authorities in their *Opinion on the protection of children's personal data* (Opinion 2/2009 of the Article 29 Working Party) stressed that a person who has not yet achieved physical and psychological maturity needs more protection than others. However, improving conditions for the child and strengthening the child's right to the development of his or her personality do not only mean taking legislative and administrative action by the government, legislature or data protection authorities. This should first of all be done by passing on the knowledge on privacy aspects of new technologies at each and every stage of children's education.

The protection and care necessary for the wellbeing of children refer to their right to development, and to the fact this right can only be properly enjoyed with the assistance or protection of others. This protection falls on the family, on society and on the State. It must be recognised that in order to achieve an appropriate level of care for children, their personal data will sometimes need to be processed extensively and by several parties. The approach to protect children's privacy is based on education – by families, schools, data protection authorities, children's groups and others – on the importance of data protection and privacy, and on the consequences of giving out personal data if not necessary.

If our societies are to strive for a true culture of data protection in particular, and of the defence of privacy in general, one must start with children, not only as a group that needs protection, or as subjects of the rights to be protected, but also because they should be made aware of their duties to respect the personal data of others. In order to achieve this goal, schools should play a key role.

Children and pupils should be brought up to become autonomous citizens of the Information Society. To this end, it is crucial that they learn from an early age about the importance of privacy and data protection. These concepts will enable them to make informed decisions about which information they want to disclose, to whom and under which conditions. Data protection should be included systematically in school curricula not necessarily as a separate subject, but taking into consideration in each kind of school classes the age of the pupils and the nature of the subjects taught.

The development of digital skills is usually based on relations between technology and a practical result to be achieved. The educational actions in privacy protection should be based on the same win-win scenario. They should however respect the fact that digital skills are a very personal and individual set, and will differ from child to child.

Institutions of public and private education as well as all the civic society involved in the educational process should understand data protection issues as a core of digital skills and promote innovative ways to teach about privacy, and to deliver to children practical tools to deal with it.

Brussels, May 2016

OPENING STATEMENTS BY ARCADES PARTNERS

Research Group on Law, Science, Technology and Society (LSTS)*

Ladies and Gentlemen,

The Law, Science, Technology and Society (LSTS) Research Group of the Vrije Universiteit Brussel (VUB) is particularly proud of the ARCADES project, and more particularly of the publication of the present Handbook.

The prime objective of ARCADES was to bolster up the efforts of European data protection authorities in privacy awareness of children and youngsters through school education. To do so, the project brought together three data protection authorities and us, VUB's LSTS Research Group, a leading research group with internationally recognised excellence in the field of privacy and data protection (and solid experience in working together with data protection authorities). As the sole ARCADES academic partner, our mission was to lead the consortium's work towards the finalisation of the present Handbook: a practical, innovative, markedly European and future-oriented reference text for teachers.

We have learnt a lot during this project. We knew data protection authorities were active trying to reach children and youngsters, as well as their teachers. With ARCADES, we realised the richness of existing initiatives, discovered the strength of the authorities' commitment, and found out that teachers are not only in need for guidance, but also highly interested in obtaining it and sharing it with their pupils.

We always believed children and youngsters do care about privacy, and should not be blamed for spoiling it, but – instead – better educated on how to defend it. Thanks to ARCADES, we met children and youngsters who taught us about the importance of knowing how to control our personal data, and that one is never too young to start thinking about privacy.

[*] Vrije Universiteit Brussel.

Since the beginning, we envisaged work on this Handbook as an inclusive process, taking stock of all available materials and all relevant knowledge, in Brussels and beyond. We integrated thus crucial feedback from teachers and their pupils, but also education specialists, and reached out for the civil society and online safety experts, as well as the wider community of data protection authorities.

We did all this from the perspective of privacy and personal data protection as fundamental rights. We always kept in mind they both are rights recognised as such in the Charter of Fundamental Rights of the European Union, and that this so because of their high significance for democratic life. Teaching about privacy and data protection shall thus not be (exclusively) about keeping minors ‘safe’. It must be also be about keeping them aware of their rights, and ready to exercise them.

The publication of this Handbook is thus, in our view, great news not only for teachers, but more generally for anyone who believes education should help children and youngsters become better (digital) citizens.

Prof. Dr. Paul De Hert
Brussels, May 2016

Inspector General for Personal Data Protection of Poland (GIODO)

Ladies and Gentlemen,

We are very proud to present to you this book as evidence of over a year and a half of work dedicated to introducing data protection and privacy in schools. I am very pleased that the Inspector General for Personal Data Protection of Poland has had the opportunity to take part in this project.

In the EU are produced many educational materials on issues of personal data protection in a digital world addressed to children, youth and parents. Their value cannot be overstated – in an era of rapid technological developments, children start using the Internet from a very early age for learning, fun and communication. Unfortunately, they very often recklessly share information on themselves and others. Regardless of the many educational materials available online, the role schools should play in this process is irreplaceable.

When we started our work on the ARCADES project, we set ourselves the goal of developing practical materials for schools and teachers to help them to teach students in an interesting and at the same time efficient way about the need to protect their privacy. We are convinced that the knowledge on the protection of privacy and personal data as well as on the safe use of the Internet should constitute an essential element of school education. This publication offers practical guidance on teaching privacy and data protection at schools.

We could assess the value of this type of materials looking at the impact of the competition for the best lesson's scenario organised within the framework of ARCADES for schools in Poland. We invited teachers to develop, based on the practical guide drawn up within the project, a model lesson's scenario on personal data and privacy protection. And we received a dozen of excellent proposals meeting the methodical requirements binding in Poland. Many of them showed in a very original way how to teach children and youth about the protection of personal data as well as their rights and the proper use of them in an effective and interesting way.

Therefore, we are all the more pleased to present to you this Handbook, hoping that it will receive recognition both among teachers in the EU and the entire European education community, as well as all EU data protection authorities.

Dr. Edyta Bielak-Jomaa
Warsaw, May 2016

Information Commissioner of the Republic of Slovenia (IP RS)

Ladies and Gentlemen,

It is with great pleasure that I present to you this publication, the result of a fruitful cooperation between the partners of the ARCADES project. In it you will find all crucial information about data protection and privacy that children in schools should be made aware of, together with practical tools that can be of assistance when teaching about these topics.

Why did we take up the project? In our everyday work as a data protection authority we are faced with questions, cases and complaints which concern children, be it in the role of a victim in a situation where their privacy has been violated or, even worse, in the role of a perpetrator, bullying other children on the Internet or social platforms. This is why we believe education of children is key – to prevent rather than to cure, to teach the young how to protect their personal data and privacy and be able to use all new technologies responsibly and with care of others.

The Information Commissioner of Slovenia is active in the field of awareness rising. Every year we publish materials aimed at safe and responsible use of new technologies and we learn the importance of the roles we play as parents, teachers and experts in education for empowering the children to be able to use all information services for their benefits, but also to stay safe and use them responsibly. They might be well ahead of us by their knowledge about the technical part of the use of Internet. But what they lack is experience, and the awareness of time, of the fact that they have the whole future in front of them – a future where the data that are available on the Internet about them may well come one day to haunt them, to prevent them from getting a scholarship, or the work they desire, or the partner they love. This is the perspective and the knowledge we can give them.

We started the ARCADES project a year and a half ago and in this short time we achieved important goals. We produced a set of teaching materials for teachers, unified and ready to be used by all teachers in the EU. We organized very successful trainings. The feedback from the teachers in Slovenia was extremely positive. The teachers found that the seminars offered them a lot of valuable information in a very practical form of examples, and interactive content they will be able to use in practice in their class. We also organised a contest for best model lesson scenarios – and to our great pleasure the winners of the contest in Slovenia belonged to the youngest age group, only just starting primary school and on the verge of discovering all the potentials of the Internet.

To sum up, the ARCADES project produced a number of tangible results that have the potential to make a big impact on raising awareness of data protection and privacy in schools among the children. It is my great wish is that this publication will reach as many schools in different EU Member States as possible, and raise the level of knowledge about data protection and privacy.

Mojca Prelesnik
Ljubljana, May 2016

Hungarian Authority for Data Protection and Freedom of Information (NAIH)

Ladies and Gentlemen,

Internet culture has a real effect on the habits of youths in all aspects of life. New words are created, new communication forms are being used, worldwide events affect them globally and simultaneously right away – all this influences our children's thinking and behaviour. We emphasize, however, that these changes are inevitable but not condemnable at all. Awareness, caution, a critical approach and an analysing attitude are absolutely advantageous in this field.

The Hungarian National Authority for Data Protection and Freedom of Information (NAIH) started operating on 1 January 2012. It resumed the legal protective activity of the former data protection commissioner, operative between 1995 and 2011. The Hungarian DPA receives complaints from citizens and, in case of well-founded suspicion of severe data breaches, it can also initiate data protection administrative procedures.

The Internet has an extraordinary scope of processing of personal data and data of public interest with regard to the incredibly high number of information, data processing activities and data subjects as well as the power of unlimited publicity. The protection of children's personal data has always been a priority for all of us dealing with data protection issues. Due to their age and lack of proper life experience, they are more vulnerable, and the consequences of infringements may severely affect their personality and mental development. Hence, our DPA pays particular attention to Internet-related data processing activities affecting minors. Prevention and the dissemination of information have therefore the utmost importance, whilst the remedy of infringements and awareness-raising of data subjects and the public are also fundamental requirements.

We are convinced that introducing individual data protection education courses and providing state-of-the-art and practical knowledge in teacher training is inevitable today to turn students into trained and conscious users of modern IT technologies, and to help them become confident digital citizens. The success of our publications – including the present Handbook – clearly indicates that among Hungarian experts dealing with children (teachers, child protection specialists, NGOs) there is a great need to exchange best practices and knowledge.

An ARCADES seminar for 200 registered participants – teachers and experts in education – was organised on 20–22 October 2015 in Budapest at the National University of Public Service. The agenda of the seminar was divided into two parts: the plenary session introduced the project and presented the handbook while active workshops offered the possibility to discuss with experts specific topics such as personality distortion, emotional effects of Internet use or practical advices. Most of the teachers were informed about the event via their headmasters connected with the network of the Educational Institute, while some had read the news on the specific ARCADES webpage created by NAIH. Based upon the immediate responses but also on the opinions provided via the evaluation sheets, the seminars can be described as successful and very useful. Moreover, the 15 applications for the contest of the *Best Privacy Lesson* sent to NAIH systematically referred to and covered the topics and ideas of the handbook and also the information and knowledge we tried to share with the participants of the seminars.

Furthermore, in March 2016 we initiated with the Ministry of Education and the universities responsible for teacher training the inclusion of data protection training programmes for the teachers of the future, to whom the Hungarian DPA offers its experience, knowledge basis and international networks with pleasure.

Dr. Attila Péterfalvi
Budapest, May 2016

PART I

THE PRIVACY AND DATA PROTECTION EDUCATION LANDSCAPE

ARCADES, A EUROPEAN PROJECT TO BOOST PRIVACY EDUCATION

Urszula Góral and Paweł Makowski*

1. MANY INITIATIVES ON A NATIONAL LEVEL

Through cooperation in the framework of numerous projects, including projects co-financed by the EU, it appeared that many data protection authorities (DPAs) conducted educational activities. These many interesting initiatives developed on a national level were executed independently, in parallel, but were nevertheless very similar in essence. While cooperating with other authorities, GIODO, the Polish DPA, thus identified the need to coordinate these types of initiatives by disseminating good practices as well as enabling access to knowledge – instead of reinventing the wheel. It can thus be said that international cooperation among DPAs led to the conclusion that many states undertook educational activities on their own, dedicating time and effort to designing adequate tools, while others had already achieved satisfying results in the area. Therefore, it seemed appropriate to support synergies among these parallel actions, and to create common solutions enabling a more efficient execution of educational activities by DPAs.

Undoubtedly, each authority encounters in its country similar problems and challenges whenever it plans to undertake educational activities through cooperation with schools. Preparing proper teaching aids, creating attractive tools for both teachers and pupils, or training of teachers require extensive resources – as regards knowledge as well as financing. Cooperation with the public authorities supervising the functioning of schools is also necessary. As shown by the experiences of DPAs, most of them – more or less successfully – cooperate with those institutions (for instance introducing content related to personal data protection and the right to privacy in the curricula). The analysis of these actions enables the setting up of a certain matrix that could be used as a pattern by all authorities interested in conducting educational actions. Thus, and considering also the borderless nature of the Internet, there is a need for a

* Bureau of the Inspector-General for the Protection of Personal Data (GIODO), Poland.

common approach at the European level, and for the development of common and effective teaching approaches.

2. POLISH EXPERIENCES

In its activities in previous years GIODO prioritised education of children and youth through many initiatives. Struggling with common financial problems, it has developed satisfying solutions, certainly with the assistance of other DPAs, and using their experience. One example of such inspiring experiences are the actions taken by the Czech DPA. Close cooperation with this authority enabled GIODO to learn about Czech lesson scenarios, introducing content concerning privacy and personal data protection into courses such as literature, biology or history lessons. Such way of action has been successfully introduced into Polish schools within the *Your data – your concern* programme. The main goal of this programme, uninterruptedly and effectively implemented by GIODO for six years, is to widen the educational offer of Polish Education Centres for Teachers, primary schools, secondary and high-schools, by introducing content on personal data protection and the right to privacy. One of the stages of the programme is to train and equip teachers of schools and Education Centres with educational materials containing, *inter alia*, information on personal data protection as well as lesson scenarios, and thereby prepare teachers to shape aware, responsible and open attitudes among pupils. Another element of the programme is to carry out at schools and Education Centres lessons related to personal data protection (among other meetings and trainings), as well as drafting lesson scenarios and preparing evaluation reports on actions undertaken during the programme.

3. URGENT NEED FOR EDUCATION ON PRIVACY AND DATA PROTECTION

Its experience shaping policy in the field of education and designing current patterns, together with the considerable interest expressed by teachers in Poland in the programme *Your data – your concern*, inspired the Inspector General for Personal Data Protection of Poland to bring its activities to the European level. This resulted in the ARCADES proposal, which was submitted to the European Commission in March 2014, within the framework of Fundamental Rights and Citizenship programme managed by the Directorate General (DG) Justice and Consumers. The application was accepted in July 2014 and a grant was thus awarded for an action of four partners – the Polish Inspector General for Personal Data Protection (coordinator), the Information Commissioner of the Republic of Slovenia (IP RS), the Hungarian National Authority for Data Protection and Freedom of Information (NAIH), and the Law, Science, Technology and Society (LSTS) Research Group of the Vrije Universiteit Brussel (VUB), based in Belgium. The project consortium was chosen because of the experience of partners in developing teaching aids for schools.

4. ARCADES OBJECTIVES – WHAT IS IT ALL ABOUT?

The project goes hand in hand with other European actions aimed at raising awareness on personal data protection and privacy. As stated above, many of such initiatives are taken by EU data protection authorities, which, independently of their enforcement competencies, pay much attention to educational activities. Data protection and privacy are fundamental rights, protected both by national legislation and EU law. DPAs's role is to guard those rights. They also have the role of educating the general public in this field. *The Resolution on Digital Education for All*, drafted at the occasion of International Conference of Data Protection and Privacy Commissioners held at Warsaw in 2013, is but one example of such commitment. The Resolution, which recommends that specific protection should be provided to minors with respect to digital technology, was also an incentive for DPAs to pay attention to actions directed to schools.

This is extremely important in an era of rapidly developing digital technologies that are increasingly being used by young people. Therefore, DPAs produce educational materials addressed to youngsters, teachers, as well as parents, since there is also a great need to educate them in the field of data and privacy protection.

Such way of thinking of DPAs functioning in Europe is upheld by the provisions of the new General Data Protection Regulation (GDPR) of 27 April 2016. In its Article 57, among many tasks envisaged for DPAs, it provides for an obligation to *promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing.* It is of great significance that the aforementioned provision stresses the need for specific attention of activities addressed to children.

Polish experience obtained through the *Your data – your concern* programme shows that in the process of disseminating privacy knowledge among children, it is of critical importance to introduce those topics into school lessons. The day-to-day work of teachers participating in the programme illustrates there is a significant need for preparing materials for teachers, so they can efficiently and interestingly teach personal data protection at schools. The special role of schools for children and youth education on society's functioning, as well as for the safe discovering of the digital world, was also hinted by the Eurobarometer report of 2008 (*Towards a safer use of Internet for children in the EU – a parent`s perspective*). And it is at schools in the first place where children and youth notify accidents relating to privacy infringements. The main objective of ARCADES project was thus to produce relevant materials to help introducing content dedicated to personal data protection into schools in the EU.

5. ATTAINING THE OBJECTIVES

For teachers to be able to effectively transfer their personal data protection knowledge, and raise the awareness and improve the skills of children and youth in the field of privacy protection, proper educational materials are a key prerequisite. To this end, ARCADES project partners first summarised existing knowledge on privacy and data protection education at EU schools.[1] The resulting report contains a mapping of available information, materials on the rules of privacy and personal data protection directed to teachers and students and documents on major trends and common (as well as best) practices. The document is certainly not exhaustive with relation to all initiatives taken in the EU, yet it is an invitation to open a discussion on the requirements that teaching materials in this area should meet.

With such background, we could commence the preparation of educational materials to inspire teachers and make them ready to conduct lessons on personal data protection. This is how what was to become the ARCADES Teachers' Manual was prepared.[2] This material is directed towards teachers of primary, secondary and high schools who want to increase their knowledge in the field of personal data protection, acquiring simultaneously practical materials helpful in conducting lessons dedicated to this topic. It actually aims to provide this kind of useful tools for teachers of any EU school wishing to educate children and teenagers about privacy and personal data protection. It is written in clear

[1] G. González Fuster, P. De Hert, and D. Kloza, Deliverable 1.1: State-of-the-Art Report on Teaching Privacy and Personal Data Protection at Schools in the European Union, ARCADES, March 2015 <http://arcades-project.eu/images/pdf/State_of_the_art_report.pdf> accessed 01.05.2016.

[2] For an earlier version, see: G. González Fuster (ed.), *Deliverable 1.2: The European Handbook for Teaching Privacy and Data Protection at Schools – the set of materials for teachers*, ARCADES, September 2015, <http://arcades-project.eu/images/pdf/The_European_Handbook_for_Teaching_Privacy_and_Data_Protection_at_Schools.pdf> accessed 01.05.2016.

and simple language that will help teachers find the right words to explain to their pupils the issues at stake. Each of the ten thematic chapters of the manual covers different facets of privacy and personal data protection, advances a set of key ideas and puts forward subjects for discussion, recommended activities or concrete tips. The first draft of the manual, a revised version of which is presented in this Handbook, received favourable assessments from the national teaching centres in Poland, Hungary and Slovenia, which guarantees it is adapted to the requirements set up for educational materials used for school classes.

The manual was presented at seminars held in the framework of the ARCADES project in October 2015 by the partners from Poland, Slovenia and Hungary. Each of these events assembled almost 200 teachers. The aim of the seminars was to convey relevant knowledge on personal data protection and privacy to teachers, so that they would be able to forward the knowledge to their pupils. The participants attending the events in Poland, Hungary and Slovenia were therefore provided with both essential information about data protection issues and educational materials in the form of a handbook. Feedback from teachers shows they are often facing difficulties, not being equipped with adequate knowledge and resources when teaching pupils about data protection and privacy. They have reported they often have incidents related to data protection and privacy breaches at schools, but they lack instructions and guidelines on how to react. Therefore, we welcomed their positive opinions provided at the evaluation phase with even bigger satisfaction – they proved that each seminar could be described as successful and very useful, which only firmed our belief that our materials have the teachers' support, and that teachers see them as having practical value for their lessons.

This view was also confirmed by the number of applications in the competitions organised in Poland, Hungary and Slovenia. Publishing educational materials or narrative teaching solely based on a textbook is no longer efficient: new teaching methods that meet the needs of the students should be embedded in the curricula, to develop an effective educational approach. Creating personalised, real world lesson scenarios can capture children's interest and enhance their engagement – in addition to learning how to react in day-to-day situations. Therefore, preparing standard lesson scenarios dedicated to personal data protection was the topic of the competition. All scenarios submitted to the competition were based on ARCADES materials, confirming their usefulness.

The winners of national competitions for best lesson plans had the occasion to demonstrate them at the ARCADES Final Conference, held in March 2016 in Barcelona. During this Conference was also held a Workshop of the International Working Group on Digital Education, led by the French DPA

(CNIL). The activeness of the ARCADES consortium had been noticed by this group, resulting in such joint event in Barcelona where were considered a training kit model as well as guidelines for a 'competence framework' in the field of data protection and privacy.

6. EU RELEVANCE AND FUTURE PROSPECTS

Up to now, most of all available privacy and data protection educational materials for children and youngsters had been produced on a national level. The exchange of experiences among ARCADES project partners has helped drafting not only efficient but also more EU-oriented tools. This notably implies that, in the end, the project has managed to produce 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. Materials drafted in the course of this project thus present a wider perspective than the national one, making them transferable and ready to use at schools across all EU countries.

Despite the fact that the project has come to an end, we believe that the ARCADES materials will remain a source of inspiration for many teachers in different EU Member States. We hope that they will also be of direct use for EU DPAs and their educational activities, since the content presented in this publication delivers not only essential knowledge in the field of privacy teaching but also a set of practical tips. Therefore, we encourage everyone to carefully read this publication and to actively use it, boosting in this way privacy education in Europe.

MESSAGE FROM THE DIGITAL EDUCATION WORKING GROUP

Pascale Raulin-Serrier and Sophie Vulliet-Tavernier*

The *Resolution on Digital Education for All*[1] adopted at the 35th International Conference of Data Protection and Privacy Commissioners in Warsaw in 2013 invited data protection authorities to reinforce their engagement in training actions, targeting all members of the public to help citizens to become informed and responsible actors in the digital environment, to efficiently make use of their rights, and to be aware of their duties in this field. As a matter of fact, during the last few years, many data protection authorities representing the main regional areas of the world have been exchanging their experiences and taking important initiatives on global awareness of children, young people and the educational community regarding data protection and privacy.

Within this framework, the Resolution charged the International Data Protection Working Group on Digital Education with implementing annual priority Action Plan Programmes, such as '*Develop a tutorial pack aimed at training trainers with regard to the protection of data and privacy*' and '*Develop a web platform sharing content and teaching material in the field of digital education*', in order to fulfil its main operational objectives.[2]

The European ARCADES project and its creation of a set of teaching materials fit particularly well with the actions set out to contribute to the production of training kits for educators in the field of data protection and privacy. As there exists no uniform model of teaching kits aimed to train educators, as far as we know from our analysis of the current landscape mapping teaching

[*] Digital Education Department of the Commission Nationale de l'Informatique et des Libertés (CNIL), and Coordinators of the International Data Protection Working Group on Digital Education.

[1] <https://icdppc.org/wp-content/uploads/2015/02/Digital-education-resolution.pdf> accessed 15.05.2016.

[2] That is: (1) Promoting privacy education as part of digital literacy programs; and (2) Playing a part in training relay persons by organising or contributing towards 'training of trainers' on data protection and privacy.

resources,[3] teaching privacy and personal data protection at EU schools may necessarily require embracing the peculiarities of European approaches referring to European legislation.

To this end, the present Handbook is intended to be used to help teachers to be harnessed for the preparation of children and teenagers to mobilise and develop relevant skills, knowledge and understanding in order to respond appropriately and effectively to the many challenges and opportunities presented by everyday situations in a democratic society, applying in the physical world but also in the digital, online world.

In this context, the present Handbook and in particular its set of teaching materials are intended to go far beyond 'media literacy' or 'digital literacy' education, and to encompass new dimensions related to 'legal and ethical literacy', that is, an understanding of where the relevant laws define the guidelines and behaviours in an on-line and off-line environment.

The feedback received thus far from members of the International Data Protection Working Group on Digital Education demonstrates keen interest in the dissemination of the Handbook as a very useful and comprehensive tool as set out among teachers, educators, public educational authorities and other actors to enable the children and teenagers to fully encompass their rights, freedoms and obligations in a democratic society.

Of course, teachers are encouraged to examine this resource and then use, adapt or even explore all areas of concern related to privacy through tip sheets provided, in compliance with their pedagogical activities to suit their permanent students' needs. Therefore, we wish to express our appreciation to the ARCADES consortium and core partners who have contributed to create this innovative material and who are also rolling them out to the teens and their parents, far beyond teachers.

[3] As illustrated in two study reports of the Working group of Data Protection Authorities on Digital Education, produced in 2014 and 2015.

THE MANY FACES OF PRIVACY EDUCATION IN EUROPEAN SCHOOLS

Gloria González Fuster, Dariusz Kloza and Paul De Hert*

Privacy education is already a reality in some schools in Europe. Strengthening this trend is a priority for many actors in the field. This contribution explores why this is so and investigates what can be learnt from the review of current practices. Therefore it first examines the reasons for teaching about privacy at schools and subsequently overviews and assesses the relevant efforts undertaken thus far. It concludes that it is important to ensure children know about privacy not just to keep them safe, but primarily to help them grow as free individuals.

1. WHY PRIVACY EDUCATION?

1.1. PRIVACY PROBLEMS ARE REAL AND THEIR CONSEQUENCES OFTEN SERIOUS

Privacy problems are real. For some people, e.g. the academic authors of this paper working on such issues on a daily basis, this might appear almost self-evident. For others, in various walks of life the urgency and importance of privacy issues may not be so obvious.

Let us start with a most mundane example. Not many people would feel comfortable if their names, addresses and professions were published on a website of a parish without their permission. Similarly, few people would be pleased to find on such websites details of their medical condition, even if minor. The problem concerns not only the fact that these pieces of information are made available to the public, but also the possibility that people could infer other aspects of one's life, such as belonging to a particular religious association. This example concerns facts that the Court of Justice of the European Union

* Vrije Universiteit Brussel (VUB), Research Group on Law, Science, Technology & Society (LSTS).

debated already in 2003, regarding a Swedish woman, Mrs Bodil Lindqvist, and the website she ran. The Court was asked whether her putting online personal information about others without their consent breached Swedish data protection law. The Court held it did.[1]

There are many other examples of things that can happen to all of us. All over the globe, numerous people play via the Internet. The gaming experience is often possible only upon registration, requiring disclosure of some personal data, and often linked to the payment of a subscription fee. In 2011, Sony Corporation's PlayStation Network suffered a hacker attack. The personal data of some 77 million user accounts were compromised and released to the public. These data included not only names and e-mail addresses, but also login details and passwords, dates of birth and credit card details. If only e-mail addresses had been leaked, most of people would have probably just tolerated a few more spam messages a week. However, pieces of information such as passwords and credit card numbers raise more serious problems, also because the majority of people use one and the same password for many of their on-line activities. Sony Corporation immediately urged its customers to verify their credit card history.[2] This example is not standalone: data breaches occur as a matter of fact on a daily basis all over the world.[3]

Data breaches such as this one, and – more generally – the many problems that can happen with data and affect privacy, raise a wide range of questions regarding the responsibility of those involved. In some circumstances, individuals might have a clear responsibility for deciding what data they share, for instance deciding whether to post some information about others online or not. In others, they might have little choice, for instance if they are pushed to accept certain data handling practices in order to play a game that they just purchased (or that was offered to them by their family). In all cases, it is possible that individuals are not completely aware of the consequences of their decisions or the risks associated to certain data disclosures.

All these issues might be labelled as 'privacy' issues, understood as encompassing the protection of personal data. They often overlap with questions about secrecy, safety and security. Whilst 'privacy' is only one of the possible angles through which such issues can be viewed, this does not change the fact the harms to privacy can result in serious consequences for individuals. Such harms to

[1] Case C-101/01, *Bodil Lindqvist* [2003] ECR I-12971.

[2] PlayStation.Blog, *Update on PlayStation Network and Qriocity*, 26 April 2011 <http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity> accessed 25.05.2016.

[3] For an interesting visual presentation, cf.: <www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks> accessed 20.05.2016.

privacy are damaging enough for adults. As adults, we generally want to keep some information for ourselves and for our most trusted ones. We might feel uncomfortable even when someone else learns our secrets, if not meant to. Things get worse when our secrets are used against us. Dealing with spam is a small concern in comparison with stolen money, identity theft, cyber-bullying, blackmailing or sexual harassment, just to name a few. But things get much worse if a child – a person who has not yet reached maturity and thus is vulnerable – becomes involved one way or another in any of these.

1.2. PRIVACY LAWS OFFER UNIVERSAL PROTECTION AND EMPOWER INDIVIDUALS

One way in which we can contribute to have our privacy protected is by being careful with our own personal data. In that sense, a good deal of protection depends upon us. Behind our own duty of care there are however also legal requirements imposed on those who handle our personal data. These requirements are meant to protect us against their misuse of our data, acknowledging it is not enough for us to be aware of risks and take care.

Roots of these requirements are traceable back to 1890. In response to the popularisation of photography and its increasing use in the press, which was found too invasive, the idea of privacy as a 'right to be let alone' was launched in the United States, echoing European legal developments.[4] Contemporary legal protection of privacy is offered universally, i.e. extending to everybody. It is set forth predominantly by international human rights law, for instance in the European Convention of Human Rights (1950),[5] but also in the Charter of Fundamental Rights of the European Union (2000).[6] In parallel, privacy protection emerged progressively in the legal orders of Member States of the European Union. European data protection law spells out the conditions for lawful processing of personal data, grants a series of subjective rights to individuals and foresees the existence of independent authorities to monitor compliance.

The dry way privacy laws are construed often requires some effort from individuals. It is true that their provisions are usually set in a somehow paternalistic and ultra-prescriptive tone, but their purpose is to protect our

[4] S. Warren and L. Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 5, 193. Cf. also: G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Dordrecht 2014.

[5] Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS 5; <http://echr.coe.int/Documents/Convention_ENG.pdf> accessed 20.05.2016.

[6] Charter of Fundamental Rights of the European Union [2000] OJ C 361/1.

liberty and in these provisions we are still left with room for a lot of manoeuvre, at least in principle. In such cases the care for privacy comes back to our own hands as a form of empowerment. Whenever we make choices of that type, we also bear the consequences of our choices. This is why we are entitled to meaningful and transparent information about the data processing at stake. For example, we often need to give consent to subscribe to an online service, and in this way we agree to certain processing practices of our personal data. Consent once given can normally be withdrawn anytime later. This choice is, in theory, a very powerful tool in the hands of an individual.

1.3. PRIVACY LAWS RECOGNISE THE NEED FOR SPECIAL SAFEGUARDS FOR CHILDREN

Contemporary children, due to their 'breezy familiarity'[7] with the technological know-how, have been called 'digital natives'.[8] They act on information fundamentally differently from their predecessors.[9] Their use of technology is widespread and growing. Statistics show that already in 2011 more than 75% of European kids had used the Internet for a wide range of purposes, from communicating with their peers (especially using social network sites) to receiving contents (e.g. listening to music) to playing games. Some of them produce contents on the Internet, e.g. by writing a blog.[10] With the passage of time, children are going online more, at younger ages, and in more diverse ways.[11] Thus it is not surprising that children are increasingly at the forefront of innovative data processing practices. Sharing a selfie photo with their school diploma has already become a common practice. Each day brings some innovation: smartphone applications for measuring baby milk consumption or a 'smart watch' allowing mum and dad to always know where their kids are.[12] This does not mean, however, that children are more aware than adults of what happens to their personal data when the data are in the hands of the others. They are not necessarily aware of the risks associated with such data handling and of the possible impact of such practices on their lifes, both in the short and in the long term.

[7] *American Libraries Association v. Pataki* [1997] 969 F. Supp. 160.

[8] M. Prensky, 'Digital Natives, Digital Immigrants' (2001) 9 *On the Horizon* 5, p. 1.

[9] Ibid.

[10] S. Livingstone et al., *Risks and Safety on the Internet: The Perspective of European Children,* London School of Economics and Political Science, London 2011, p. 33.

[11] S. Livingstone (eds.), *EU Kids Online. Findings, Methods, Recommendations*, London School of Economics and Political Science, London, 2015, p. 6.

[12] On this subject, see notably: G. González Fuster, 'GDPR: we all need to work at it!', *Better Internet for Kids (BIK) Bulletin*, 31 March 2016, <https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=694148> accessed 20.05.2016.

Privacy laws offer universal protection. This protection extends logically to children. However, children are vulnerable individuals. They do not always know how to protect themselves from the threats arising from sharing their personal data with the help of technology. When a piece of data on a child is being handled, not only existing risks are elevated but also this child is exposed to new types of risks. Therefore children necessitate specific safeguards. It was only recently that EU's laws have started to openly incorporate such a need. The recently concluded (April 2016) reform of the EU data protection framework explicitly recognises the necessity for a specific level of legal protection for children. The preamble to the General Data Protection Regulation argues that

> […] children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child […].[13]

1.4. SOME PRIVACY PROBLEMS CAN BE AVOIDED BY BEING AWARE

The old wisdom has it that 'prevention is better than cure'. In some instances, taking preventive measures lies entirely within the powers of those who handle our personal data. We cannot do much if, for instance, our Internet service providers become victims of a hacker's attack. It is rather the responsibility of these providers to offer adequate safety and security for their products and services.

But there are situations in which taking rational action to prevent these risks and dangers from happening, or – at least – minimizing their possibility to materialise, falls also within our possibilities. The simplest way is to reflect before sharing personal data or consenting to certain data handlings.

A condition for these approaches to work in practice is to be aware of the threats associated with personal data handling and of the ways to protect oneself against them. Studies found that while the vast majority of Europeans see 'disclosing personal information as an increasing part of modern life', they

[13] Recital 38; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

are not sufficiently aware of the ways in which to protect their personal data.[14] Individuals are typically depicted as 'uninformed and confused' and hence often 'misinterpreting their own behaviour'.[15] We have already mentioned that the law empowers us and consent is a powerful tool in our hands. But it is a common practice that we click 'I agree' without giving even a slightest thought about possible implications of our agreement to handle our data. Statistics further show that Europeans lack information on the available remedies in case something goes wrong.[16] More importantly, they are not aware of the existence of a national data protection authority that could offer them assistance in such situations.[17] But even among those who are aware, an accurate and sufficient perception of threats is usually lacking.[18] Put simply, these threats do not speak to their imagination: 'it would not happen to me, too small probability' or 'I will think about it only when it happens'. Sometimes it is simply too late. Privacy harms building on the irreversibility of disclosure of information are rather irreparable.

All in all, it surfaces that the relation between individual awareness and privacy protection is not always straightforward. Individuals are expected to be sufficiently informed and aware of threats in order to make the right choices. However, it is well known that – statistically speaking – in most of the cases they are not. This paradox is even more acute as regards to children, as it is undisputed that, by definition, they are not in a position to make choices as informed and responsible as those made by adults. We might nevertheless be tempted to insist on the fact that, for everything to go well, they should. Indeed, much effort is often put in insisting on the idea that children should, in regards to their privacy, stop behaving like children.

1.5. EMPOWERING THE MOST VULNERABLE

Privacy education for children must thus move beyond such conundrum by integrating a wider perspective. It is important to recommend children to think

[14] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, Brussels 2011, p. 5, <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> accessed 20.05.2016.

[15] G. González Fuster, 'How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection' (2014) 19 *IDP. Revista de Internet, Derecho y Política*, p. 99.

[16] European Union Agency for Fundamental Rights, *Access to Data Protection Remedies in EU Member States*, Publications Office of the European Union, Luxembourg 2014, pp. 32–34.

[17] European Commission, *Special Eurobarometer 359*, op. cit., p. 174.

[18] J.B. Rule, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*, Elsevier, New York 1980, p. 184.

twice about what they do with their personal data, but it is also as important to let them know their personal data deserve protection by the others too. Taking the right decisions about disclosing data is a crucial element of privacy protection, but it is not the only one. Teaching this to children does not only contribute to keep them safe, but also to empower them; these two objectives go hand in hand.

An empowered individual will more successfully protect herself against privacy problems. To be empowered is to be aware of dangers, but also of existing rights and rules, and the ways foreseen to remedy problems. And if children are empowered – that is to say, if they know not only about privacy harms and online risks, but also about what they are entitled to, and who is obliged to do what – they shall, ultimately, also be safer.

Therefore we found it exemplary that the reformed data protection legal framework in the EU not only explicitly recognises the need for special protection of children, but that it also implicitly recognises the value of raising their awareness about privacy. Thus the same legal framework tasks therewith certain public authorities and – in doing so – pays special attention to children. These authorities, normally called 'data protection authorities', are a key component of the fundamental right to the protection of personal data. The legal framework entrusts them with many and varied roles.

Historically speaking, data protection authorities from the beginning of their existence in the 1970s have been occupied not only with 'supervision' of whether data protection laws were observed, but also with a wide range of other roles, from ombudsmen, auditors to consultants to policy advisers.[19] All these activities have a common goal of a greater level of protection, and one of those tasks is public education.

The law has progressively reflected the broadening of their mission. The newly adopted General Data Protection Regulation (GDPR), which will apply from May 2018 on, explicitly tasks these supervisory authorities therewith. Article 57 lists their duties and, among other, states:

> each supervisory authority shall on its territory [...] promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention.

[19] C.J. Bennett and C.D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge 2006. For an overview and evaluation, cf. e.g.: European Commission, *Evaluation of the Means used by National Data Protection Supervisory Authorities in the promotion of personal Data Protection. Final Report*, Brussels 2009.

The GDPR thus explicitly acknowledges that children need to know about the risks associated to personal data processing, but also about the applicable rules, safeguards and rights. Awareness of risks shall in fact be instrumental for them to usefully exercise their rights.

It is worth mentioning that raising privacy awareness among children is actually a concern present well beyond European borders. The United States (US), for instance, was a pioneer in the regulation of online privacy protection, with the adoption in 1998 of the Children's Online Privacy Protection Act,[20] applicable to websites that collect information from children under the age of 13. The Federal Trade Commission in the US, involved in its enforcement, manages various websites specifically targeting awareness raising among children.

2. THE PRIVACY EDUCATION LANDSCAPE IN EUROPE

The ARCADES project reviewed many activities undertaken for the education of children on privacy in European schools, noting their diversity.[21] The project's focus was on analysing available teaching materials.

2.1. WHO?

Actors producing guidance or concrete materials for privacy education in schools might fall under some generic categories and approach the issue of privacy protection from different angles. International organisations such the United Nations Educational, Scientific, and Cultural Organization (UNESCO)[22] have a particular interest in the rights of children and thus also in their right to privacy. The same is true for the Council of Europe, which also intersects with privacy education from a human rights perspective. The EU is involved in the area both from an online safety perspective and from the point of view of fundamental rights.

Data protection authorities are also active in the field, as their awareness campaigns can include initiatives targeting directly children (for instance,

[20] Children's Online Privacy Protection Act of 1998, 5 U.S.C. 6501–6505.

[21] G. González Fuster, P. De Hert, and D. Kloza, *State-of-the-Art Report on Teaching Privacy and Personal Data Protection at Schools in the European Union*, Vrije Universiteit Brussel, Brussels 2015, <http://arcades-project.eu/images/pdf/State_of_the_art_report.pdf> accessed 25.05.2016.

[22] On this subject, see notably: P. Hladschik and D. Steurer, 'Human Rights Education – Know Your Rights!' in M. Nowak, K.M. Januszewski and T. Hofstätter (eds.) *All Human Rights for All: Vienna Manual on Human Rights*, Intersentia, Vienna/Graz 2012, pp. 606–612.

via their website) or parents, but also teachers, or even direct participation to education by supporting staff members of schools in teaching. Finally, civil society organisations also play a role, be it through active participation or by the preparation of teaching aids.

The inclusion or not of privacy issues in national curricula falls ultimately under the competence of the state, and not all Member States of the European Union have taken steps in that direction. What is clear, in any case, is that different actors generally cooperate in privacy education efforts taking place at schools.

Children are typically the ultimate target of privacy education at schools. Initiatives, however, might be designed to first reach their teachers. Occasionally, privacy education efforts at schools attempt to get actively involved also parents, in the understanding that they are a crucial component of children's privacy protection and that the best way to approach them is through schools.

2.2. WHERE AND WHEN?

Privacy education can take place at any educational level. If in some Member States of the European Union elements of privacy education appear already in the curricula of kindergartens, generally it will take place in schools, ranging from elementary via middle to high schools.

Educational efforts taking place at schools are not the only way in which attempts to increase the privacy awareness of children are made. Children, parents and teachers can also be targeted through media, be it traditional (e.g. television or newspapers) or new media (e.g. websites). A variety of activities is organised in public spaces (e.g. libraries or educational fairs) or during specific events (e.g. Safer Internet Day).

2.3. HOW?

In the Member States of the European Union where privacy education is formally part of school education, it might be integrated in different ways. For instance, it can be a dimension of education on general awareness of fundamental rights, or part of the computer literacy programme, which includes the responsible use of information and communication technologies. Children learn the former usually within a 'civic education' class, while the latter within 'computer science' or 'media' class, but these labels can differ from country to country.

Privacy education supported by data protection authorities is an ingredient of their wider public awareness-raising tasks, which may target children either directly or indirectly, predominantly via their parents and teachers, educational professionals and principals who would later on reach children.

When data protection authorities engage directly, they can offer on-line resources (including dedicated sites), launch especially designed campaigns or put in place competitions. They normally intensify their activates on celebrations such as the European Data Protection Day (28 January). They sometimes attend open days of various schools and libraries as well as trade fairs.

When these authorities engage indirectly, they might go to schools for study visits or training activities such as lectures, seminars or workshops. These might be standalone activities or form a part of a series. Attendance thereto is usually free. Many data protection authorities have issued awareness-raising materials for children, either on-line or in print, in form of dedicated websites as well as posters, postcards, booklets, brochures, leaflets, comic strips, videos, tests, quizzes and sometimes even guidelines and lesson plans. Again, these resources are usually freely available.

Data protection authorities cooperate with each other, both on a European and an international level. The Article 29 Working Group, an advisory body comprising all data protection authorities from Member States of the European Union, issued in 2009 a seminal opinion on the protection of children's personal data.[23] The 35th International Conference of Data Protection and Privacy Commissioners (Warsaw, 2013) adopted a *Resolution on Digital Education for All*,[24] setting in motion the work of an International Data Protection Working Group on Digital Education. In parallel, data protection authorities from all over the world often organise study visits and staff exchanges among their counterparts with a view to share best practices.

Data protection authorities also cooperate with other bodies and institutions beyond schools, such as local city councils or libraries. For instance, the French

[23] Article 29 Working Party, *Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)*, WP 160, Brussels, 11 February 2009 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf> accessed 25.05.2016. This Opinion was preceded by: Idem, *Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools)*, WP 147, Brussels, 18 February 2008 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp147_en.pdf> accessed 25.05.2016.

[24] International Conference of Privacy and Data Protection Commissions, *Resolution on Digital Education for All* (2013) <https://icdppc.org/wp-content/uploads/2015/02/Digital-education-resolution.pdf> accessed 20.05.2016.

data protection authority, led the setting up of 'EducNum', a collective for digital education bringing together more than 60 partners from the field of education, research, digital economy, civil society and political institutions.[25] Activities of these authorities can also target policy makers, often with the view to shape school curricula or otherwise inform and influence policy development. Often their contribution is based on studies commissioned to gather knowledge on the state-of-the-art, e.g. the perception of privacy threats among children.

International and supranational bodies might set up standards and policies for privacy education, but also be directly involved in educational activities. For example, the Council of Europe marked the 50th anniversary of the European Convention on Human Rights with the launch of 'COMPASS', a digital tool pursuing the development of human rights knowledge, skills and attitudes. One of the themes developed therein were the rights of children.[26] In 2007 was first published Council of Europe's Internet Literacy Handbook,[27] now in its third edition, and in 2012 the Council set up a Strategy for the Rights of the Child (2012–2015).[28]

The efforts of the European Union with regard to privacy education were given support by the € 50 million 'Safer Internet Programme' in 1999. Following the adoption in 2012 of the European Strategy to Make the Internet a Better Place for Children[29] it is now referred to as 'Better Internet for Kids'. Built on four pillars, the Strategy noted, in the context of 'Stepping up awareness and empowerment', that

> children, 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.[30]

The Strategy further 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'.[31] Observing that online safety as

[25] <www.educnum.fr> accessed 18.05.2016.

[26] <www.eycb.coe.int/compass> acceded 18.05.2016.

[27] Council of Europe, *Internet Literacy Handbook*, 3rd ed., Strasbourg 2007, <www.coe.int/t/dghl/StandardSetting/InternetLiteracy/InternetLiteracyHandbook_3_EN.asp> accessed 26.05.2016.

[28] Council of Europe, *Strategy for the Rights of the Child (2012–2015)*, CM(2011)171 final, Strasbourg, 15 February 2012, <www.coe.int/t/DGHL/STANDARDSETTING/CDcj/StrategyCME.pdf> accessed 26.05.206.

[29] European Commission, *European Strategy for a Better Internet for Children*, COM(2012) 196 final, Brussels, 02.05.2012.

[30] Ibid., p. 8.

[31] Ibid.

a specific topic was included in the school curricula of more than 20 education systems across Europe, the Strategy ultimately noted that

> schools 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.[32]

Member States of the European Union were thus invited to step up the inclusion of teaching online safety in school curricula by 2013, reinforce informal education and provide for 'online safety' policies in schools and adequate teacher training, also with the support of public-private partnerships. The industry, in its turn, was invited to cooperate in 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, exchange and promotion of best practices among Member States in the areas of formal and informal education on online safety. However, 'privacy' education through this online safety prism focuses primarily on raising awareness about online threats for children, as opposed to placing emphasis on awareness of their fundamental rights and their multiple dimensions.

2.4. WHAT?

A common feature of existing materials is that they generally do not simply aim to transfer knowledge to children, but rather to work towards learning and reflection. The ultimate goal is generally to promote a reflexive, responsible use of emerging information and communications technologies, and in particular of the Internet. These materials also do not focus solely on privacy protection, as educating thereon usually overlaps with teaching about of online safety and security problems, eventually leading to promoting a certain 'digital responsibility'.

The materials commonly address:

- clarifications as to what 'privacy' is; some also explore 'surveillance',
- significance of these notions in the contemporary society,
- suggestions to decide in the first place whether to share personal data or not,
- if personal data are shared:
  - suggestions on how to stay safe on-line, e.g. how to choose a secure password or how to set-up privacy settings in social media platforms;

[32] Ibid.

  - how to give valid consent for sharing data (when possible for children) and how to withdraw it,
  - clarification that once information is shared on-line, it is usually difficult to take it down (i.e. the idea that Internet 'never forgets'),
  - available help and possible remedies, e.g. a right to ask a data protection authority for assistance;
- the role of parents in protecting their children's personal data.

The main purpose of such educational efforts, however, is not always clear. In many cases, emphasis is patently put on teaching children how to reinforce their own privacy and increase their familiarity with their fundamental rights. In other cases, online safety considerations might put a greater emphasis on preventing perceived risks, thus attempting to keep children as far away from threats as possible, as opposed to explaining to them that they have a series of subjective rights and the power to demand compliance with some data processing obligations.

To conclude this part, the following diagram provides an overview of who does what, for whom, how and where in educating European children on privacy protection.

Table 1 – The privacy education landscape at a glance

Who?	To whom?	Where?	How?	What?
– regulators • governments • supranational organisations • international organisations – standard setters – data protection authorities – non-governmental organisations – industry	– children – parents – teachers – carers	– kindergartens – schools • elementary • middle • high – media – public spaces – public events	– official curricula – indirectly • resources for teachers • resources for parents – directly • resources for children	– definitions – significance – rights – remedies – safety tips

3. CONCLUDING REMARKS

Both the reality and severity of privacy problems is often underestimated. It is already bad when any individual falls victim of any of such problems, but the things get much worse when the victim is a child. Children are vulnerable predominantly due to their insufficient awareness of threats in general, and especially of those arising from the use of technology, and thus they merit special protection. At the same time, they are also 'digital natives' who navigate seamlessly in the digital world.

The protection of privacy starts with the individual's own care. The law then steps in to offer universally a relatively high level of protection but it also leaves room for manoeuvre to individuals, for example by means of consent. In order to take advantage of this choice, an individual must be first and foremost aware of possible threats and of how to act against them. Children, just as their parents and teachers, can relatively successfully deal with many privacy problems if they possess sufficient knowledge about them. We cannot, however, fall into the trap of believing that children's privacy will be protected if we insist they should always think twice and, in general, know better. If they really knew better, they would probably no longer be children.

This is precisely where a broad approach to privacy education steps in. Such education is not only about dealing with privacy problems or about being conscious of them. It has the ambition to make children aware of threats, but also of rights and rules. It is a reminder of the fundamental rights dimension of privacy and of the fact that children need to know about privacy not just to keep them safe, but primarily to help them grow as free individuals.

Education on privacy has been present in European schools already for some time and its value is widely acknowledged. The multiple efforts undertaken thus far by multiple actors at various levels deserve to be applauded, but more is still needed. We foresee here a special role for data protection authorities. Due to their role in society and – more importantly – the expertise they hold, they can play a crucial role both in energising and improving privacy education in schools. They can actively push in that direction, in the name of their awareness raising obligations. They can also effectively contribute to its quality, notably ensuring that information that is disseminated through schools is in full accordance with applicable legal provisions.

We found it exemplary that with the passage of the General Data Protection Regulation in the EU, data protection authorities have become legally obliged to raise awareness about privacy protection in a wide sense and – in doing so – they are obliged to pay special attention to children, due to their vulnerability.

Consequently, children should definitely not be underestimated, but they should also not be left alone when navigating the digital world with its many slippery roads. Their 'digital nativity' should be complemented and balanced with a 'digital responsibility'. Schools are one of the best places, together with the home, to teach them about all this, treating them like children but also – and at the same time – as real data subjects.

Education is obviously not a panacea for all privacy problems. Privacy protection of children requires much more, including adapted information and strict rules on the processing of children's data. It is nevertheless a jigsaw piece in the puzzled privacy protection landscape.

PART II

THE TEACHER’S MANUAL

TEACHER'S MANUAL PRESENTATION

This manual aims to provide a useful tool for teachers of any EU school wishing to educate children and teenagers about privacy and personal data protection. Its ambition is to be of direct use all across the EU, and thus it focuses on providing essential knowledge that is valid and relevant among all EU Member States, based on relevant legal instruments applicable across Europe, and most notably the EU Charter of Fundamental Rights. For additional legal information, teachers should refer to the national data protection authority of their own country.

The text is written in language that will help teachers find the right words to explain to their pupils the issues at stake. It is structured in ten chapters covering different facets of privacy and personal data protection, all of special relevance for children and teenagers. Each chapter advances a set of key ideas and puts forward subjects for discussion, recommended activities or concrete tips, depending on the subject. When appropriate, chapters include also 'real life' cases or examples. Additionally, the final sections of each chapter highlight ideas that could be especially important for younger children, and those that could be of special interest for older or more advanced pupils. Teachers are encouraged to familiarise themselves with the whole manual, and to freely use the different elements of the chapters in accordance with the needs of their class.

The following authors contributed to the text and graphics (in alphabetical order): Viktor Árvay (NAIH), Jelena Burnik (IP RS), Paul De Hert (VUB), Piotr Drobek (GIODO), Gloria González Fuster (VUB), Urszula Góral (GIODO), Dariusz Kloza (VUB), Laura Kozma (NAIH), Paweł Makowski (GIODO), Marta Mikołajczyk (GIODO), Kata Nagy (NAIH), Anže Novak (IP RS), Zsófia Szántó (NAIH), Julia Sziklay (NAIH), Polona Tepina (IP RS) and Zsófia Tordai (NAIH).

1. INTRODUCING PRIVACY

What is privacy? And why is it important?

OBJECTIVES

- Learn about privacy.
- Shape a reflective attitude towards it.
- Understand the importance of privacy offline and online.

KEY ISSUES

Privacy is about protecting what is **private**, about shielding yourself and what is closest to you from the gaze of the others. Privacy is also about the possibility '**to be yourself**' and to have the chance to live in accordance with your own preferences, shaping your life in line with your own will. Privacy is thus also about being able to reject interferences with your private sphere by others – be it the State, parents, friends, teachers or strangers.

The value of privacy has been recognised by psychologists. They suggest there is a '**restricted privacy**' and an '**open privacy**': 'restricted privacy' would be about keeping things secret, preserving the **intimacy** of your body, your emotions, or your thoughts, whereas 'open privacy' would be about being able to **express yourself in public**. Both types of privacy are necessary, notably to maintain our sense of self-worth and to protect our image in the society and social relationships.

Childhood is a unique period in each human being's life, during which the protection of privacy is particularly important. **All children**, regardless of where they live, have the right to life and development, to grow up in an environment that respects freedom and dignity, to **privacy** and to **personal data protection**.

Privacy has always played a pivotal role in the functioning of **modern democracies**, and has thus been recognised as a **human right**. Its legal recognition became especially prominent after the Second World War as a reaction against totalitarian regimes. Its value is acknowledged in all European legal systems, typically as a **fundamental right**, as well as internationally. States shall not interfere with the right to privacy, but they must also ensure that this right is protected from attacks by others, like private companies.

The **Charter of Fundamental Rights of the European Union** enshrines the right to respect for private life in its Article 7.

New technologies raise special challenges for the protection of privacy. We increasingly communicate, work, study, have fun using technology… we actually increasingly **live with and through technology**. Everybody – also children – should be able to enjoy their privacy rights always, when they are **offline** and when they are **online** or connected.

REAL LIFE CASES

Famous people are particularly vulnerable to privacy violations. The media know that publishing funny or unexpected pictures about them may attract many curious people. The photographers known as '**paparazzi**' can spend many hours trying to catch images of celebrities. Even famous people, however, have a right to privacy, and thus the media should not publish pictures of them that do not have a particular public interest (for instance, because they are just going about their daily life) or if they reveal something very private that the celebrity would prefer to keep private (for instance, if they went to the hospital for a health check). Many famous people have been fighting against the publication of pictures of them in the press – including actors, fashion models, and princesses.

IDEAS FOR DISCUSSION

Pupils can discuss these questions:

1. ***Personal experiences***: Have you ever had your privacy violated? What happened? How did you react?

2. ***Shaping a reflexive attitude:*** Can you imagine a society where there would be no privacy at all? Would you like to live there? Could you think of any problems that would emerge? Try to think of special categories of people that could have special privacy needs: people with health problems they do not want to share publicly, journalists wishing to carry out confidential investigations, teachers who wish to keep some distance from their pupils (and vice versa), people who want to be politically engaged that do not want to be scrutinised by their opponents, etc.

RECOMMENDED ACTIVITIES

1. This exercise can help pupils think about what constitutes their privacy, how we might need more 'privacy' in some contexts than in others, and how it feels to have privacy invaded:
   - Everybody in the classroom should greet each other, as if they had not seen each other for a few months.
   - **Observe** the different ways of greeting, and **discuss** these questions: Do close friends greet each other in the same way as not so close friends? Would you greet a member of your family differently? How do strangers greet when they meet for the first time? And how would you feel if a stranger wished to greet you too effusively?

2. To explore the many dimensions of privacy, write on the board the word 'privacy' and invite pupils to **draw a mind map** of related terms. First, write down any words connected to privacy. Second, try to create groups of words that seem to relate to different dimensions of privacy (for instance, privacy of the body, privacy of communications, privacy of thoughts and feelings, etc.).

FOR THE YOUNGEST

Young children should learn that privacy is about keeping things for oneself, but also about having space to be themselves. They should know that people **should respect their privacy**, and that they should **respect other people's privacy** too.

FOR THE MOST ADVANCED

Most advanced pupils should understand that the right to privacy is a **fundamental right** that plays a crucial role in the functioning of democratic societies. It marks the limits of the State's intervention in the lives of individuals, helping us to live in freedom.

2. INTRODUCING PERSONAL DATA PROTECTION

What is personal data? And what does it mean to have a right to the protection of personal data?

OBJECTIVES

- Discover the meaning of **personal data protection**.
- Find out what '**personal data**' is and why it should be protected.
- Learn about '**sensitive data**', or data deserving special protection.
- Increase awareness of our **rights** as data subjects.

KEY ISSUES

In addition to a right to privacy, the law also grants individuals a **right to the protection of their personal data**. This right is recognised as a fundamental right in modern societies because of the dramatic effects misuse of personal data can have on the life of individuals: for instance, when personal data are mistakenly linked to the wrong person in a public file, or when an organisation gains too much knowledge about some people by accumulating a lot of disparate information.

The first laws on personal data protection saw the light in the **1970s**, when governments and companies started using computers to store and process information on individuals. There were fears that the machines would give to some big entities more and more power over individuals, and individuals, in their turn, would have less and less control on what happened to information about them. Nowadays, the processing of personal data is more widespread than anyone had imagined, making the right to personal data protection more necessary than ever.

The **Charter of Fundamental Rights of the European Union** enshrines the right to the protection of personal data in its Article 8.

The law protects all '**personal data**', that is, any data that can be **traced back to a particular person**. It might be a piece of written information, a picture, a video, or even a sound recording. It could be a telephone number, an email account, or somebody's shopping list, as long as these can be linked to a specific individual. Even if the data look uninteresting or irrelevant at first sight, they will be considered personal data that deserve protection. The combination of different apparently uninteresting data could indeed reveal many interesting things about a person. Thus, the law protects all personal data in general, and applies even when data are just collected.

There are some types of data that are particularly **sensitive**, and thus are especially protected by law. We consider sensitive data, for instance, the data that refer to peoples' political or religious **beliefs**, their **health**, their **ethnic origin** or their **sex life**. These types of data are granted reinforced protection to avoid people being discriminated on the basis of any of these issues, and to prevent any stigmatisation, but also to allow people to keep these matters as private as they wish.

To prevent the misuse of personal data, the law gives **a series of rights** to any individual whose personal data are processed, imposes **obligations** on those who wish to gather or use other people's personal data, and foresees that an **independent data protection authority** shall monitor that all existing rules are actually respected.

Individuals whose data is processed are called '**data subjects**'. We, as data subjects, all have the right to:

- be informed about **who** uses data about us, **which data** they use, and **for which purpose** ('right to be informed');
- **ask** those who use our data to tell us exactly which data they have about us ('right of access');
- require the **correction** of any wrong data ('right to rectify');
- require the **erasure** of data when those who use it have no valid reason to do so ('right to object');
- **refuse** or **consent** to some uses of our data;
- **complain** to an independent authority if our rights are not respected; and
- claim protection of our rights before a **court.**

REAL LIFE CASE

In 2007, an Austrian university student, Max Schrems, was studying the laws on privacy and personal data protection and decided to test his 'right of access': he had a profile on Facebook, so he contacted them and asked for a copy of all the data Facebook had about him. As he had only been using Facebook for a few years, and not very often, he was very surprised when, in answer to his request, they sent him more than 1.200 pages of information about him. He was even more surprised when, reading all the information, he discovered that Facebook kept pictures that he thought had been deleted, as well as other data that he believed they should not have. Since then, Schrems has initiated a European-wide initiative putting pressure on Facebook to respect all their obligations, notably by taking them to court.

IDEAS FOR DISCUSSION

1. ***Thinking about the problem.*** Personal data protection applies whenever people collect personal data, even if they just want to collect the data, store them, and promise never to use them at all. Pupils should be invited to think about why is this so: Why could it be a problem that an organisation or company starts collecting plenty of data about everybody? Do you think it should be allowed for them to collect data about you without you knowing?

RECOMMENDED ACTIVITIES

1. ***Recognising personal data.*** The protection of personal data applies to all personal data, but it is not always easy to know if data are 'personal data' or not. As a matter of fact, data could not be 'personal data' at a certain moment, and become 'personal data' afterwards. To understand better these issues, pupils should **look at a picture** of somebody whose face they cannot see, and discuss whether they think it is personal data or not. They should consider then what would happen if somebody tagged online the picture with the name of the person: Would it be personal data?

FOR THE YOUNGEST

Youngest pupils should be made aware that whenever somebody wants to have data about them, they have some **rights** on that data.

FOR THE MOST ADVANCED

Advanced pupils should know how to recognise what is personal data, and have a clear view of their **rights** upon such data: to know who has them and why, to access them, to rectify them and sometimes to have the data deleted.

3. WHO WANTS YOUR PERSONAL DATA?

Why is the protection of personal data so important nowadays?
Who is interested in getting our data, and which obligations must they respect?

OBJECTIVES

- Get a picture of why organisations collect, store and use our personal data.
- Learn about the obligations they have when they use the data.

KEY ISSUES

Nowadays, **we all produce huge amounts of personal data** on a daily basis. We create personal data when we are **online**, sometimes because we post information, pictures, or videos about people or share them with others, or simply by checking our emails, reading online news, playing online games – because these activities generate data that might be linked to us. We also create personal data **offline**, when we make a phone call, when we shop and pay with a bank card, when we use public transport, or even just when walking by – if our image is caught by a CCTV camera. In reality, an increasing share of our **offline** activities often have an **online dimension**: when we go to the cinema, to a concert or to a football match we might buy the tickets online, also generating more data.

Generally speaking, companies and organisations collect, store and use our personal data to deliver a specific service and deliver it the best way they can. Often they will pursue a **highly important objective**, like providing childcare or medical treatment.

Some companies, however, like to collect **as much data as possible** about people in general and about their customers in particular basically for what is known as **'marketing purposes'**. This allows them to refine the way they work and increase the number of costumers or make them spend more money for their services.

Personal data can thus have a considerable **economic value**. For many companies, personal data are an object of desire and a source of considerable revenue: some of them use personal data for advertising and making or increasing their profit. Personal data can also be of **great interest** for **public authorities**, as they can allow them to gain new insights on individuals or groups of individuals.

The uncontrolled use of personal data, however, could grant private companies and public authorities excessive power, leaving individuals in a delicate position.

To prevent the misuse of personal data, the law imposes a series of obligations on those who wish to process them. Known as 'data controllers' they have the obligation to:

- process personal data **fairly**;
- process personal data only for a concrete, **specified purpose**;
- use as little data as possible (that is, use only data that are adequate, relevant and not excessive) and store them **only as long as this is necessary;**
- keep the data **accurate**, **complete** and **up-to-date**, ensuring their quality; and
- keep the data **safe** and **secure,** preventing access to anyone who does not have the right to lay hands on them.

IDEAS FOR DISCUSSION

1. ***Data breaches:*** Pupils should think about the importance of imposing a series of obligations on companies and organisations that use huge amounts of personal data by reflecting on data breaches, that is, the cases when the wrong person gets access to personal data stored by a company or institution. They should consider questions such as: Have you ever heard of any case of 'data breach', or about companies or organisations losing control of the data they have? Would you be worried if a company that has information about you had been attacked by hackers? Which kind of 'data breaches' would worry you the most? Why?

2. ***Hackers with good intentions?*** Following up the previous discussion, pupils should consider the fact that some hackers claim they actually unlawfully try to access data just to demonstrate that the security measures in place are not good enough, and that the ultimate goal of their unlawful actions would be to push companies to reinforce security measures, and thus to provide more effective protection. Pupils might think, for instance, of the case of company producing electronic devices for children (such as toy cameras, or toy tablets) that would be attacked by hackers aiming to reveal serious security failures in the way in which the company stores the data of children: Would hackers have the right to do so? What are the possible risks linked to their acts? Would there be better ways to address the problem?

RECOMMENDED ACTIVITIES

1. ***Loyal clients.*** Many supermarkets and commercial chains encourage their clients to have loyalty cards that they need to or may show every time they shop. This exercise aims to start a reflection in the class about the loyalty schemes and the processing of personal data that they entail.

- First, pupils should **talk about** their perception of loyalty cards: Do you think they are useful for costumers? Do you think they are useful for companies? What kind of information do you think companies collect through these cards?
- Second, each pupil should **pick up** a loyalty card that they or their family uses, and provide a short description of: 1) the information that one has to give to the company to obtain a card; 2) the information that the company collects when they use the card, and 3) the purpose of this data collection according to the company. This might require checking up the company's website or a brochure, or asking them.
- If there are pupils whose family does not use any loyalty card, they can, as **an alternative**, describe the information that shops collect about them when they shop, if any. For instance: when they shop online, do companies register information about their shopping activities?
- **Share** and **compare** the results of individual explorations.
- **Discuss** what can be the advantage for companies to collect information about their clients.
- **Reflect** about what has been learnt through the exercise: Were pupils aware of the data that was collected about them and their family? Do they think people are generally fully aware of what is happening to their personal data? Would it be useful for them to be better informed?
- Finally, **reflect** specifically about possible privacy risks: Is it a problem if a company holds a lot of information about what their family consumes? Pupils should think about what could reveal consumption patterns for instance linked to food, or to cultural products: who could be interested in knowing whether the members of the family eat healthy foods? What kind of information can be deduced from the books or films somebody is buying? Would any of these data be sensitive?

FOR THE YOUNGEST

Youngest children should learn that the data about them are **precious**, that people should only collect data about them if they have a good reason, and that they can only do it very carefully.

FOR THE MOST ADVANCED

The most advanced pupils should be made aware of the **vast quantity** of personal data that we generate daily, the many **reasons** why a **variety** of companies and organisations might be interested in using them, and the purposes for which the data could be used. They should also learn that whenever somebody processes personal data, some **obligations** must be respected in order to protect us.

4. DECIDE WISELY, AND REMEMBER TO LET OTHER PEOPLE DECIDE TOO

We all have a say when somebody wants to collect or use our personal data. This means that people should take into account our wishes with regard to what happens to our personal data and that we should do the same when it comes to other people's data.

OBJECTIVES

- Learn about the possibility to **refuse** or **consent** to the collection of some personal data.
- Be aware that consent can be **revoked.**
- Understand that sometimes we need to ask for **other people's consent** before sharing content online.

KEY ISSUES

Sometimes we are **obliged** to give some personal data about us to other people. If we want to have a pizza delivered home, we surely need to give our address to the pizza company – otherwise they wouldn't know where to deliver it.

In some cases, however, companies would like to collect **more data than strictly necessary.** They might wish to know some additional data about their costumers or the users of their services, like their age, gender, or favourite hobby. They may ask for these data, but they need to tell what they plan to do with it, and should give people the possibility to **refuse** or to **consent.**

To be valid, the consent of the person needs to be **freely given**, **specific**, **informed** and **unambiguous**. This means that:

- we cannot be forced to 'consent' to give our data;
- people can only ask us to consent to specific data uses, and not generally to whatever purposes they might think of;
- people can only ask us to consent if they give us detailed information about we are consenting to; and
- people can only say we gave our consent if we expressed this clearly.

Before deciding whether to accept or refuse a request for consent, individuals should take the time to understand **which data** will be collected, **for what purpose**, who will be **responsible** for keeping the data safe, and **how to contact them** if they change their mind and prefer the data to be deleted. If all this is not clear, or if they are not comfortable with any of this, individuals should **not consent**.

As it can be difficult for **children** to understand the consequences of giving personal data away, the law says **that when they are using online services directed to them they cannot be asked to consent** before they reach a certain age. Therefore, if a company or organisation wants to ask children who are not old enough to consent by themselves for personal data, they should **ask their parents** (or the person holding parental responsibility over the child), who will then refuse or consent. This does not mean that adults do not have to take into account the children's' views on all this, which they should actually take into consideration as much as possible. Indeed, children have a right to **express their views** in all matters that affect them.

Even when somebody has consented to give away personal data about themselves, they remain **free to change their minds**. This is particularly important in relation to data that might let other people know where individuals are, known as **'location data'**. It could be that a person accepted to have her mobile phone located by an application to search for an address, but then wishes to move around untracked by others. It is her right to revoke the consent. Devices that give information about where they are should actually regularly remind people about it: it could be they forgot they had given consent, or that consent had been given by another person using the device.

Everybody who is in a position to give consent has also the right to **revoke the consent**. Additionally, when parents gave consent on behalf of their child, but the child has grown up and, having obtained the capacity to consent, prefers to revoke such 'parental consent', they can also do it.

Finally, it is important to know that we can infringe **other people's rights** if we do not ask them whether they consent to us sharing some data about them. When we wish to post online a picture with other people, we need their authorisation. We should ask them if they agree with the idea, and **respect their decision** if they tell us they prefer not to have the picture online. If the person is a minor, we should ask the parents or a guardian.

IDEAS FOR DISCUSSION

1. ***Freely given:*** In principle, we are only able to ‘consent’ to some data processing practices when we are completely free to say no. Sometimes, however, those who ask for our consent seem to be in a special position, for instance because they are very popular, and it is not that easy to refuse. Pupils should think whether they feel really ‘free’ to use or stop using the online services and applications that they use regularly (and which collect personal data about them), like social networking platforms. Consider questions such as: Why do you actually use a specific service and not another? Is it because most of the people you know use it too? Do you feel pressure to use a service because of this?

RECOMMENDED ACTIVITIES

1. ***Which terms and conditions:*** This exercise is aimed at pupils who are mature enough to actually consent to data processing practices. It aims to illustrate that sometimes we express our ‘consent’ without taking the time to be properly informed about what we are consenting to.
   - Pupils should, first, **write down the name** of an application or online service that collects personal data and that they use particularly often. They should ideally not all chose the same, but at least a few different services.
   - Second, they should write down **anything that they remember** from the ‘terms and conditions’ or ‘privacy policy’ of that service, which are supposed to explain what does the company do with their data, and that they certainly had to accept in order to register. If they do not remember much, they should at least try to remember if they came across ‘terms and conditions’ or a ‘privacy policy’ at all.
   - Afterwards, they should **compare** their answers with reality, by checking the service or app and their real ‘terms and conditions’ or ‘privacy policy’.
   - Finally, the class should discuss what can be learnt from this experience: Do pupils actually know much about what the companies tell them? Did they really take the time to read? If yes, do they think everything was well explained?

FOR THE YOUNGEST

Youngest pupils should know that they **should never give away data about them** without the permission of their parents. Also, they should understand that they cannot post information about other people (including sharing pictures or videos) without asking them first.

FOR THE MOST ADVANCED

The most advanced pupils should acquire the **skills necessary to give (or refuse) consent**: when somebody asks them for their personal data, they should make sure they understand what is the purpose, which data will be taken, who will keep them and for how long, and how to contact them if they want more information or their change their minds. They should always feel free to say no, and question anything they did not understand. Equally, before using **personal data about other people**, they should **ask them** – and respect their choices.

5. DIGITAL IDENTITY

How to grow up with a digital identity? Online information about us can have serious implications in our life so it is important to ask ourselves what should we share, when and under what circumstances.

OBJECTIVES

- Become aware of our online presence, and adopt a more reflexive attitude towards disclosing information online.
- Think about the importance of people's **digital identity**.
- Reflect about how to control our digital footprints.

KEY ISSUES

The combination of all online information about us defines what can be called our '**digital identity**' or 'online presence'. This is the picture of us that somebody could get if they did not know us at all, but knew our name, just by making a search with an online search service. It can be seen as an element of our '**identity**', which has many dimensions: we are not exactly the same person in the eyes of our grandmother as in the eyes of our best friend, we do not behave exactly in the same way in our room and in a shop, we might not have the same reputation at school and where we spend the summer holidays.

As people increasingly use the Internet, **'digital identities'** and **'online reputation'** have become very important. When somebody looks for a job or applies for a scholarship, potential employers and funders could have a quick look online, to get some supplementary information about the candidate, and, if they find something they dislike, not hire them or give them the scholarship. If one day you meet somebody you would like to be your friend, or your partner, it could also be that this person checks up the Internet to know more about you.

Our 'digital identity' is never exactly the same as our real identity. In some cases, our 'digital identity' is particularly **misleading**, and makes people believe that we have done things we never did, or keeps reminding everyone of something that we consider is a thing of the past.

Europe has now recognised a '**right to be forgotten**' (technically speaking, a **'right to be delisted'**), which allows individuals to request search engines not to show, when people look their names up, any results that are **inadequate, irrelevant, or no longer relevant.** The existence of this right reminds us that the results that people see when they look us up can have a real impact on our lives.

This right, however, does not mean that one can ask for the removal of any personal information that is online. Actually, even when we do have the right to have some information removed, it could be that **in practice it is not easy** to get any data off the Internet. Or it could be that when it is removed other people have already copied them on their devices, and spread it around.

The best thing to do is, thus, to **think twice** before we post any information or media online. Minors should be aware that all data about them are like 'digital breadcrumbs' or '**digital footprints**' that could one day be **traced back to them**, and that are **difficult to erase**. Some are actually so difficult to erase that it might be better to think about them as '**digital tattoos**' that could threaten to stay with you forever.

REAL LIFE CASES

- A Spanish man was once caught urinating in public and sanctioned for that. In accordance with Spanish law, as the police did not know where to send the fine, they made a public announcement in an official journal, which was also published electronically and made accessible through search engines. The man eventually started to work as the headmaster of a school. A pupil made a search using the headmaster's name, discovered the sanction and shared this with all pupils. This seriously affected the image they had of their headmaster, rendering his job very difficult.

- A Hungarian student had made some pictures during a history lesson at his University, where one could clearly see his face and some Nazi symbols. These pictures where published online, and when people searched for the student's name on the Internet, they automatically appeared. He was worried that this could affect his chances to get a job, so he asked the search engine to stop linking the pictures to searches made using his name. With the help of the data protection authority, he managed to obtain this.

TIPS

There is something online about you that you would prefer to get rid of?

- First, contact the person who published it, and ask them to delete it.
- If it was you who posted it, try to delete it yourself. All online services should have a way to get rid of your whole profile or account, if you wish.

- If that does not work, contact the person or the company who owns the website or the platform.
- If that still does not work, ask an adult to help you. You can also contact your data protection authority for guidance or help.

IDEAS FOR DISCUSSION

1. ***Why should online reputation matter?*** Pupils should think about when and why could their online identity matter. This can notably be done by:
   - Thinking about **typical situations** where people may check out online information about other people. For instance: related to work (Would you do an online search on somebody before offering them a contract to work in your company?), housing (Would you do an online search on somebody before sharing with them an apartment?), social relations (Do you think it is possible that people you meet in the future will be tempted to know more about you by checking the Internet?), etc.
   - Thinking about **special categories of people** for which online reputation can be very important. Pupils could discuss what would happen if any of them was to have a career in politics, or become a famous actor, or a famous sportsperson: Would there be a special interest in online information about them? Would they then prefer to have some pictures or data about them offline?

2. ***What feels totally wrong online?*** Pupils should think about which data can be especially problematic when publicly available online. To do so, they can reflect on their personal experiences, and try to remember if they have ever seen something that gave them a really bad impression about somebody. Think, for instance:
   - About data that could be **too intimate:** Are there things it could be wiser never to share online? What? Why?
   - About data that could be **misunderstood:** Are there things that could be too easily taken out of context? Are there pictures that are ambiguous and could lead to wrong interpretations? Are there profiles that give a too partial account of who you are?
   - About data that could become **rapidly obsolete**: Are there things that look cool today but might be completely out of fashion tomorrow? Have you ever felt ashamed about something you had done a few years ago?

RECOMMENDED ACTIVITIES

1. Pupils should be encouraged to **explore** which **information about them** is available online. In some cases, this could lead them to unexpected

discoveries, like seeing that some information which they thought was private is actually available to the general public, or to the realisation that what they believed was only accessible to their (online) friends is actually also accessible to anybody. To avoid any unpleasant situations for the pupils, they should be able to do their exercise on their own – possibly at home.

- They could be invited, afterwards, to **reflect in writing** and/or **discuss** in the class on what they have learnt through this experience.
- As they explore in private the information about them that is available online, some pupils might discover that **there exist other people in the world that share the same name**. Pupils should be encouraged to talk about their experiences about finding information about homonymic persons. In particular, they should consider this question: What could happen if somebody was looking about one of the pupils in the class that has the same name as other people?

FOR THE YOUNGEST

Youngest children should realise that anything that is online could be seen by many different people, and that the different pieces of information about us that are online give people a certain image of us, so we need to think twice about what to put there.

FOR THE MOST ADVANCED

The most advanced pupils should understand that online information could have serious implications for their lives, so it deserves all of their attention. As a basic rule, they should avoid publishing online any information they would not be comfortable sharing with a wide audience.

6. ONLINE TARGETING

Being connected is not only about actively posting and sharing information that we chose: whenever we use electronic devices, we could be producing and sending away data about us and about what we are doing. These data are particularly valuable for companies that sell advertisement space, that often collect our data while offering 'free' services.

OBJECTIVES

- Realise that online activities are often monitored.
- Learn that companies show ads and products on the basis of previous behaviour.

KEY ISSUES

Whenever we use computers, mobiles, tablets, game consoles or any device to communicate or connect to the Internet, we are **generating data**. Some of this data are **about what we are doing**: the websites we visit, the videos we watch, the games we play, the people with whom we exchange messages, or the searches we make, as well as many other types of data. Some of the data are **about where we are**: this data are used to locate us on a map, or to connect us to a local version of a website, for instance. Finally, some of the data are **about us** (our phone number, our email account, all our identifiers): they allow companies to link up all this information and build a quite detailed picture of **who we are**, the kind of life we live, **what we like** and **how we could spend our money**. As a matter of fact, they might also have a pretty accurate idea of how much money we have. Companies and other organisations, indeed, use all of this information to '**profile**' people, placing them in different categories.

We are not always **aware** of all this data collection, even if, in principle, whoever collects our data and uses them should tell us about it clearly. In practice, people tend to accept all sorts of '**terms and conditions**' before using an Internet service or downloading an application without even reading them. If they read them, they might not really understand them – which most probably is the case if they are minors.

Likewise, nowadays websites that collect personal data using what is known as '**cookies**' have to inform the public about what data is being gathered and for what purpose, allowing them to accept or refuse. Most people, however, do not have time to think about the cookies of each website, or have trouble understanding what is actually at stake.

Most of the time, companies will actually **profile** people based on their online behaviour in order to **sell advertisement space**.

If a website is visited often by children, they will try to sell advertisement space on it to toy companies, arguing that they are the best public for it. As a matter of fact, companies are also able **to adapt the content of each ad to what they think is of interest for each user.** When children that seem to like puzzles visit the website, they will be shown ads for puzzles.

These practices are called '**behavioural advertising**' or **'targeting'.** Minors should be aware of the fact that online content is sometimes targeting them on the basis of their previous behaviour: the links they see when doing an online search are partially determined by data gathered about them, as well as by the products that are given special relevance in some online shops.

Minors should, in general, know that many companies that seem to be offering their services '**for free'** are not asking for money from their users because they **make money** thanks to the data they collect about them. As the more people they attract, the more money they will probably make, it is convenient for them to let people use their services 'for free'.

IDEAS FOR DISCUSSION

1. ***Could little bears spy on children?*** Some companies, including toy companies, are developing 'smart toys' that would interact with their owners and send the company information about the children. The information is, in principle, supposed to make the reactions of the toys more realistic and interesting, but it could also be used by the companies to gather extra data about children. Pupils should discuss whether it seems to them a good idea that children have bears or dolls with cameras and microphones that can record sounds and images and send them to a company. Would they like to have one? If so, do they think they should be able to turn them off? What if they forget to turn them off, and the toy registers things they would not like a company to know?

2. ***Equal chances?*** When we are online, some of the content we see depends on what some companies think we are interested in, or would like to buy, on the basis of the information they have about us (and their interpretation of it). This could mean, for instance, that pupils from the same class are shown different ads when they visit the same website. Sometimes, the content of the

ads displayed might not be particularly important or life changing – some pupils could be shown ads for some clothes, and others for another type of clothes. It could be, however, that the differences are actually about things that matter more: you could see ads for travel that the others do not see, ads for different school or university programmes, ads for different scholarship opportunities, or even different jobs. Pupils should discuss whether they see this as being fair, think of cases where it could be a problem, and talk about possible ways to deal with it.

RECOMMENDED ACTIVITIES

1. ***Anonymous information?*** The following exercise is an invitation to think about the information that can be derived from our activities and preferences.
   - Each pupil should choose a **fictional name** that should cover up their identity, and write on a paper, under their fictional name, a series of pieces of **information** to be determined by the teacher depending on the pupils' age. They can include: favourite TV programmes, favourite clothes, favourite sports, languages spoken, favourite music, recently watched film, recently read book, etc. During this first stage, the teacher should not explain the purpose of the game.
   - All pages should then be mixed. The teacher should randomly pick up a page and start reading it aloud. The author should do their best to conceal their identity, not to be unmasked. All other pupils must **try to guess** who is the author: Can they guess it with one piece of information? Maybe with two? Maybe with three?
   - Afterwards, or in case nobody could guess who the author was, they should all think about **who could be interested** in contacting a person with that kind of a profile: would that data have a commercial value even for somebody who does not know who is the author?
   - The exercise can be **repeated** with different pages/profiles.
   - Finally, advanced pupils can be asked to think about how could companies get **online** information similar as the information provided by the pupils: Does somebody keep track of the things we search for? Does somebody ask us to express what we 'like'? Does somebody have information on products we have been checking? Does somebody have information on the videos we like to watch? And so on.

FOR THE YOUNGEST

Youngest children should be told that many of the electronic devices they use (or could use soon, maybe) are connected and **generate data about their lives**:

mobile phones, computers, tablets, game consoles, … Through all of these devices, companies try to get information about what we are doing to be able to sell us their products and services.

FOR THE MOST ADVANCED

The most advanced pupils should get an understanding of how their activities can be tracked through the different devices they use, and realise that some of the information they see online, like ads, might not be the same as what other people see.

7. KEEPING SECRETS REALLY SECRET (AND DATA REALLY SAFE)

Making sure that our data are protected starts with us. To keep our data safe, we must behave carefully, and take some basic technical precautions.

OBJECTIVES

- Be aware of the threats that can put data in danger.
- Learn how to better protect our personal data.
- Learn about ‘**privacy settings**’.
- Be aware of **‘identity theft’** and ‘**phishing**’.

KEY ISSUES

We keep our **digital data** in many different places. Some of it is in physical things we have, like computers, or tablets, or smartphones. Some of it is actually stored by other people, and we might reach it by logging into an account or profile. It is important that we take all the necessary measures to make sure that our **data is secure**.

We should thus make sure that we protect our devices, for instance by locking them and accessing them with a code. We also need to make sure that we protect our online profiles and accounts. As most of them can be accessed using a password, it is crucial that we have **strong passwords** and that we keep them **strictly to us**.

Keeping our passwords for our personal accounts and profiles secret means keeping them **seriously and strictly to ourselves**, and **not sharing them with anybody**; not even with our best friends, or with the love of our lives. Keeping our own passwords safe is **our responsibility** and we should not share them with anybody.

Pupils should know that if anybody asks them to disclose to them their personal passwords as a proof of their friendship or of their love, they should not accept this, because it could put in danger their data and the data of all their contacts. As a matter of fact, the person who asks should, as a proof of their friendship or love, fully respect their privacy and **stop asking**.

Online, we need to make sure we are always in control of what happens to our data by mastering the ‘**privacy settings’** of the services we use. Privacy settings are mechanisms that allow the users of services to decide (to a certain extent) who will be able to access their profile information as well as any other content they might share.

Even if 'privacy settings' are supposed to help users exercise control over their data, sometimes it is **not easy** to use them: there could be, for instance, different settings to control the information of a profile, to decide what happens to posts, to choose who will see comments to other people's posts, etc.

It is important that minors:

- do not share publicly any information such as their real address, phone number or email accounts;
- have a clear understanding that the information they post, upload or share may be available to everybody, unless they can limit it so it will only be available to a few people, and they should know who these people are;
- know which information can be found when somebody searches for their name or alias.

Keeping our data safe also requires paying attention to the emails we receive. Some of the messages we get may actually be a **fraud**, or a scam. For instance, you could receive an e-mail telling you that you have won an award with a big prize, or inherited a great fortune from somebody you had never heard about. To access the fake award or the non-existent money, they will ask you for some personal information that they will actually use to take money from you.

A particularly dangerous practice is what is known as '**phishing**', whereby people are made to believe that a company they know well wants to have access to some of their **confidential data**. It could a message that **looks like** it has been sent from somebody you trust, like a bank, or an email provider, or the company allowing you to buy online games and applications…

Phishing messages will tell you they absolutely need you to provide your password or any other data such as your date of birth, telephone number or address, and then use this information to access your online accounts making if as they were you, in what is known as '**identity theft**'. With only a few credentials, mischievous people could even try to use your money (or your parents' money).

Minors, therefore, need to be **very cautious** when they receive emails like that and **never give away any confidential information** even if the messages sound alarming or urgent.

TIPS

- Lock your devices so you are the only one that can unlock them, for instance with a password.

- By checking the history of your web browsing, people could see which websites you have been visiting. When you do not want this to happen, remember to ask the browser to stop remembering, or to delete what was already registered (normally, through the 'tools' menu).

- When you install an app on your phone, check which information it wants to access.

- When you receive 'spam' (unsolicited emails), do not open the attachment – just ignore it. It might contain links to malicious software.

- Create **strong passwords** in a way that will allow you to remember them:
  - Do not use as your password data about you such as your birthdate.
  - Do not keep your password near your computer, phone or tablet.
  - Try to use long passwords with a variety of types of characters: include small and capital letters, numbers, signs.
  - Avoid just typing characters because they are close to each other in the keyboard.
  - You can easily remember a password if it comes from a sentence, such as: I Like Strong Passwords and Protecting Privacy: ILSPP.
  - Remember to log off when you use public computers or shared devices.
  - Change your password every now and then, just in case.

- If you receive an email asking you for data, it could be a scam. Take the time the read it carefully, check all the details and, when you can, look up the Internet to see if somebody has already received a similar message, for instance by searching for one of the sentences used in the email with a search engine. Otherwise, ask for advice around you. Remember you should **never send to anybody your passwords** through email. Serious companies will never ask for confidential information to be sent by email: if you receive an email that looks like they are asking for that, it is most probably a **phishing** attempt.

RECOMMENDED ACTIVITIES

1. ***Set your privacy.*** This exercise aims to help pupils realise the importance of paying attention to the 'privacy settings' of the online services or applications they use. Pupils should:
   – First, **chose** an online service or application that they use often, and which has 'privacy settings' or different privacy options. Ideally, not all pupils should choose the same, so there will be different services to compare. Nonetheless, some pupils could work in parallel or together on the same service.
   – Second, **describe** how the service works if the user does not actively change anything: in other words, what are the '**default privacy settings**'? What would happen if you just register? Will your profile information be online and accessible to everybody through search engines? Does this profile information include data that such as your real name, date of birth, a picture of you with your face? What will automatically happen to the data or pictures you send to others or post using your account?
   – Third, **detail** which privacy options are available to users: What can you actually change? Can you set your profile to private? Can you share info with only a few people? Do you really control who will access the data?
   – If there are pupils who do not use any online service or application with privacy settings at all, they could, as an alternative, work on their **offline practices of sharing information**: What information about them is available to people as they walk on the street? What information or pictures do they share with others? Could they change their 'privacy settings' if they wished? How? They could think for instance of: wearing sunglasses, sharing information with somebody only if they promise not to tell anybody, etc.
   – Finally, **share, compare** and **discuss** the results of the different explorations. Consider these questions: Were the pupils fully aware of the 'privacy settings' of the services they use? Do they think these really allow them to control their data? Are they easy to find, and easy to use?

2. ***How do we shape our privacy?*** This exercise should work as an invitation for younger children to think about the ways in which we manage daily our privacy preferences and requirements – and the different 'tools' and strategies we use:
   – In small groups or on their own, pupils should **list** different groups of people depending on what kind of information they share with them: for

instance, 1) mum & dad; 2) siblings; 3) friends; 4) other pupils; 5) teachers and other adults they know well; 6) unknown people on the street. (There might be also other categories, such as 'really best friends', 'neighbours', 'grandparents and other members of the family', 'favourite doll', etc.: children should figure out themselves which are the relevant groups for them);

- For each group, pupils should **enumerate** information that they would only share with that group. For instance: Are there things you would only tell your (best) friends? Do you talk about the same things with your parents and with other members of the family? Are there some kinds of information that you think your teacher should know, but probably not strangers on the street?
- The class should gather their answers together, and talk about **how we actually make sure** that we share what we want with only the people we want. For instance: we do not walk down the street in our pyjamas, we speak with some people about certain things only when nobody else is around, sometimes we speak softly, sometimes we ask people to promise to keep a secret, etc.
- The teacher should **explain** that privacy is about controlling who knows what about us, and that, just as we make an effort to control this in our everyday life, when people go online they should also remember to control what they share with whom.

FOR THE YOUNGEST

Youngest children should learn that, just like there are some people who could be tempted to steal their stuff, there are some people who would like to steal their data. They shall thus be careful with what they do with them, think about where they store them, and never give data about them to strangers.

FOR THE MOST ADVANCED

The most advanced pupils should learn to act responsibly with their data: have strong passwords, keep them private, and beware of phishing. They should also be aware of the 'privacy settings' of the services or applications they use.

8. FAMILY, PRIVACY AND PERSONAL DATA PROTECTION

Parents can be very useful to help children protect their privacy and personal data. Sometimes they could also, however, be a bit too invasive.

OBJECTIVES

- Learn about how their parents can help them in protecting their privacy and personal data.
- Think about whether parents can also infringe their privacy, and what to do about it.
- Suggest opening a discussion with their family.

KEY ISSUES

Parents can play a **crucial role** in the protection of privacy and personal data of their children. While children are unable to consent to some personal data practices, it is generally the parents (or a guardian) that will have the capacity to **refuse or consent** to those practices.

This does not mean, however, that parents should take these decisions without taking into account the children's wishes. On the contrary, parents should listen to their children, and help educate them so they can in the future **take the right decision** about what to do with their data. Parents should thus **help children defend their rights** and help them learn how to do so.

In practice, however, it can happen that parents are unfortunately playing an active role in **infringing** children's privacy and personal data protection rights:

- Parents certainly need to know about some of their children's activities to ensure their safety and education – it is their responsibility. Their **surveillance**, however, can sometimes go too far and unnecessarily invade too many spaces of their children's lives. In some cases, children are unaware of how they are being tracked, which is particularly problematic.
- Parents can also '**over-share**' information about their children with other people. For instance, some parents post pictures or videos of their children to social media without controlling who has access to them, or without realising that these images could be linked indefinitely to their child's name. These pictures and videos might look sweet to them, but could, in other contexts and later on, generate embarrassment, or even be misused.

When they feel uncomfortable about any of these issues, children shall be able to **talk about them** with their parents. They should at least be granted some zones of **privacy** and be made **aware** of how the data about them is used. As they grow, they should be granted more power in deciding what happens to their data, and certainly have a say on any pictures, videos, or any information about them posted online.

REAL LIFE CASE

Some users of the photo-sharing social networking service **Instagram** launched the trend **#BabyRP**, a sort of role playing where people play the roles of 'baby', 'mum' and 'dad' by using pictures of real babies and children that they take from other users, without asking permission. In some cases, the real parents discovered that strangers had been using their children's images only after these had been shared widely by their fake families, with fake names and in imaginary situations.

IDEAS FOR DISCUSSION

Pupils can be asked to discuss these questions:

1. ***Personal experiences***: Have you ever felt that your parents invaded your privacy? When? What did you do about it? Sometimes, parents interfere with their children's privacy without even realising it: for instance, during a dinner with other family members or friends, they could share an anecdote about their child that they think is very sweet or just funny, but that their child finds extremely embarrassing. Do you think your parents have the same ideas as you on what needs to be kept private?
2. ***Looking for rules:*** Do you think parents have the right to monitor their children's activities? Why should they need to do that? Should there be any limits to their surveillance? Should rules be different depending on the age of the child?

RECOMMENDED ACTIVITIES

1. ***Acceptable practices?*** This exercise can help pupils think about what their parents know about them and their activities. Pupils should:
   - **List** the ways in which parents could, in general, monitor their children's activities. Think for instance about checking their online behaviour,

keeping an eye on their phone communications, accessing their social media accounts, tracking how they spend their (electronic) money, etc.
- **Underline** the practices that, in their view, are not acceptable.
- **Compare** the answers with the other pupils' answers. If there any differences, explore why.

2. ***You teach them.*** Sometimes it can be difficult for parents to support their children in protecting their privacy and personal data protection because they know little about the devices and services that their own children use daily. This exercise aims to encourage the class to think about this problem, and to realise that maybe they have some very valuable knowledge that they could use to digitally empower the whole family. Pupils, on their own or in small groups, should:
   - **Imagine a lesson** about a device, social networking platform, application or any other digital service that they enjoy very much using and know very well, but that their parents do not use at all, or do not know that well. What should their parents know if they were to use it? Why is it so useful, or such fun to use it? Describe how it functions, and what are its advantages.
   - **Include in the lesson some privacy tips** for the parents, so they can protect their privacy and personal data when using it: Should they create an account using their real name, or preferably not? Are there any privacy settings they can change? Will a company be collecting data about them? Who will see the info they share?

FOR THE YOUNGEST

Youngest children should be clearly made aware that they their parents have a key role in helping them protect their privacy and personal data. If they ever feel their parents are invading their privacy, or not protecting their rights as they would like them to do, they should talk with them about this. The parents could have a good reason for doing what they do, or, in some cases, not have realised that they were interfering with their children's privacy.

FOR THE MOST ADVANCED

The most advanced pupils should know that their parents have a key role in helping them protect their privacy and personal data, but that they too have a crucial role to play, and that their views on these subjects do matter.

9. KEEPING SAFE, FEELING GOOD

Through the Internet we may come across things that hurt us, as well as people that are not particularly nice or considerate, or even individuals with bad intentions. Children should do their best to avoid predictable dangers, as well as any behaviour that could hurt others.

OBJECTIVES

– Consider possible risks online.
– Think about '**cyber bullying'** and online '**hate speech**'.
– Think about the possible dangers of **'sexting'.**
– Prevent risky behaviours.

KEY ISSUES

Online, just like in the offline world, **not everybody is your friend**. Through social networks, in online games, or just by commenting on things online, you could come across people that look very friendly, but this does not mean you should trust them. Children and teenagers must be aware that, just like they would not go and tell their personal life to strangers on the street, they should never give any confidential information to strangers online. This especially includes not giving anybody **phone numbers** or **addresses** that people could later use to bother them.

As a matter of fact, just like in the offline world, online even your friends can sometimes hurt you. We know indeed that people can sometimes behave in strange ways when they communicate online, perhaps because they think nobody sees them, or because they are not completely aware of the **implications** of their online behaviour.

Sometimes, people hurt other people on purpose. The term **'cyber bullying'** is the action of harming or harassing somebody through the Internet, in particular when done on purpose and repeatedly. There are actually many types of cyber bullying, ranging from spreading false rumours through social media to continually annoying somebody by pestering them.

All these behaviours can have **dramatic consequences** on the victim. It is thus crucial that minors do not engage in any activity (like posting, commenting or sharing) that could be experienced as 'cyber bullying' by anybody, and that they are ready to support their peers if any of this happens to them. If they go through the situation themselves, they should be able to talk to their parents (or guardian), or a responsible adult, to make the situation **stop** as soon as possible.

A particularly disgraceful way of hurting others online happens when people attack a person or the group they belong to because of their gender, their ethnic origin, their religion, disability, sexual orientation… or any other 'difference' that they wrongly perceive as giving them a reason to be degrading. This is sometimes called '**hate speech**' and is not only distressing for the person attacked, but also for the whole group of people concerned. Minors should be aware acting like this is wrong, and that the law foresees sanctions for those who do it, so they should actually report 'hate speech' whenever they encounter it.

Finally, pupils should consider the possible dangers linked to **'sexting'**, that is, the practice of sending and receiving of sexually explicit photos, messages or videos – be it by text messages, emails or through social networking sites. Teenagers who might be tempted to send or receive this kind of images often do not have a clear perception of the many ways in which the photos, messages or videos might end up in the wrong hands: they should thus be reminded of the fact that whoever gets access to such a piece of information might share it further or even make it publicly available to everybody, just **by being negligent**, **by mistake**, **as a (bad) joke** or **even on purpose** to upset them. In addition, teenagers often do not imagine the possible **major negative implications** of these scenarios, which could leave them vulnerable to much embarrassment, or even to blackmail.

IDEAS FOR DISCUSSION

1. ***Personal experiences about cyber bulling (and how to stop it).*** Pupils should address these questions: Have you ever come across anything that appeared to be 'cyber bullying'? What did you do? Some experts say that in those situations people should try to show the victim of cyber bullying that they support them, and that they are not intimidated by the bullies. Is that easy to do? What else can be done?
2. ***The most private things.*** Pupils should engage in a discussion about the dangers linked to **'sexting'** by considering, for instance, an imaginary scenario like this one:
   - **Scenario**: An imaginary girl, called G, and an imaginary boy, called B, both teenagers, decide to celebrate their anniversary by exchanging sexually explicit images of themselves, because they have read it could be

fun. They promise each other they will not share them with anybody. The day after, the boy goes to the swimming pool and accidentally forgets his phone in the changing room, outside the locker. While he is swimming, another boy sees the phone, check its content, finds the picture of the girl, and decides to share it through a very popular social network, using B's account – that is, to all his online 'friends'. He then leaves the phone where it was, and goes away. In the meantime, G, who was just about to write on her blog about her latest holidays, suddenly sees the picture pop up through the social network, apparently sent by her boyfriend's profile. Almost immediately, she starts receiving mocking and degrading comments from people, including people who were not B's online 'friends'. Very angry and extremely disillusioned, she decides to take revenge by posting on her blog, that is, open to everybody, B's picture, and sends an email to B's father (whose email address she finds online), to make sure he is aware of it.

- **Discuss:** What could happen next? Is there anything G and B could have done to avoid this situation? What exactly? Do you think this scenario could actually happen in real life? If not, what kind of problematic scenarios can you imagine?

RECOMMENDED ACTIVITIES

1. ***Think before you share***. There are many reasons why some unsuitable information might be posted online by children or teenagers without sufficient prior thinking about the consequences. For instance, children may think it is just funny to share publicly a picture where their friends look ridiculous or weird, without realising that the picture could be shared again and again and become widely exposed, which their friends will not find funny at all. Or, in a moment of anger, minors could feel like writing online something particularly nasty about somebody, without realising that this may not only upset the attacked person, but actually also poison their daily life for a long time. This exercise invites people to **reflect** upon those cases. Pupils should:
   - **Describe** situations where they could imagine that somebody would share or post online information that would later become a problem, and what kind of problematic content could find its way online: for instance, teenagers at a party could share pictures of behaviours that should only be known to those who were there, friends who have an argument might tell secrets they were not supposed to tell, etc.
   - **Discuss** what could be done to prevent problems: Are there any types of data that one should never share? Would always asking for other people's permission before using data about them be a good idea?

FOR THE YOUNGEST

Youngest children should know that through the Internet they could run into all sorts of people. Even when these strangers or new 'friends' look friendly, one cannot be completely sure they deserve trust. Children should never give to strangers or online 'friends' any personal data such as their telephone number or postal address, or any pictures.

FOR THE MOST ADVANCED

Most advanced pupils should adopt a reflective attitude towards their online behaviour. They should remember to always ask themselves if the information they share or post could have a negative impact on somebody (including themselves, but not only!), for instance if it was to be used in a different way than initially foreseen.

10. TAKING ACTION

Having the right to personal data protection means that you have some rights that you can use, so you should not be afraid to use them – directly or with the help of an adult. In case of doubt, contact your data protection authority for guidance. And, in case of an urgent problem, you should know whom to contact too.

OBJECTIVES

- Master **personal data protection rights**.
- Know **what to do** when an organisation does not respect your rights.
- Be aware of the existence of a **data protection authority.**
- Know **whom to contact** when you face a difficult, urgent situation.

KEY ISSUES

Anybody whose personal data are being used by an organisation or a company has the right to ask them **which data** they have, to make them **rectify** the data if inaccurate, and to have them **delete** the data if there is no need for them to have the data anymore. If you **consented** to a company getting your personal data but later change your mind, you can inform them and they should also take immediately the necessary steps to **delete** the data. These are everybody's basic **personal data protection rights**, which everybody should be able to use directly by addressing the company that has data about them.

If a company sends you commercial messages, or keeps calling you, and you are not interested in what they want to tell you, you can **tell them to stop**. Often this is done by 'unsubscribing' to their mailing list. All commercial messages should state clearly who the sender is and how to unsubscribe so they stop sending information.

Young children are not supposed to exercise their personal data protection rights on their own, but they can **ask their parents (or the holder of parental responsibility) or a responsible adult** to help them to effectively protect their data.

If the company or organisation processing the data does not react appropriately, or does not respect people's choices, it is possible to contact a **data protection authority.** This is an agency whose function is to make sure that personal data are always processed following the existing rules, and that whoever uses people's personal data respects people's rights.

The **data protection authority** can offer guidance and, when appropriate, investigate a complaint. They might also get in touch with the company or organisation, and perhaps solve the problem.

Some situations, however, need much **urgent action**, and cannot be tackled by data protection authorities. Minors sometimes discover that somebody has shared online information about them that can cause much distress, and that must be removed immediately. Sometimes this happens by mistake, and sometimes it happens because of ill-intentioned people, who will not cooperate in taking down the information.

In all these cases, children and teenagers can try to get the information removed as quickly as possible by contacting the website or the service provider, like a social networking platform. As this can sometimes be difficult, they should not be afraid to talk about it with **their parents or guardian, or a responsible adult**, who should be able to assist them.

If they prefer, minors can also directly contact an **Insafe helpline**. These are helplines specialised in giving a hand to children and teenagers when they go through difficult online experiences or encounter inappropriate content, and are generally accessible for free and anonymously. They can also be of help in **online harassment** cases. In case of serious problems, minors should not hesitate to contact **the police**.

RECOMMENDED ACTIVITIES

1. ***Using your rights for real:*** This exercise requires some time (a delay of at least some weeks needs to be foreseen to wait for replies), but it can be particularly useful for pupils to actually experience what it means to have a right to personal data protection. Each pupil shall:
   - **Choose** a company or organisation that they think could have personal data about them.
   - **Write down** why they have picked up that particular company or organisation, and which data they think they have about them.
   - **Make use of their right of access** by contacting the company or organisation, and asking them to tell them which data about them they have.
   - **Wait** for an answer for at least a few weeks.

- **Explain** to the class which entity they contacted, why, which data they thought they had, whether they received an answer, and what did they find surprising about it, if anything.
- **Compare** their own experiences with that of the other pupils. In light of all the results, consider these questions: Can it be useful to exercise the right of access to your personal data? Why? Is it easy to get a reply? Could the data protection authority be of any help?

FOR THE YOUNGEST

Younger children should know that they can **exercise their control on data about them** with the **help** of their parents or a responsible adult, and that there exists a **data protection authority** that has the mission to ensure that everybody complies with personal data protection rules. They should also know that if they ever find online something that disturbs them, it is better to call for help.

FOR THE MOST ADVANCED

Most advanced pupils should know which are their **personal data protection rights**, and feel comfortable with the idea of **exercising them**. They should understand that they have the right to speak up if they think that somebody is misusing data about them, and know there is a **data protection authority** that can give them more information or guidance. Additionally, they should know that if they are in trouble due to something that is online, adults can help them.

THE MINI-BILL OF PRIVACY AND DATA PROTECTION RIGHTS

This 'bill of rights' lists the basic rights all children and youngsters enjoy under EU law.

You have a right to privacy. We all have a right to privacy since we were born. 'All' includes babies, children and teenagers. Grown-ups have a right to privacy too.

You have a right to the protection of your personal data. Nobody can process other people's data without respecting some rules, like processing as little data as possible, and always keeping them secure. By processing data, companies and organisations can gain important benefits, but they also get more and more power. The rules help us to protect our data and ourselves, and to keep them in check.

All your personal data deserves protection. It does not matter if the data are already public, maybe because one day you accepted to share them. It does not matter if the data were never 'top secret', or do not look particularly intimate. Whenever somebody processes data about you, they have to comply with the rules. Even boring, ordinary data could cause trouble.

You have the right to know who has data about you, what they use them for, and how they do it. You are entitled to have some control on what happens to your data, and this is only possible if you are informed of who is using the data, why, and how. So those who wish to process your data have the obligation to tell you about all this.

You have the right to receive clear information. You should always be able to understand what they are telling you. They are obliged to be transparent, so don't let them be obscure. If something is not clear, dare to ask!

You have the right to know exactly what data they have. Let's imagine they explained what they wanted your data for, and how they will use it. Or maybe they forgot. Or maybe it was really, really obscure. In any case, you can ask them what they know about you, and they are obliged to tell you.

You have the right to correct any inaccurate data about you. It could sometimes be a big problem if people have wrong information about you. It could lead them to the wrong conclusions, and they could take wrong decisions about you. If you notice they have the wrong data, you can ask them to correct them, and they are obliged to do it.

You have the right to be heard. Sometimes, organisations or companies are obliged to process some data about you. But often they have no good reason why, so they will just ask if you let them use the data nevertheless. Adults and more aged teenagers have the right to consent to this kind of practices. If you are a younger child or teenager, it is probably not you but your parents who can consent, or not consent. However, before they do anything, they should consult you and see what you think.

You have the right to complain. If somebody is not respecting the rules, let them know you are aware of your rights. If they do not get it, ask somebody to help you, and insist! Data protection authorities have been set up in each country to help people with all issues related to the protection of their personal data, they can also provide guidance and assistance.

Now you know your basic rights, make sure you…

… use them! You will become a master of your privacy and data protection rights only if you exercise them. People are collecting data about us every day, so make it a habit: think about who collects what and why they do so, how they use the data, and for what purpose.

… use them wisely! These rights are given to us so we use them to make sure our data are protected, not to compensate reckless behaviour. The best way not to lose track of your personal data is to make smart decisions before sharing any.

… and always remember that other people have exactly the same rights too. Make sure you respect everybody, for instance by not sharing pictures showing other people, or information about them, without asking them first. Be kind and polite, also online.

SELECTED LESSON PLANS

The teacher's manual was conceived as an invitation for teachers to design their own lesson plans, adapted to the needs of their pupils. During the ARCADES project, the data protection authorities of Poland, Slovenia and Hungary called for teachers to submit examples of plans that could be shared more widely, and be potentially useful for their peers even across borders. Each national authority selected the best lesson plan among all submissions in the national competitions, and they are made available here, introduced by their authors.

These awarded plans illustrate different possible approaches to teaching privacy and data protection. Lesson Plan 1, *The Little Elves*, offers a scenario for younger children to integrate in a playful manner the basic principle according to which one needs to think before sharing data over the Internet. Lesson Plan 2, *Who Wants Your Personal Data?*, is directed towards an older audience and aims to provide pupils a wider picture of personal data processing practices. Finally, Lesson 3, *Online Dangers*, focuses on awareness of risks that might be encountered online.

LESSON PLAN 1: THE LITTLE ELVES

Nina Jelen

1.1. THE BEST SCHOOL YEAR EVER!

This year was really successful for our school, the primary school Podkum, OŠ Ivana Skvarče Zagorje. We pulled off loads of projects, learned a lot and had fun at the same time. And just when we decided to calm down, rest a little bit and focus only on the school curriculum, the award by the Information Commissioner surprised us! And that made our school year one of the best school years ever. After the announcement that we won, our school was flooded with elves from the poem of the winning lesson, elves songs and dancing. Our classrooms were full of laughter and happiness.

And not just that… Our little, country branch school became one of the famous schools in Slovenia. They gave us names like 'the best school' and 'the most successful one', they wrote beautiful articles about us, we were on TV news and radio. We became famous as our elves from the story… but in a good way.

The truth is that I did not imagine we would be the ones winning this contest. The project was designed for older children as well and they have such knowledge and ideas about the web, and they are using it every day. I thought we were too young and too inexperienced. So it was quite a shock when we got the call from the Information Commissioner's office and received the good news. But if you really think about it…

I agree 100% that we have to start teaching children about the web already when they are young. They are so naive and unaware of how wide the web is. They do not realize that you can meet good and also bad people on it… as in real life. Before we discussed it, they were ready to share all their personal information on the web. It is impossible to cut children from using the Internet, and we should not do so. As we are preparing them for real life, we should also prepare them for life online.

I am really happy that I planned and carried out this lesson, even if we would not have won. I think that my children learned a lot from it. And if next year or the following they also hear from their parents something about using the web, acting on it, or how to behave if you are a web user, then I think and I hope that they will remember about our web rules, as they become real web users.

I am truly grateful for everything that happened to us. For everything the Information Commissioner's office did for us. Because of this award, we experienced so many things. I think that was a once in a lifetime thing and something that will never happen again to most of my children and me. We had a chance to play on the big stage in Ljubljana, we got books, computers, and we even travelled to Barcelona, which was incredible! We were on the news, on the radio, all over newspapers, so we saw how news are made at the studio, how a newspaper article is written… I have no words to describe what all of this means for a little branch school. Not only to ours, but to every little school in Slovenia.

Our little school became BIG! because we proved that even if we are small and outnumbered, we have everything and more than the big ones have! Thank you for everything!

1.2. THE LESSON PLAN

1.2.1. Description

Topic	Privacy and data protection on the Internet
Duration	45 min
Grade	2nd grade, primary school (Slovenian system)
Age	7 – 8 years old
Goals	– to understand the importance of data protection. – to learn how to recognise 'personal data' and why we need to protect them. – to learn about 'sensitive personal data' which need special protection. – to raise awareness about the rights we have in relation to the protection of our data. – to learn about dangers on the Internet.
Forms of teaching	Individual, group, frontal.
Methods of teaching	Discussion, explanation, demonstration, dramatisation, method of reading and textual exercises.
Teaching aids	– the poem (author: Nina Jelen) – props for dramatisation: elves' hats, camera, toys, an apron, a pot, a screwdriver, a dance dress… – hand-out: registration form for the *Cool kids* website

1.2.2. Lesson Development

STARTING MOTIVATION	
Teacher	**Pupils**
The teacher expressively reads the poem about *Elves behind the hills* (see below) and shows illustrations. The story is then repeated with the pupils. Who were the elves? What were they like? Were they good or bad? Why did others like to visit them? (Read the part of the poem that describes why, after the unfortunate events, did the others like to visit the elves) Did they have any funny habits? What were they? What did Fotko do? Was it right that he published the video? How did the elves feel then? Why did other creatures like to visit them after that) (read the part that describes why the creatures like to visit the elves after the unfortunate event) The teacher stresses that whatever is posted on the Internet could stay there forever. How did the story end?	The pupils actively participate in the discussion and repeat and recap the story.
MAIN PART OF THE LESSON	
The pupils are shown the picture of the new social networking site *Cool kids*, a mock up site targeting younger kids like them. It offers games, chat with other kids, and many more activities.	The pupils are invited to share their thoughts about the website. Would they like to sign up?
Without further explanation the pupils are given hand-outs: a registration form for the new website *Cool_kids.com*. The form requires many personal data to be entered.	
The instructions to the pupils are: fill in the form with the data that you think are appropriate and can be made public on the Internet without worry.	The pupils fill in the hand-outs, that is, the registration form for *Cool kids* website.

After the forms are filled in, the teacher and pupils slowly discuss every category of personal data the pupils were willing to share on the Internet.	
The teacher explains that it is not appropriate to disclose on the Internet the name, surname, and address, date of birth, phone number, e-mail or passwords, data about parents or places where they are. The same goes for photos about themselves or their friends.	The pupils follow the discussion and add an exclamation mark in the form where the data they had entered should actually not be posted on the Internet.
The teacher explains that we have special rights regarding our personal data and that we have to protect them. The teacher explains how personal data can be exploited by shops and companies.	
The importance of security is highlighted. Like in real life, also on the Internet some people may have bad intentions. That is why pupils should never trust people they do not know. On the Internet someone may easily pretend to be someone else, as was seen in the story about the elves.	The pupils share their experiences.
The teacher explains that the pupils must take care of their online identity. In real life they try to be good and hardworking and they should do the same regarding their identity on the Internet. Did others see that the elves were in fact hardworking and good after the embarrassing photos were posted on the Internet?	
The teacher explains that the pupils must at the same time also take care of the data about their friends and the people they know. That is why Fotko (The Cameraman) did not do the right thing when posting pictures without asking for permission first.	
The pupils are presented with the class poster: *Golden rules of cool kids on the Internet.* They hang the poster in their classroom.	
END OF THE LESSON	
The pupils dramatise the story/poem about elves behind the hills. They play it expressively.	

1.2.3. Specific Materials to be Used

1.2.3.1. The poem

Elves behind the hills
(or how the little elves embarrassed themselves)

Over the hills in a village far, far away,
Little elves lived happily every day.
Their souls were pure and clean,
They were never ever mean.

They helped each other, they were good.
They were always in a joyful mood.

From far, far away people came to see
How good and cheerful elves can be.

Pepe had good hand skills,
He knew how to fix a car and how to make drills.

Pepe*: Oh, what a nice oily machine. It will surely take me three days and nights to fix this. I think that Vrtavka (The Spinner) is going to be very happy when she sees that I fixed her car. I can't wait to surprise her!*

He was good with the hammer and the axe,
But his ears were always full of earwax.

Pepe: *Hmm…should I drill this screw too?*

So… When he was thinking about car gears,
He was also drilling with fingers in his ears.

Vrtavka: *Pepe, are you fixing my car? Oh, you are my hero! Thank you!*

Smrdec (The Smelly One) had the biggest heart,
He was helpful, kind and smart.
Smrdec: *Good morning, Ms. Špegi. Look at your beautiful tree. Can I water it? You have so much work to do. My little cute tree…*
But sometimes he just felt it in his heart
To release a good and smelly fart.

Spak (The Funny One) brought tears of laughter to his homefolks,
He could tell such funny stories and jokes.

Spak: *A hedgehog bumps into a cactus. And what does he say? 'Oh, mommy!'.*
It often happened so that some elf
Fell really clumsily off a shelf
And of laughing so much this elf
Peed unfortunately on himself.

Vrtavka (The Spinner) liked to dance and spin,
She did loads of practice at the gym.
She was the elves' dancing queen,
Being all gracious, strong and lean.
Vrtavka: *Hmm… how was that in the show? You step on your fingers, you raise yourself high in the sky, then you raise your hand and your leg… oops…*
Unfortunately she often fell on her head or chin,
Sometimes she ended up on the floor, or even in a bin.

Špegi liked to cook pasta for every child around,
Out of her house you could only hear one sound:
Nom, nom, nom, …
Špegi: *Come here my little children. Špegi has pasta for you. With meatballs, cheese, warm or cold… Come here!*
She had pasta everywhere,
On the floor, in her pocket and in her hair.

Without his camera, Fotko never left the house.
He took pictures and made movies of people, trees and the little mouse.
Fotko: *My camera is the best in the whole world! The most modern, the coolest! I'm going to put these movies on the web! Everyone will want to see them! Maybe I'll become a famous star Fotko Kuštroglavec!*
I'll put this on the web now!

And step by step…
He put everything – EVERYTHING on the web!
Of course… in a minute… it all spread…
To the next village, town and all around the world, it was said!

And EVERYONE saw:
How Spak's laughing too hard,
How Smrdec releases a very loud fart,
How Špegi is rolling pasta in the backyard.
How Vrtavka just fell clumsily down,
How Pepe pulls out of his ears something brown.

The video was instantly a huge success,
For Fotko that was a real breakthrough bless,

But the little elves felt nothing but sadness and shame,
They did not enjoy at all this attention and fame.

From far, far away people came to see,
How embarrassed and weird elves can be!

O, Smrdec, what a disgusting fart!
Špegi, look. You have spaghetti in your nose.
And you Vrtavka, you better stop dancing. You are clumsy! You'll never be a real dancer!
Pepe, wouldn't you wash your ears? You are sooooo nasty!
And you Spak… your belly is like jelly candy when you're laughing.

Poor elves just wanted to run away,
To sit silently and hide in the hay,
And think sadly about the day,
When everything was not so grey.

Their tears never dried,
So restlessly they cried.

Even Fotko wanted to quietly disappear,
When he realised what he did to his elves dear.
Fotko: *Dear elves, where are you? What has happened to our village? Where are laughter and happiness?*

But the damage was done,
There were no happiness, no joy and no sun.

Elves needed years and years to recover,
That they were the weirdest elves on every magazine cover.

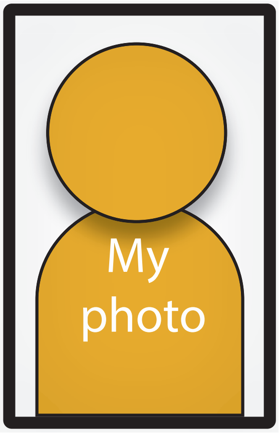
And although Fotko made a new movie,
Where he showed elves nice, helpful and groovy:

How Pepe is working hard,
How Spak made old men laugh in his yard,
How Špegi's hanging out with kids and making great food,
How Smrdec is taking care of the neighbour's foot.
How Vrtavka just made a successful kick and flick and trick.

And although again…
From far, far away people came to see,
How good and nice elves can be,
Elves' smiles were never again so wide,
From that day a little piece of their hearts – stayed tied.

1.2.3.2. Mock-Up Registration Form

www.cool_kids.com



Nickname*: ______________________

Name and surname*: ______________________

Date of birth*: ______________________

Address: ______________________

Phone number*: ______________________

Credit card number: ______________________

Email address*: ______________________

Password for email account: ______________________

My school*: ______________________

Extracurricular activities: ______________________

Places where I love to go: ______________________

Hobbies and interests: ______________________

My parents' job: ______________________

* **must be filled**

1.2.3.3. Golden Rules For Young Web Users

1. Don't give away your personal information like your **name** and **surname**, **date of birth**, **phone number**, **e-mail** and **password**.
2. Don't give away information about your **family**, **friends** or **school**.
3. Be polite, always.
4. Do not post strange or unsuitable **images** or **videos**.
5. Remember, what is on the web is **very difficult to take down**!
6. If something on the web makes you uncomfortable, **tell your parents**.
7. Do **not talk with strangers**, never send them any pictures and do not try to meet them in real life.

LESSON PLAN 2: WHO WANTS YOUR PERSONAL DATA?

Małgorzata Szyszko and Katarzyna Wiączek

2.1. INTRODUCTION

There has been a dynamic development of modern information and communication technologies in recent years. The Internet offers a range of services used by very keen young people who, often recklessly, share a lot of information about them. In the virtual world this allows for easy data acquisition and identification of these young people. In fact, this may become a threat to the security of their personal data and privacy.

We teachers notice these phenomena and are convinced that there is a need for measures to protect the students' community. This is a big challenge, because issues related to personal data protection and privacy create also a new area for us – teachers. It is thus great that various institutions, i.e. GIODO or the Panoptykon Foundation, carry out information and education sessions and that we can count on their support and cooperation.

On the basis of materials provided by these institutions, using our own experience in pedagogical work, knowledge of different methods and forms of work with students, and using interesting teaching aids, we undertake to educate young people on the issues of personal data protection and privacy. It is possible to offer to young people studying in junior high school meetings with specialists, appeals, or contests. However, it seems that the best way to convey difficult content related to personal data protection are lessons conducted in well-known groups, teams or entire classes.

Taking this into account, we, teachers working at the Marshal Józef Piłsudski Middle School No. 119 in Warsaw (*Gimnazjum nr 119 im. Marszałka Józefa Piłsudskiego w Warszawie*), decided to prepare a scenario for junior high school students that can be performed at several types of lessons, and where content might be revised during lessons. We assume that students have already a basic knowledge of personal data protection and privacy, that they have gained in previous years of study.

Students can actively participate in the implementation of the subject. The plan foresees work in groups with the use of materials prepared in advance by the teacher, and the presentation of group work results. Tasks for the groups have a direct relationship with the content covered by the opening presentation, and the discussion that certainly will take place in the class.

In our school we have conducted this scenario at several types of lessons: computer science with 1st grade students and educational lesson with 2nd grade students (the version with supporting teacher) and English lesson with advanced group of 3rd grade students. This diversity follows the assumption that different age students have different levels of knowledge about personal data protection and privacy, and therefore we use different degrees of difficulty.

The scenario allows teachers to achieve the marked objective, but we need to prepare for that class very carefully and adjust the quantity of content to the level of each group. The resulting lesson certainly arouses great interest among students, as evidenced by their activity while working in groups, participation in discussions and taking extra homework.

2.2. THE LESSON PLAN

2.2.1. Description

Addressees of classes: students of 1st, 2nd and 3rd grade of middle school (Polish system).

Type of classes: classes with the class teacher: computer science, English.

General goal: The classes will help youngsters understand why personal data protection is so important nowadays. Pupils will learn as well who is interested in obtaining their data and what principles such people observe.

Specific goals: Pupils shall:

- learn why institutions, organisations and companies collect, store and use our personal data;
- get to know the obligations of the entities using our data;
- learn that one's data shall be disclosed consciously, and that one has to check the information on the privacy policy implemented by the data controller.

Working methods:

- Teacher's instructions, together with distribution of hand-outs to pupils, and group work;
- displaying a multimedia presentation prepared by the teacher;

- talk, discussion;
- using IT tools.

Forms of work:

- Drawing pupils attention to the information provided to them by the teacher;
- group work with the use of instructions and materials prepared by the teacher and computer with Internet access;
- watching a multimedia presentation;
- talk, discussion on key issues and examples related to the lesson's subject.

Teaching aids and materials:

- Room equipment – tables arranged for group work;
- files containing tasks for particular groups in printed form;
- computer with Internet access, projector;
- A4 sheets of paper, crayons, felt-tip pens;
- magnetic board (optionally, pin board or big cardboard).

Key words: personal data, data collection, being a data controller, processing, security.

2.2.2. Lesson Development

2.2.2.1. Introduction (basic knowledge)

Nowadays, a very rapid development of information and communications technologies is taking place, and we benefit greatly from it. Large amounts of data are produced, which are obtained by various entities, collected off-line or on-line. The volume and pace of this phenomenon generate problems referred to the adequate protection of disclosed personal data.

The uncontrolled use of personal data by institutions and companies may cause problems for many of the people to whom the data relate, in particular minors. This often results from unawareness or lack of knowledge on how to act, so as to ensure oneself security and privacy protection. Using the knowledge, experience and information resources of institutions such as data protection authorities or relevant NGOs teachers can – by conducting interesting lessons, using activating methods – make children and youth aware of why the protection of personal data and privacy are so important these days.

While preparing a lesson on the subject *Who wants your personal data?*, we assume that students already have basic knowledge on personal data protection and privacy. Repeating such information will, however, constitute a good prelude to the introduction of new contents.

2.2.2.2. Teacher's activities before the lesson

In order to conduct this class, teachers should carefully prepare: tasks for pupils in particular groups, the equipment enabling the execution of these tasks, a presentation on the subject *Who wants your personal data?*, and proposed homework.

Immediately before the lesson a classroom shall be prepared – 3 tables for group work and other objects necessary for the pupils to execute the tasks.

2.2.2.3. Subsequent stages of the lesson

1. Beginning of the lesson – welcome, information on the form of work, dividing pupils into groups, assigning the tasks – 5 minutes;
2. Pupils carry out their tasks – 10 minutes;
3. Pupils present their tasks and the results of their joint work – 5 minutes;
4. Presentation plus talk and discussion under direction of the guiding teacher on the topic *Who wants our data?* – 20 minutes;
5. Summary of the class, discussing homework – 5 minutes.

2.2.2.4. Detailed description of subsequent stages of the lesson

1. Beginning of the lesson

Pupils are invited to the classroom and informed that they will work in groups. They are asked to join one of the following three groups:

- Pupils who like preparing newsletters, jigsaws are invited to join group 1. The group members receive a magnetic board, on which they post segregated inscriptions meaning personal data, examples of data and entities to which we give our data online.
- Pupils good at searching for information online and quick recording form group 2, which is provided with a computer with Internet access and a projector.
- Pupils who like drawing and artistic skills form group 3. Students are given sheets of paper, crayons and felt-tip pens needed to make drawings, which can be examples of avatars.

2. Children carry out their tasks. They have circa 10 minutes for this. The teacher supervises the pupil's work, checks whether they have understood

their tasks, monitors progress and draws their attention to the time destined for execution of tasks. If necessary, they discipline the pupils.

3. After having performed the tasks, group leaders present the tasks and the results of joint work of each group.

4. After ending the stage of group work, pupils are asked to gather near the screen, on which a presentation will be displayed.

   We give the subject of the class: *Who wants your personal data?* The presentation is combined with a talk and discussion. It is done in such a way that pupils are given the possibility to speak before replies to questions asked or keywords appear. We refer to and emphasise the importance of tasks performed by the pupils when these contents pop up in the presentation.

   Particular attention should be drawn to the pieces of information in the presentation directly referring to specific goals, which we want to achieve by means of prepared class materials and methods, i.e.:

   - Pupils have to be given a reply to the question of why institutions, organisations, companies collect, store and use our personal data;
   - need to be explained the obligations of those using our data; and
   - pupils should be taught that one's data have to be disclosed consciously and that one has to check the information on the security policy implemented by the data controller.

5. Ending of the lesson – we summarise the lesson, emphasizing that personal data protection is very important nowadays. We ask a few questions to make sure that students have learnt something new and strengthened their previous knowledge.

   We give and shortly discuss homework. We organise jointly tidying up the classroom. We thank the pupils for participation in the class.

Homework:

- Homework (lesson with the class teacher): Pupils have to talk with their parents about the issues discussed during the class, i.e. *Who wants your personal data?*
- Homework (IT):
  - Pupils have to talk with their parents about the issues discussed during the class, i.e. *Who wants your personal data?*

  - Create an avatar from a picture according to the instructions given by the teacher – additional homework for volunteers.
- Homework (English): write down new words and make sentences using them.

Evaluation: We check pupils' knowledge at the final stage of the lesson, but also during the lesson. The presentation, which constitutes the basis for a talk and a discussion, is displayed in a way which gives students the possibility to speak before a reply to the asked question or a keyword appears. We observe pupils reactions. At the end of the lesson, we ask them which pieces of information have been new for them, and ask a few questions to check what they remember.

Other remarks: The developed scenario is quite universal and can be realised during different classes, which allows involving different teachers. Might be introduced an element of secrecy by not giving the lesson subject at the beginning of the class, but only after realising the tasks in groups. For the work in groups to run smoothly, pupils' tasks need to be carefully prepared and the pupils need to be provided with all necessary materials. In the group arranging the inscriptions, a mobile magnetic board is the best solution. However, if we do not have such a board, we can use a pin board or even a big cardboard on which we stick sheets of paper with information. A lesson on data protection and privacy is not just one of many, but rather on the contrary – one of few lessons which we can realise by enriching the core curriculum, and hence, it is worth preparing such a lesson in a very responsible, careful and interesting way.

LESSON PLAN 3: ONLINE DANGERS

Eszter Keszy-Harmath

3.1. THE FUTURE HAS BEGUN…

In recent years, us, educators, have felt very strongly that our art of teaching requires not only the usual renewal, but a renewal that must rely heavily on technology. Today's students, the 'Z' generation, were born into the world of information technology. They are willing to learn and to pay attention only when they can use these tools for picking up new information. Unfortunately, the young people of today are living in such a world even outside the classroom, and a large part of their free time is spent with such media. They have no idea that besides the advantages of technology, many dangers are hidden in that world. We, the less young, might face difficulties when meeting new applications. But then we realize that even though all kids are using new communication platforms (be it Facebook, Twitter, or Skype, for instance) they do not realize the risks they may face. There is need for action, and teachers might not know how or where to start. The ARCADES teachers' seminar held by the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) was of great help to find the right way to do that. We received much useful information and guidance to show students how they can become conscious Internet users.

After the lecture, I talked with my pupils at the *Karácsony Sándor Általános Iskola*, in Budapest, and we put a lesson plan together, which gave them tasks and helped them to realize online dangers, pitfalls and solutions. Staff of NAIH followed the lesson and it was eventually announced to us that, as winners of the national competition, we would represent Hungarian schools in the ARCADES Final Conference.

Attending the Final Conference allowed us to meet the other top teams, discover new ideas, and hear about the lesson plans developed in Poland and Slovenia. We learned how this wide and colourful topic can also be addressed in other ways, focusing on different age groups. We learned from them and from NAIH representatives a lot of new, interesting and useful things regarding personal data protection. We thank them for their kindness. And thanks to all those who have worked to make us more familiar with this urgent problem and possible solutions, helping us to teach our pupils caution and vigilance.

3.2. THE LESSON PLAN

3.2.1. *Description*

This lesson plan was developed for the subject area of Media Studies, for a small class of the Hungarian 8th grade. Its main theme are online dangers, including sexting and cyberbullying. The provided scenario covers only a segment of the privacy knowledge that should be delivered to pupils. At least seven similar lessons could be foreseen to address all online dangers, as well as different aspects of data protection.

Objectives and tasks of the lesson				
Developing memory skills	Improving visual perception, attention and concentration skills	Deepening of learned knowledge	Vocabulary expansion	Developing interoperability
Developing oral skills	Developing thinking skills	Developing monitoring skills	Developing communication skills	Developing cooperation skills

3.2.2. *Lesson Development*

Time frame	**Occupational unit**	**Description of activity**	**Methods**	**Class work forms**	**Supporting aids**
3 minutes	Preparation, warming-up	Solving a crossword puzzle (definitional skills and knowledge survey). Definitions to be solved: icon, nick, television, electronic signature, router, netiquette, e-mail, troll. The solution is: INTERNET	Developing memory skills, activating previous knowledge	In pairs	Handbook
2 minutes	Correction	Discussion	Explanation	Frontal work	Independent correction
2 minutes	Discussion	The motto of the 21th century might be *Let's be just healthy and let's have enough Internet signal strength!* – What is the meaning of the motto? – Do you agree with it?	Explanation	Frontal work	Interactive table: projection
3 minutes	Graphic	The centre element of the graphic: INTERNET Task: fill the blank spaces with words connected to INTERNET	Creating a mind map, explanation, free association	Frontal work	Table

Time frame	Occupational unit	Description of activity	Methods	Class work forms	Supporting aids
3 minutes	Poster	Interpretation of the illustration *Confessional* by Pawel Kuczynski	Image interpretation, discussion	Frontal work	Image
3 minutes	Audio- visual effect	Screening of the video *Wo ist Klaus?* (available in several languages at: www.klicksafe.de/ueber-klicksafe/downloads/klicksafe-werbespots/download-wo-ist-klaus/) Analysing the video about online dangers	Discussion	Frontal work	Video
5 minutes	Conversation	Task: describe the meaning of the following words: grooming, troll, flaming, meme, sexting, cyberbullying	Guidance Promote self-expression Wake up own ideas Encouragement	Frontal work	Table
7 minutes	Scene	Task: pull a card and perform the given scene	2 situational performances under the teacher's direction in connection with cyberbullying and identity theft	Group work	Cards
2 minutes	Telling an unfinished story	ARCADES recommended activity *The most private things*	The teacher reads the story to the class	Frontal work	Interactive table, handbook
10 minutes	Discussion	Questions: – What could have happened? – How could the boy and girl have prevented the situation? – Could this story happen in real life as well? – If not, what other stories can you imagine?	Discussion, explanation	Frontal work, single work	
5 minutes	Discussion with the aim of raising awareness while using the Internet and thinking about risks before taking a decision	Questions: What would you do in a risky or dangerous situation? Where to seek help? – parents, – adults, – DPA, – ombudsman, – Internet hotline, – Internet helpline	Teacher's statement, explanation, evaluation	Frontal work	Interactive table, handbook

GLOSSARY

Behavioural advertising: ads that are displayed because, on the basis of the data previously collected about the user, they seem to have higher chances of having an impact on them.

Consent: the freely given, specific, informed and unambiguous expression of acceptance of some uses of personal data, given by the person associated with the data.

Cyber bullying: harming, tormenting, harassing or threatening somebody using technology, in particular if done on purpose and repeatedly.

Data controllers: the entities responsible for the processing of personal data.

Data subject: the person that can be associated with some personal data, and has a number of rights over such data.

Digital identity: the image of a person as it can be built with online information about them.

Identity theft: impersonating somebody, in particular by gaining enough information about a person to be able to pretend to be such an individual.

Personal data: any data that can be connected to a person, as long as we know who the person is. The data can take any shape: it can be written information, an image, a sound, a fingerprint, etc.

Phishing: the attempt to obtain information such as usernames, passwords, or credit card details by masquerading as a trustworthy entity in an electronic communication, typically by email.

Profiling: process where information about a person is gathered and analysed. Based on this information individuals are assigned categories/profiles that are composed of people with similar characteristics, preferences, activities. Additional information about people may be assumed or implied based on the collected data.

Right to privacy: traditionally described as ‘the right to be let alone’, this fundamental right is actually a broad notion that protects the confidentiality of communications, the inviolability of the home, family life, personal data and, generally speaking, everybody’s right to live their own life, free for undue interference.

Right to the protection of personal data: this fundamental right protects people by giving them a series of rights on the data about them processed by others, imposing on those a series of obligations, and establishing a data protection authority to monitor compliance with the rules.

Sensitive data: data deserving reinforced protection, such as data about peoples’ beliefs, their health, their ethnic origin or their sex life.

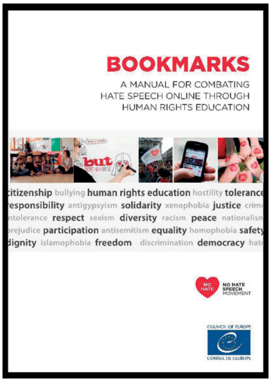
RESOURCES

Data protection authorities: Looking for more information on the data protection rules applying in your country, or perhaps specific guidance? The full list of EU national data protection authorities and their contact details, listed by Member States, can be accessed at http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm. In many of the websites of data protection authorities it is possible to find materials targeting children and youngsters, as well as school teachers.

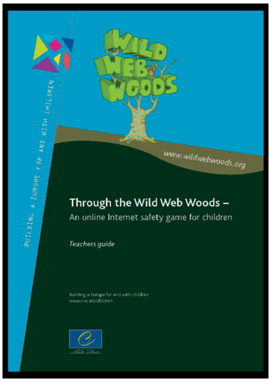
Safer Internet Centres: Need help regarding online safety for minors? Safer Internet Centres typically comprise an awareness centre, helpline, hotline and youth panel. More information and links to national centres can be found at https://www.betterinternetforkids.eu/web/portal/policy/insafe-inhope.

The Charter of Fundamental Rights of the EU: This document lists all fundamental rights recognised as such in EU law. Its Article 7 states that everyone has the right to respect for their private and family life, home and communications, and Article 8 establishes that everyone has the right to the protection of personal data concerning them. To access the full text of the Charter in all EU official languages: http://eur-lex.europa.eu.

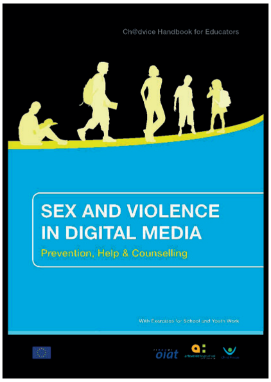
Handbook on European Data Protection Law: To learn more about European data protection law, both at the EU and Council of Europe level, the *Handbook on European Data Protection Law* published jointly by the Council of Europe and the EU Agency for Fundamental Rights (FRA) in 2014 is an excellent starting point. It is freely available, in many EU and a few non-EU languages, at http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law.



Bookmarks: Subtitled A Manual to Combating Hate Speech Online Through Human Rights Education, this booklet targets educators wanting to address hate speech online from a human rights perspective, both inside and outside the formal education system. It is designed for working with learners aged 13 to 18, although activities might be adapted to other age ranges. Versions in English and French can be accessed through the Council of Europe, and other language versions are available through national contact points. More information can be found here: www.nohatespeechmovement.org/bookmarks.


WILD WEB WOODS
www.wildwebwoods.org
Through the Wild Web Woods –
An online Internet safety game for children
Teachers guide
BUILDING A EUROPE FOR AND WITH CHILDREN

Through the Wild Web Woods: An online game commissioned by the Council of Europe to help children to safely navigate the Internet. It is available in more than 20 languages and accompanied by a teachers guide. Follow this path: www.wildwebwoods.org.


Ch@dvice Handbook for Educators
SEX AND VIOLENCE
IN DIGITAL MEDIA
Prevention, Help & Counselling
oiat

Sex and Violence in Digital Media: A teacher handbook with useful information on media violence and phenomena such as cyber-bullying, sexting and grooming. Produced by the Austrian Institute for Applied Telecommunications (OIAT), it is available in several languages and can be downloaded via this link: https://www.saferinternet.at/chadvice/.

This handbook offers practical guidance and tools to teach privacy and personal data protection to children and teenagers at schools in Europe. It covers issues such as individual rights, online safety, digital identity, behavioural advertising, cyber bullying and parental surveillance, addressing them in a clear and sound manner. Teachers and education experts will find in it not only key relevant notions thoroughly explained, but also ideas for discussion, concrete exercises and useful tips adapted to different ages and school levels, as well as award-winning lesson plans. Privacy and data protection experts and professionals, including data protection authorities, will enjoy new insights on how to engage with privacy education and, more generally, on how to raise the awareness of minors on these issues. A Mini-Bill of Privacy and Data Protection Rights, a glossary and a list of resources are also provided.

The volume constitutes the first comprehensive manual of this kind with European reach. It is the result of the coordinated work of legal scholars and data protection authorities. Prepared in the context of the Introducing Data Protection and Privacy Issues at Schools in the European Union (ARCADES) project, co-financed by the European Union's (EU) Fundamental Rights and Citizenship Programme, it is the outcome of a joint effort by all project's partners: the Inspector General for Personal Data Protection of Poland (GIODO), the Information Commissioner of the Republic of Slovenia, the Hungarian National Authority for Data Protection and Freedom of Information (NAIH), and the Law, Science, Technology and Society (LSTS) Research Group of the Vrije Universiteit Brussel (VUB).

ARCADES

Co-funded by
the European Union

LSTS
LAW, SCIENCE,
TECHNOLOGY &
SOCIETY STUDIES
Vrije Universiteit Brussel
Belgium

National Authority for Data Protection
and Freedom of Information

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

INFORMACIJSKI POOBLAŠČENEC
INFORMATION COMMISSIONER

ISBN 978-1-78068-423-9

9 781780 684239