



European Commission – Directorate-General Justice  
With financial support from Fundamental Rights and Citizenship Programme



# **The Summary of Research Studies “Good Practice in Children’s Privacy Protection” and “The Analysis of Target Groups Needs” in Lithuania and Italy**

2010-2011

This publication has been produced with the financial support of the Fundamental Rights and Citizenship programme of the European Commission. The contents of this publication are the sole responsibility of the Lithuanian consumer institute and CODACONS and can in no way be taken to reflect the views of the European Commission.

## CONTENTS

1. GOOD PRACTICE .....	3
1.1. Good Practice in Italy .....	3
1.1.1. Legislative environment.....	3
1.1.2. Self regulation .....	3
1.1.3. Court decisions.....	4
1.1.4. Studies and researches.....	5
1.1.5. Education initiatives.....	5
1.1.6. Conclusions .....	6
1.2. Good Practice in Lithuania .....	7
1.2.1. Legislative environment.....	7
1.2.2. Self regulation .....	9
1.2.3. Court decisions.....	9
1.2.4. Studies and research.....	10
1.2.5. Education initiatives.....	11
1.2.6. Conclusions .....	12
2. THE ANALYSIS OF TARGET GROUPS NEEDS .....	14
2.1. The Analysis of Target Groups Needs in Italy .....	14
2.1.1. Internet Usage .....	14
2.1.2. Personal Data.....	15
2.1.2.1. Understanding personal data .....	15
2.1.2.2. Publication of personal data on the Internet .....	15
2.1.2.3. Understanding threats of disclosure of personal data on the Internet .....	16
2.1.2.4. Privacy violations on the internet .....	17
2.1.3. Protection of Personal Data.....	17
2.1.3.1. Measures to ensure better protection of children’s personal data on the Internet .....	17
2.1.3.2. Privacy policy .....	18
2.1.3.3. Implementation of rights of data subjects.....	18
2.2. The Analysis of Target Group Needs in Lithuania.....	20
2.2.1. Internet Usage .....	20
2.2.2. Personal Data.....	20
2.2.2.1 Understanding personal data .....	20
2.2.2.2 Publication of personal data on the Internet .....	21
2.2.2.3. Understanding threats of disclosure of personal data on the Internet .....	21
2.2.2.4. Privacy violations on the Internet.....	22
2.2.3. Protection of Personal Data.....	22
2.2.3.1 Measures to ensure better protection of children’s personal data on the Internet .....	22
2.2.3.2 Privacy policy .....	23
2.2.3.3. Implementation of rights of data subjects.....	23

## **1. GOOD PRACTICE**

### **1.1. Good Practice in Italy**

#### **1.1.1. Legislative environment**

Italian legislation on children data protection is accomplished with the international standards since the ratification in 1991 of “**The United Nations Convention on the Rights of the Child**” and with the **European Regulations** since the adoption of the **Data Protection Code** in 2003. In particular, the Code’s chapter II refers to “the prohibition to disseminate any reports or images concerning underage persons that allow his/her identification”. The Code application is supervised and enforced by the Italian Data Protection Commissioner (DPC). The DPC also releases specific handbooks and guidelines for users, to inform on the current legislation or to advice on certain digital tools as the social networks. Other important documents at national level are: the **Directive n. 104** released by the Ministry of Education in 2007 to regulate the use of mobile phones and other electronic tools in order to protect pupils’ privacy during educational activities; the **Ministerial Decree – 8 January 2007** which introduced the obligation for the Internet Service Providers to block child pornography sites within 6 hours from notification; and the **Resolution on Children’s Online Privacy**, promoted by the Canadian DPC and adopted in Italy in 2008, which sets the bases for a global strategy of cooperation, education and legislation to guarantee a safe internet environment. Despite the national efforts to regulate the Internet and to accomplish with international standards, **the specific legislation for minors is not sufficiently developed in Italy**. Independent experts consider that the **Italian legislation in force on providers’ liability and court decisions is not really targeted at the interests and rights of minors**.

#### **1.1.2. Self regulation**

In Italy the main codes of conduct to protect children’s rights on the Internet come from main private actors and public stakeholders in this field. The **Self-Regulation Code “The Internet and Minors”** (2003) of the Ministry for Innovation and Technologies aims at raising users’ awareness on safe internet use; creating strict rules to avoid risks and dangerous contents; protecting young people’s privacy; ensuring better cooperation in fighting “computer crimes”. Unfortunately, it is considered

simply as an agreement among the parties who signed it instead of a binding legal instrument and its protectionist principles do not promote a diffused culture of prevention among users and providers. However, the internal “**Code of conduct for Internet service providers**” was signed by their category association in 1997 to create a proper cultural, economic and technical environment for the development of the Internet Market. The code refers to some important principles and obligations concerning the respect of human life and of minors’ sensitivity and privacy. To protect children against sexual exploitation, it invites the ISPs to adopt filtering and blocking systems and to inform end users on how to implement them.

Furthermore, the self-regulations of specific operators are also interesting. Since 1990, journalists are subject to the “**Treviso Paper**” which sets deontological standards in relation to the treatment of news items that involve underage citizens directly or indirectly in any multimedia communication channel. Also the main mobile phone operators adopted, in 2005, a “**Code of conduct for premium services and child protection**” to regulate, among other aspects, on-line services (as chats) and “children’s services” (their advertising, fares, control by adults, etc.). Even though, these measures are not sufficient since they are **limited in the number** and, due to their nature of ‘**soft laws**’, the punishments in case of breaches are too mild to guarantee a proper children’s protection against the service providers interests.

### 1.1.3. Court decisions

**Court decisions related to the violation of children’s privacy are rare.** The most recent one (dated 24/02/2010) regards the accusation, by the Milan Court, of three executives of **Google Inc.** responsible for violating the privacy of a youth by **posting the copy of a video that depicted the child, who has Down Syndrome, being bullied while they should have notified to the DPC its publication by a private user.** The judgment remarks the duty of Google to make explicitly clear to users what their responsibilities are regarding their own and other people’s privacy. Furthermore, the judgement is interesting for showing two fundamental legal lacks regarding the ISPs: they have no obligation to monitor user-generated content and neither to ensure that users fulfilled the obligations attributed to them by the rules on privacy when publishing information about or from third parties.

#### 1.1.4. Studies and researches

In the last years, **the specific studies and in-depth researches on the Italian context have been few**. We believe that this is probably linked to the absence of an efficient national regulation.

The publications registered by our mapping are mainly essays or university thesis that **analyse the risks that represent the use of Internet for minors**, especially the ones linked to violation of their privacy and “computer crimes”. From the “**EU Kids Online**” study of the Italian context, within a specific European Research, came up that 17,6% of teenagers aged 12 to 19 have been victims of e-harassment. Other interesting studies focus on **children’s behaviours and attitudes towards the new media**, some of them including surveys to measure the youth habits and their knowledge on their privacy rights. These studies provide useful **recommendations to parents and educators**. In particular, the Save the Children’s study, “**Connected children. Italian preadolescents and new media**”, highlighted that minors are “active explorers” and that approaches of supervision and prohibition are not effective. Finally, it is important to remember the “**Young People and the New Media**” study that aimed at developing a strategy to improve security in cooperation with institutional and educational bodies, suggesting some solutions within the existing legislation.

#### 1.1.5. Education initiatives

Apart from research, in the educational field, Italy counts on a **wide range of awareness activities addressing young people** directly and indirectly (through adults and stakeholders). In addition, **there is a significant number of institutes and centres, public and private, that operate monitoring the digital world and organizing meetings, trainings and other educational activities** to promote a safer and more conscious use of the Internet among young people and families. Some of them are: **CORECOM**, the Regional Committee for Communication; the **Privacy Development Lab** set up by the Italian Data Protection Authority; the **Italian Institute for Privacy**, recognized at European level for its network of experts on legislation for the new technologies; the **Digital Youth Consortium** (since 2006, Digital World Foundation), an NGO bringing together public institutions and the main ICT companies for the construction of an inclusive knowledge society by blending innovation and education; **EASY**, the Italian Awareness Centre, established in accordance with the UN Convention on the Rights of the Child and supported by a strong network of national stakeholders; **EAST**, the Italian Safer Internet Centre, co-founded by the European Commission, active even in the

implementation of national and EU policies/initiatives; and **Postal Police** which investigate to prevent online crimes. These institutions, together with other NGOs and Italian Ministries, carry out a wide range of awareness activities such as: competitions, as the “**Global Junior Challenge**” to detect best practices in the fighting of digital division; awareness-raising campaigns, as “**EASY weeks**”, with meetings, laboratories, role-plays, etc.; digital platforms and websites, as “**STOP-IT**” (against child pornography) and “**Security on the Net**” (informing on privacy rights and social networks use); virtual meetings, as “**Unicef Infobus**”, a prevention campaign performed through a social network; and concerts, as “**One click for you**” with the participation of 3.000 teenagers. Furthermore, every year Italy participates in the European initiative of “**Safer Internet Day**”. All the activities target young people and therefore refer the most popular activities among them: social networks, chats, forum, dating sites, etc.

#### 1.1.6. Conclusions

**Even if young people and adults in Italy are highly informed about the risks linked to the Internet use through awareness actions and educational initiatives, the lack of a proper and specific legislation for protection of minors is evident.** To reduce the cases of electronic harassment and violations of children’s privacy, a step forward in the legislation is necessary. Without proper regulations that effectively limit the ISPs (through **obligations, sanctions and remedies**) and that provides **effective measures to control user-generated contents**, children’s privacy won’t be fully respected and guaranteed.

Furthermore, the **user complaint process** is an aspect which should be improved: the numbers of “computer crimes” detected through research surveys is not reflected in the number of court sentences (which are very rare). This could be due to the lack of proper information on how to access it or to the length and difficulty of the process itself.

Finally, the **interaction between research and legislation** must be enhanced with the involvement of the Government. In this sense, the experience of the centres and experts networks reported could have positive effects on the update of legislation and should be strongly taken into account.

## 1.2. Good Practice in Lithuania

### 1.2.1. Legislative environment

Lithuania as a member of several international organisations has ratified and implemented a number of international instruments which recognise the right to privacy and personal data protection - **European Convention for Protection of Human Rights and Fundamental Freedoms, Charter of Fundamental Rights of the European Union, Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** and others. The right to privacy is also enshrined in Article 22 of the **Constitution of Lithuania** which guarantees the inviolability of the private life as well as of personal correspondence, telephone conversations, telegraph messages, and other communications. The right to privacy and secrecy is a 'specific civil right of natural persons' under Article 2.23 of the **Civil Code of the Republic of Lithuania**. This article also states that information on person's private life may be made public only with his or her consent.

As a member of the United Nations, in 1995 Lithuania has ratified **the Convention on the Rights of the Child** which establishes the right to privacy as one of the fundamental rights of the child. The same right of the child is recognised also in the **Law on Fundamentals of Protection of the Rights of the Child**.

The main legislative framework for personal data protection is established in the **Law on the Legal Protection of Personal Data**, which implements the Directive 1995/46/EC. The law lays down the basic personal data protection principles, processing standards and rights of data subjects. Unfortunately, the law does not specifically regulate the processing of personal data of minors. According to the Law the State Data Protection Inspectorate is responsible for its supervision and monitoring of the implementation.

In addition to the main principles and standards of the Law on Legal Protection of Personal Data, the processing of personal data in the field of electronic communications is governed by the **Law on Electronic Communications**. This law additionally establishes specific duties for data controllers processing personal data for direct marketing purposes.

The **Law on Services of Information Society** regulates the provision of information society services and encourages the self-regulation, i.e. establishes the right of trade, professional and consumer associations to draw up codes of conduct (ethics) designed to regulate activities of the service providers. The law also states that the Information Society Development Committee under the

Ministry of Transport and Communications should encourage drafting up codes of conduct regarding the protection of minors. Despite this duty prescribed by law, until now there are no codes of conduct based on Article 16 of the Law on Services of Information Society determining the rules on professional ethics related to the protection of minors.

Lithuania has developed a comprehensive regulation to protect minors from dangerous internet content. The **Law on Protection of Minors against Detrimental Effect of Public Information** prohibits dissemination of information which has a detrimental effect on minors, such as information of violent, erotic, criminal, paranormal nature, information which invokes fear or horror, promotes gambling, self-mutilation or suicide, degrading human dignity, sexual relations between minors, and defines related responsibility of public information producers and disseminators. A separate category of such information of detrimental effect to minors is information related to minors' personal data published in prescribed cases. The supervision of the implementation of the provisions of the law is carried out by the Inspector of Journalist Ethics.

Control of illegal public information on the internet (restricted and forbidden public information), including the detection, monitoring and closure of internet websites with illegal information, is governed by the Procedure on the Control of Forbidden Information on Public Use Computer Networks and the Distribution of Restricted Public Information approved by the **Resolution No. 290 of the Government of the Republic of Lithuania**. The rules of the procedure foresee publication of restricted information (information which has a detrimental effect on minors) in electronic media and other internet websites. It obliges the Police Department under the Ministry of the Interior to ensure the proper operation of a special phone number and mailbox enabling any person to report publication and distribution of information which is prohibited or restricted by the laws of Lithuania. It also obliges the Lithuanian Criminal Police Bureau and other law enforcement institutions to carry out the investigations within their competence.

The State Data Protection Inspectorate as main personal data protection institution has published several recommendations related to the protection of personal data on the internet. Even though none of the recommendations explicitly focuses on children personal data protection and security online, some of them, for instance, **Recommendations on Privacy protection in Using Wireless Local Area Networks, Recommendations on Safe Data Transfer by Email, Recommendations "How to avoid SPAM?"**, may be a useful reference for all internet users, including children. Service providers may refer to recommendations for preparation of ethical codes of data processing, user's identification on internet websites and safety of public electronic communication services and networks.



### 1.2.2. Self regulation

In Lithuania the only self regulatory initiative in existence is the **National Code of Practice for Safe Use of Mobile Communications by Minors** signed by the Lithuanian mobile network operators UAB „Tele 2“, UAB „Omnitel“ and UAB „Bite Lietuva“ in 2008. It aims to protect consumers under 18 years of age from possibly harmful services and content while using mobile communication media (devices) and services and to provide parents and guardians with the means of responsible use of information society services. However, this code is more a declarative than an effective measure and it cannot be considered as a legally binding code of conduct within the meaning of Article 16 of the Information Society Services Law.

On the EU level, it is worth to mention a self-regulatory agreement of **Safer Social Networking Principles for the EU**, under which one of the main Lithuanian social networks One.lt is subscribed.

### 1.2.3. Court decisions

Court practise concerning the right to privacy of children is not very rich. There are several decisions related to different aspects of the children right to privacy.

A decision concerning **the right to image** was delivered by the Supreme Court of the Republic of Lithuania in 2003 and concerns the publication of the image of a 12 years old girl for advertisement purposes in a newspaper without her consent. The court recognised the use of the picture illegal and attributed moral damages to the applicant.

Several decisions regarding the **publication of personal data of minors by media and protection against detrimental effect of public information** were adopted by the Supreme Administrative Court of Lithuania. In 2006 in an administrative case where the applicant (a TV broadcaster), asked for the annulment of the decision of the Inspector of Journalist Ethics on publication of information related to minors on TV broadcasts, the court concluded that the prohibition of publication of the information is unconditional and further determination whether it has caused negative effects on minor is not necessary. In two cases of 2007 and 2009 the same court decided that personal information of minors, including photos, may not be published in the context of the information which according to the Law on Protection of Minors against Detrimental Effect of Public Information has a detrimental effect on the development of minors, even when the consent of legal representatives was obtained. The consent cannot ensure that publication of personal data cannot make

any damage to a minor. The disclosure of such information could not be justified by the intention to protect the interests of the minor or by socially valuable purposes.

As regards the possibility to reveal identity of the minor, the Supreme Administrative Court of Lithuania decided that minors may be identified even if their name is not mentioned in the publications, but other details such as gender, father's and grandmother's names and city of residence are disclosed.

The Senate of the Supreme Court of the Republic of Lithuania as regards rights **and obligations of parents related to the privacy of the child** in 2002 noticed the necessity to strike the right balance between the child's right to personal life and parental authority. The court also underlined that the court proceedings concerning publication of information about private lives of adults in media can often affect their children's privacy.

In 2005 the Constitutional Court of the Republic of Lithuania adopted a decision related to the **control of forbidden information on public use computer networks**. The Constitutional Court addressed the question whether provisions of the Procedure on the Control of Forbidden Information on Public Use Computer Networks and the Distribution of Restricted Public Information concerning duties of providers of information hosting services and providers of public use computer networks are in line with the Article 25 of the Constitution of the Republic of Lithuania, which guarantees freedom of expression and the right to seek, obtain and disseminate information and ideas. The Constitutional Court noted that according to the Constitution of the Republic of Lithuania everyone is obliged not to disseminate information that is forbidden by law and not to violate procedure of distribution of restricted information. Persons who become aware that they are somehow involved in the dissemination of forbidden information, or otherwise contribute to the dissemination of such information, or in any other way violate procedure of the distribution of restricted information, must immediately stop such action.

#### **1.2.4. Studies and research**

Up until now in Lithuania there have been just a few efforts to conduct academic research on minor's personal data protection in electronic communication field. Several academics from the Department of Legal Informatics of Mykolas Romeris University and Center of Legal Informatics of Vilnius University have published more general academic articles related to the protection of personal data on the internet.

According to the knowledge of the author, there are only few academic publications to a certain extent relevant to the protection of minors on the internet. For instance, an article in academic journal *Jurisprudencija* entitled "**Protection of Minors Against Detrimental Effects of the Public Information**" published by Edita Žiobienė in 2006 or a Master's thesis "**Codes of conduct: their place and meaning in regulation of illegal and harmful information disseminated in computer networks**" defended by Ignas Vajega, a student of Mykolas Romeris University, under the supervision of the professor I. Rotomskis in 2007.

### 1.2.5. Education initiatives

The key educational initiatives in the area of children's personal data protection in Lithuania are carried out under the **Safer Internet (Saugėsnis internetas) project** within the framework of European Safer Internet Action Plan Programme of the European Commission. The project includes the national awareness raising node, hotline facility and project's website [www.draugiskasinternetas.lt](http://www.draugiskasinternetas.lt). Besides these activities, the project coordinators and partners also implement a wide range of visibility events, campaigns (**Safer Internet Day**), conferences (**Internet Academy on wheels TEOBUS**), competitions ("**The safe internet school**", "**Safer Internet Day in my school**") seminars for target user groups about Safer Internet, maintain a Youth Panel on the E-School portal and offer an online education programme for parents and adults to learn about children's online safety (**Online Educational Program "Window to the Future"**). Moreover, during the project some awareness raising publications ("**Tips for children**" and "**Advice for parents. Making our children safer on the internet**") were designed and distributed throughout Lithuania. A documentary film "**The Network**" on children's online safety was created and broadcasted in the TV and on the internet.

Another important national measure for information and awareness raising is a specialised **e-security website** ([www.esaugumas.lt](http://www.esaugumas.lt)) which was launched in 2006 by Telecommunications Regulatory Authority in cooperation with the Ministry of the Interior and private business entities. The website offers information about security online, presents possible dangers, such as viruses, unsolicited messages, cheating and cyber bullying, etc., and gives practical advices on how to avoid them. It has a separate section of information on "**Children and the internet**".

It is also worth to mention the **project "Development and initial implementation of an educational strategy on Internet safety for multipliers, teachers and parents"**, which was carried out by several EU consumer associations, including National Consumer Confederation from Lithuania,

in 2004 within the framework of Socrates, Grundtvig 2 programme. The project aimed to empower and raise awareness of parents, teachers and partner organisations in order to prevent child abuse on the internet and to avoid harmful effects (violence, racism, pornography, etc.) related to the use of the internet.

Activities of the **Expert Group for Cooperation on Children at Risk** established within the Council of the Baltic Sea States related to children's safety on the internet are also important. Lithuania in the expert group is represented by the Ministry of Social Security and Labour of the Republic of Lithuania.

### **1.2.6. Conclusions**

Although the right to privacy and personal data protection is recognised by the international treaties ratified by Lithuania and regulated by the Constitution, as well as national laws, there is a clear lack of special rules for protection of children's personal data. Children, as a unique group of data subjects, deserve a particular attention and protection, especially regarding their personal data in the online environment and currently applicable general data protection principles and standards established in the Law on the Legal Protection of Personal Data, are neither sufficient nor effective. Also there are some legal gaps related to the children's consent and legal capacity, representation and possibility of using and safeguarding the right to personal data protection.

Contrary to the area of children's personal data protection, in the area of children's protection from harmful internet content Lithuania has developed a comprehensive regulation through the Law on Protection of Minors against Detrimental Effect of Public Information and Resolution No. 290 of the Government of the Republic of Lithuania. Court practise in this area is also the most extensive and amounts up to three cases related to the publication of personal data of minors by media and protection against detrimental effect of published information.

The State Data Protection Inspectorate, as a state body responsible for the implementation and defence of the human right to privacy and personal data protection, could work more purposely in this area through recommendations, preventive checking and awareness raising campaigns among children, parents and teachers. These activities could help to bridge the regulatory gap in the field of children's data protection. In addition, other state institutions and non-governmental organisations should be encouraged to play a more active role in the awareness raising activities related to the children's right to privacy. This would contribute to the few existing education activities, which are very rare apart from initiatives carried out under the Safer Internet project.

The self regulation in the sphere of minor and consumer protection is encouraged by the laws, but possibilities that service providers will draft legally binding codes of conduct to protect minors as a special group of consumers on the internet are very limited in practise. As current situation shows there are no legally binding codes of conduct based on Article 16 of the Information Society Services Law drafted and the only non-binding self regulatory initiative in existance is the National Code of Practice for Safe Use of Mobile Communications by Minors. If the service providers' industries were encouraged to look for a consensus between them in specific operation areas, self regulation would add a significant value to the existing general data protection legal standards.

Court decisions in the field of children's personal data protection are rare and uniform practise is not formed. In addition administrative and criminal sanctions for personal data protection violations are not very effective and dissuasive. Moral damages for data subjects in case of their privacy violations are too low.

Finally, academic research and analysis on children personal data protection and safety in electronic communication field should be strengthened. Qualified research on the subject could contribute to the legislative amendments and better regulation of the matter.

## 2. THE ANALYSIS OF TARGET GROUPS NEEDS

### 2.1. The Analysis of Target Groups Needs in Italy

#### 2.1.1. Internet Usage

As regards **activities performed by children** on the Internet the most popular ones with daily frequency are: *collection of information (39%), load (circulation) of information about themselves or their friends (39%) and download of music and films (37%)*. Of these activities, the *load and circulation of personal information* on the Internet is the only one at risk of infringements of the users' and their friends' privacy. In Italy, *chatting with unknown person is not a prime danger*, since 43% of children involved in the survey have declared that they never do it, while only 16% do it every day.

The survey showed a large and widespread **use of social networks** among children. The most popular one is *Facebook* as 66% respondents use it every day. If we refer to the most common use of Facebook (sharing of photos, personal information, habits, activities and events to which the user will assist), we can connect the children's use of Facebook to the above mentioned load/circulation of information. Thus, a potential risk is the **misappropriation of children's personal data** and their use for illegal purposes which could go from the infringements of their rights to more serious crimes.

**Responses by parents to the question of how often their children perform such activities** reveal that *majority of the parents have no clues about it*. In this regard, it is representative that many of the interviewed parents do not know if their children chat with unknown people (41%) or load information about themselves and their friends (37%). The only activity that 31% of the parents recognize that their children perform with high frequency (several times a week) is the *collection of information on the Internet*.

Furthermore, adults involved in the survey (both **parents and teachers**) **do not share with children the knowledge on how to use internet to socialize with other people**: this is an important intergenerational gap. As regards the adults' use of social networks, 59% of parents use Facebook and 37% are not registered in any social network; 67% of teachers are not registered in any and 30% of teachers use Facebook.

Based on these data, it is important to underline the **need for a greater involvement of adults in children's usage of the internet**, both as it comes to interest in the activities children perform (especially in the case of parents) and awareness of the potential risks linked to such activities (to be

raised by parents and teachers). Children should be deeply and clearly informed on the possible consequences of their incorrect or unlimited use of internet (with respect to publication of personal data) and should be given behavioural paths to protect themselves and their friends. The main limitation is that **adults close to children may not be totally aware of the possible risks their children incur**, due to their limited use of internet as to the generational gap regarding the activities performed on Internet. For these reasons, we believe that **involvement of public and private institutions and NGOs operating in the field of protection** of minors and consumers is extremely necessary. These stakeholders should address their awareness activities towards children directly or indirectly (through parents and teachers). Even though, parents should adopt the habit of talking with their children appealing to a reciprocal dialogue on these subjects; while, on the other side, teachers should complement the parents' effort by dealing with these problematic issues within the educational context.

## **2.1.2. Personal Data**

### **2.1.2.1. Understanding personal data**

The answers to the question “**What, in your opinion, is personal data?**” disclosed a *great difference in the respondents' opinions (children, parents and teachers)*. 100% of answers have been assigned only to *name and surname* and exclusively by parents' group; 95% of the children marked this option and only 23% of the teachers identified this information as personal data. If we consider that *all the answer options provided by the survey were personal data*, no identification from the interviewed of some of them is significant and brings to light the *need to raise awareness of children, parents and teachers on the definition of personal data*. The most striking fact which can support our argument is that school name has been identified as personal data only by 12% of the children; even more shocking is that none of teachers have marked this option!

### **2.1.2.2. Publication of personal data on the Internet**

In correlation to what was underlined in the previous section, we have to indicate that the **children** who took part in the survey **are not likely to publish their personal data on the internet**. Even though, a small percentage of those who do, provide information such as *school name (38%)*,

*membership to extracurricular activity groups (26%) and name and surname (24%).* These are obviously key information which could enable a evil-minded person to misappropriate the child identity or to know exactly where to find him/her and when.

Other alarming data in this respect comes from the question if they **provide correct personal data** when registering in various sites on the Internet: *52% of the children answered “sometimes”*, while only 14% never do and 11% do not register when asked to provide this information. Furthermore, the majority of them **provide real information about themselves while communicating in social networks or dating sites** (39% do it sometimes and 19% do it often). Finally, it is important to note that 15% of the children don't think that it is necessary to **get their friends' consent before publishing their personal data** (photos, information about certain details of their lives) on the Internet while, on the other side, 35% always ask for it.

If children usually publish personal data about themselves and their friends, adults do not share the same habit. 59% of parents and 89% of teachers *never circulate on the internet information about their children/students*. Even though, this could be simply due to the fact that adults are not likely to use social networks.

### **2.1.2.3. Understanding threats of disclosure of personal data on the Internet**

Even if children, parents, teachers and service providers have ranged differently the listed **possible threats associated with the personal data disclosure on the Internet**, almost all options have scored high percentages. In particular, children (85%), teachers (70%) and service providers (86%) agreed that the most possible risk is the *misappropriation of identity* in order to make a purchase or, for instance, perform cash transactions on behalf of another person; while the prime threat identified by parents (63%) is the *electronic harassment* to intimidate another person or to cause tension. Though a general awareness has been detected, more actions must be released to inform all target groups on other possible menaces not included in the list, and especially to advert the ones who have not marked any threat (8% of children, 9% of parents and 4% of teachers). It is significant to note that *none of the service providers*, who are the ones that mostly handle this issue, *has selected the answer “I don't think there are any threats”*.

The scene is more worrying if we refer to the involvement of **parents and teachers in the familiarization of children with privacy policies and potential threats**. The majority of parents (59%) and of teachers (67%) *have not talked with children about these topics*, regardless the reason



why (someone thinks it is not important, others that it is not their responsibility or that children are already aware). It is even worse if we take into account that this lack of dialogue is present despite many parents (66%) and teachers (44%), **do not think that children have enough knowledge on possible threats** associated with the personal data disclosure on the Internet. As already stressed, the involvement of adults in warning children is urgent and necessary.

#### **2.1.2.4. Privacy violations on the internet**

When referring to **direct or close experiences of violations** (such as circulation of photos and personal data without consent or false information, misappropriation of identity, reception of unwanted proposals by unknown people), *the majority of the children interviewed have never faced big threats to their privacy*. In fact, the most common case has been the *circulation of photos or video clip on the Internet without previous consent (20%)*. *Neither parents nor teachers' have showed sufficient awareness on these violations* happening to their children or students and this should be object of work to get an improvement in their participation.

#### **2.1.3. Protection of Personal Data**

##### **2.1.3.1. Measures to ensure better protection of children's personal data on the Internet**

Almost all the **measures**, listed in the survey, **to ensure better protection of children's personal data** on the Internet have been marked as necessary by each target group, even if with a different scale of priority. The ones that have been identified as the most effective to implement are: *diffusion of a "Safe Internet" idea* – option selected by 65% of the children themselves and 64% of service providers) and *formal and informal education of children* (by 84% of parents and 59% of teachers). The need of awareness raising campaigns has been stressed too, together with enhanced responsibility of both the website administrators and the users. Implementation of better laws would surely help to make the website administrators to assume their responsibility. However, a stricter parental control would overburden children without getting results and this is why it should be replaced by more interactive educational tools. In this regard, the service providers have remarked that **educational (33%) and legal (29%) measures are the most insufficient ones**. This accords with the perception of parents and teachers.

### 2.1.3.2. Privacy policy

If we consider that **42% of service providers interviewed do not have a privacy policy**, we can understand why users (both children and adults) are not familiarized with it. Only *16% of children get informed on the website's privacy policy or set privacy settings* when publishing information about themselves or their friends. Even worse, *60% of parents and 85% of teachers never do* while publishing personal data of their children/students!

The need of more commitment from service providers is evident as the legal obligation to have a privacy policy. However, parents need to adopt the habit to control how and what personal data may be used, what are user rights, responsibilities and so on, in order to transfer this knowledge and positive attitude to their children/students.

### 2.1.3.3. Implementation of rights of data subjects

When asked to indicate **who should familiarize children with the possible infringements of personal data on the Internet and remedies to avoid them**, all the target groups have given the prime responsibility to the people naturally charged to educate children: *parents* (73% of the children and 70% of the teachers) and *teachers* (75% of the parents and 86% of the service providers). If we cannot blame children for their choice, we should at least notice that this *crossed responsibility teachers / parents* is a leitmotif that comes out in almost every discussion regarding educational issues. A surprising absence is that of the *NGOs* which are probably not identified as stakeholders in this field; this means that they should get involved with more emphasis in the promotion of the respect for children's privacy on the Internet, may be organizing the awareness and educational activities requested by the target group interviewed and therefore release the parents' and teachers' burden.

If we move to the **responsibility of protection once the children's right to personal data has been breached**, parents (31%) and teachers (41%) agrees pointing to the *State Data Protection Inspectorate* and leaving in a second place the website's manager. This selection reflects their identification with the legal process of accusation. In the answers of *teachers* we can detect also a *low interest in the protection of their students' rights*, since 19% declared that this task is not upon their responsibility. The teachers' involvement should be strongly motivated, based on the assumption that *they are an important referral for their students*.

Service providers have also registered **direct requests from users** regarding the management of their personal data. According to the respondents, users show concern mostly on *which personal data are collected and from which sources are processed* (71%), as *for which purposes* (57%). Other users' complaint are linked to the *willing to withdraw the consent to process their personal data* (71%) and to *erase their personal data or terminate any operations of processing upon them* (57%).

## 2.2. The Analysis of Target Group Needs in Lithuania

### 2.2.1. Internet Usage

As regards activities performed on the Internet, the most popular ones are downloading music, films and etc. (39% of children do it every day, 37% - several times a week), and collecting information (22% do it every day, 45% - several times a week). The survey also showed that 20% of children load (circulate) information about himself/herself or his/her friends on the Internet, 19% chat with unknown person several times a week. Taking into account that such activities could lead to very serious infringements of children's rights or even crimes, **it is very important that children knew possible consequences and rules they should respect in order to avoid such breaches.**

31% of parents don't know whether their children chat with unknown persons and 22% are not aware whether they load (circulate) information about themselves or their friends on the Internet. In conclusion, **it could mean that they have never been interested in or their children don't want to talk with them about it.**

According to the survey results, social networks are widely used by children, parents and teachers as well. 53% of respondents among children daily use international social network Facebook, and 21% use Lithuanian website One.lt or other social networks or dating websites. The majority of adults (65% of teachers and 53% of parents use Lithuanian website Klase.lt, 53% and 58% respectively use Facebook) use social networks or dating sites, so they should be quite aware about the peculiarities of such types of websites, **but it is also important that they were concerned with possible threats to privacy.** Taking into account such widespread usage of social networks among children, **it is very important that children knew possible dangers they are faced with and how to use tools provided by controllers of these websites in order to protect privacy.** However, **controllers of such websites should take appropriate actions to limit the risks with regard to children.**

### 2.2.2. Personal Data

#### 2.2.2.1 Understanding personal data

The answers to the question "What, in your opinion, is personal data?" disclosed great difference between the opinions of respondents (children, parents and teachers) – from 17% to 97%. **Taking into**

**account that all categories of data – even school name, if it would be related to particular person (for example, schoolchild, teacher) whose identity could be directly or indirectly revealed - are personal data, awareness of children, parents and teachers concerning definition of personal data should be raised.** The same could be said about opinion of respondents on possible threats associated with the personal data disclosure on the Internet.

#### **2.2.2.2 Publication of personal data on the Internet**

The results showed that the majority of children (more than 70%) never share their personal identification number, home address and information related to their religion and illnesses. Conversely, the most revealed personal data appeared to be name and surname (92%) and email address (87%).

**Worrying is the fact that children rarely question the necessity to provide correct personal data when they register on various Internet websites.** Almost half (45%) of the children always or often provide correct information during the registration process on Internet websites and even 55% always or often say truth to those with whom they socialize.

Other unadvisable behavior on the Internet is publication of personal data of other people – more than 60% of children are engaged in this activity and **only 1/3 of them always receive consent of a person concerned.**

20% of parents often publish information related to their children on the Internet, but only 49% of them always familiarize themselves with the website's privacy policy or set privacy settings. It means that **awareness of adults about necessity to get acquainted with privacy policy and set privacy settings should be raised.**

#### **2.2.2.3. Understanding threats of disclosure of personal data on the Internet**

As regards opinion of respondents on possible threats associated with the personal data disclosure on the Internet, **almost all options were indicated by more than half of respondents.** 85% of teachers, 79% of parents and 72% of children indicated misappropriation of identity in order to make a purchase or perform, for example, cash transactions on behalf of another person as the most possible threat, and 78% of service providers – unsolicited advertising for commercial purposes (SPAM). **Worrying is the fact that 10 % of children don't think there are any threats.**

Parents nor teachers don't think it's not important to talk about privacy, personal data and threats associated with the personal data disclosure on the Internet with the children/schoolchildren, so it is very important that they have enough knowledge and provide children with correct information, especially taking into account that 50% of parents and even 68% of teachers think that children are not quite aware about such threats.

#### **2.2.2.4. Privacy violations on the Internet**

As regards to facing violations of using personal data on the Internet, the majority of children said that they have never experienced indicated cases related to privacy violations on the Internet. The most experienced case is receiving unwanted proposals – 19% of children more than once received unwanted proposals by phone or e-mail. 10% said that more than once his/her photo was circulated on the Internet without his or her consent.

It seems that **parents do not have enough information about threats their children are facing on the Internet**. As it was already mentioned, 10% of children said that more than once their photos or videos were circulated on the Internet without their consent, but only 3% of parents indicated that they knew about more than one of such cases. In respect to answers of teachers, 29% said that one or more than one of such cases is known to them. Similar situation is with all indicated cases, so in conclusion, **teachers are more aware about violations of data protection and privacy of schoolchildren on the Internet**. It could mean that teachers are more interested in schoolchildren's activities on the Internet, or that children are more linked to talk about it with teachers than with parents.

#### **2.2.3. Protection of Personal Data**

##### **2.2.3.1 Measures to ensure better protection of children's personal data on the Internet**

The most important data protection measure for parents (73%) and service providers (100%) seems to be formal and informal education of children, for teachers (59%) – stricter parental control over children, for children (56%) – propagation of "Safe Internet" idea (this measure is also quite important for service providers – 67%, teachers – 47%, parents – 39%). Taking into account that all of the respondents think that educational tools should be improved, **great attention has to be paid to elaborating formal and informal education, propagating „Safe Internet“ idea and strengthening**

**understanding of personal responsibility of users. Adults should be informed how to use programs limiting children's activity on the Internet.**

The majority of service providers also advice to enhance self-regulation (78%), legislative (56%) and organizational (44%) personal data protection measures.

### **2.2.3.2 Privacy policy**

The study has shown that **service providers are quite knowledgeable and concerned about personal data protection of their website visitors.** Although according to the Lithuanian data protection laws, service providers are not directly obliged to have a privacy policy (when the privacy policy differs from the personal data processing rules) and to publish it on the website, all of the service providers participating in the survey, except one, have the privacy policy for their websites.

According to the survey results, it seems that children don't understand the necessity to familiarize themselves with privacy policy – 26% do it only sometimes, 17% never do it and 13% don't even think it is necessary. **Children have to be informed that in order to ensure personal data and privacy protection on the Internet, they should always familiarize themselves with privacy policy and select appropriate privacy settings.** It is also very important that they understand the necessity and meaning of these actions.

### **2.2.3.3. Implementation of rights of data subjects**

The results of the survey show that data subjects implement their rights very passively. The few requests which service providers received from data subjects included the request to destroy or terminate the processing of personal data and to rectify the personal data published on the website. **According to the survey data subjects have never tried to use their other data protection rights, such as to receive information about processing of their personal data by the service provider, to withdraw the consent for the processing, etc.**

With regard to obligation to familiarize children with the possible infringements of personal data on the Internet and remedies to avoid them the vast majority of adults - 95% of parents, 94% of teachers and 89% of service providers think that this is a duty of parents. 94% of teachers consider it is to be their obligation. Children do not have such clear opinion – 57% of them think that it should be done by parents, 58% - by teachers, 54 % think that they should have interest themselves.

**Those who are directly involved in children's activities on the Internet and their everyday life (managers of websites, parents, teachers) should have primary obligation to familiarize children with the possible infringements of personal data on the Internet and remedies to avoid them.** Media, state institutions, such as State Data Protection Inspectorate and others, NGO's also have to play their role in this field. **In order for these activities to be effective, children should have great interest themselves.**