ARTICLE 29 DATA PROTECTION WORKING PARTY

00483/08/EN
WP 147

Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools)

Adopted on 18 February 2008

I – Introduction

1) – Framing

This opinion is concerned with the protection of information about children. It is aimed primarily at those who handle children's personal data. In the context of schools, this will include teachers and school authorities in particular. It is also aimed at national data protection supervisory authorities, who are responsible for monitoring the processing of such data.

This document should be seen in the context of the general initiative of the European Commission described in its communication "Towards an EU strategy on the Rights of the Child". In contributing to this general purpose, it aims to strengthen the fundamental right of children to personal data protection.

This subject is not entirely new to the Art 29 Working Party, which has already adopted several opinions related to this issue. Its opinions on the FEDMA code of conduct (Opinion 3/2003), on geolocalization (Opinion 5/2005) and on Visa and Biometrics (Opinion 3/2007) include certain principles or recommendations concerning children's data protection.

The aim of this document is to consolidate this issue in a structured way, defining the applicable fundamental principles (Part II) and illustrating them by reference to school data (Part III).

The area of school data was chosen because it is one of the more important sectors of children's life, and comprises a significant part of their daily activities.

The importance of this area is due also to the sensitive nature of much of the data processed in educational institutions.

2) - Purpose and scope

The purpose of this document is to analyse the general principles relevant to the protection of children's data, and to explain their relevance in a specific critical area, namely, that of school data.

In doing this, it aims to identify issues important to the protection of children's data in general, and offer guidance for those working in this field.

According to the criteria in most relevant international instruments, a child is someone under the age of 18, unless he or she has acquired legal adulthood before that age.

A child is a human being in the complete sense of the word. For this reason, a child must enjoy all the rights of a person, including the right to the protection of their personal data. However, the child is in a special situation, which should be seen from two perspectives: the static, and the dynamic.

From the static point of view, the child is a person who has not yet achieved physical and psychological maturity. From the dynamic point of view, the child is in the process of developing physically and mentally to become an adult. The rights of the child, and the exercise of those rights – including that of data protection, should be expressed in a way which recognises both of these perspectives.

This opinion is based on the conviction that education and responsibility are crucial tools in the protection of children's data. It will examine the main principles relevant to this subject. Most of them relate to the rights of the child, but they will be examined in the context of data protection.

These principles are all contained in the most fundamental applicable international instruments. Some of these instruments relate to general human rights, but also contain specific rules for children. The most important are the following:

- Universal declaration of human rights, 10/12/48 - Arts. 25, 26, N. 3
- European convention for protection of human rights and fundamental freedoms, 04/11/50 - Art. 8
- EU charter of fundamental rights, 07/12/00 - Art. 24[1]

Other instruments which relate directly to the rights of the child are the following:

- Geneva declaration on the rights of the child, 1923
- UN convention on the rights of the child, 20/11/89
- European convention on the exercise of children's rights, Council of Europe, n.º 160, 25/01/96[2]

Naturally, the general perspective of personal data protection must always be considered, as enshrined in the data protection directives (Directive 95/46/EC, 24/10/95 and Directive 2002/58/EC, 12/07/02), and partially in other instruments.[3]

---

[1] And also:
- Helsinki Declaration, June 1964, Pr. I-11,
- International Covenant on economic, social and cultural rights, 16/12/66 – Art. 10, n. 3,
- International Covenant on civil and political rights, 16/12/66 – Arts. 16, 24,
- Optional protocol of 16/12/66.

[2] And also:
- UN declaration on the rights of the child, 20/11/59.
- Recommendations of the parliamentary Assembly of the Council of Europe on various aspects of the protection of children (n. 1071, 1074, 1121, 1286, 1551).
- Recommendations of the Committee of Ministers of the Council of Europe on the participation of the children in family life R (98)8, and on the protection of medical data, R (97), 5.
- Convention on personal relations concerning children, Council of Europe, n.192, 15/05/03.

[3] - OECD Guidelines, 23/09/80,
- Convention 108 of the Council of Europe, 28/01/81 and Additional Protocol of 08/11/01,
- UN Guidelines, 14/12/90.

II – Fundamental principles

A – In general

1) – Best interest of the child

The core legal principle is that of the best interests of the child.[4]

The rationale of this principle is that a person who has not yet achieved physical and psychological maturity needs more protection than others. Its aim is to improve conditions for the child, and aims to strengthen the child's right to the development of his or her personality. This principle must be respected by all entities, public or private, which make decisions relating to children. It also applies to parents and other representatives of children, either when their respective interests are being compared, or where the child is being represented. Normally, the child's representatives should apply this principle, but where there is a conflict between the interests of children and their representatives, the courts or, where appropriate, the DPAs should decide.

2) – Protection and care necessary for the wellbeing of children

The principle of best interest requires a proper appreciation of the position of the child. This involves recognising two things. First, a child's immaturity makes them vulnerable, and this must be compensated by adequate protection and care. Second, the child's right to development can only be properly enjoyed with the assistance or protection of other entities and/or people.[5]

This protection falls to the family, society and 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. This will be mainly in welfare areas: education, social security, health, etc. But this is not incompatible with the adequate and reinforced protection of data in such social sectors, although care should be exercised when data about children is being shared. Such sharing can obscure the principle of finality (purpose limitation), and create a risk that profiles are constructed without reference to the principle of proportionality.

3) – Right to privacy

As a human being, the child has a right to privacy.

---

[4] Enshrined in the UN convention on the rights of the child (Article 3), and, afterwards, was reaffirmed by Convention 192 of the Council of Europe (Article 6) and the EU charter of fundamental rights (Article 24, N. 2).

[5] The right to protection is so fundamental that it is stated in the universal declaration of human rights (Article 25), and was confirmed by the international covenant on civil and political rights (Article 24) the international covenant on economic, social and cultural rights (Article 10, N. 3), and, more recently, by the EU charter of fundamental rights (Article 24).

Art. 16 of the UN Convention on the Rights of the Child provides that no child shall be subject to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.[6]

It must be respected by everybody, even by the representatives of the child.

4) – Representation

Children require legal representation to exercise most of their rights. However, this does not mean that the representative's status has any absolute or unconditional priority over the child's - because the child's best interest can sometimes confer upon them rights relating to data protection which may override the wishes of parents or representatives. Nor does the need for representation imply that children should not, from a certain age, be consulted on matters relating to them.

If the processing of a child's data began with the consent of their representative, the child concerned may, on attaining majority, revoke the consent. But if he wishes the processing to continue, it seems that the data subject need give explicit consent wherever this is required.

For example, if a representative has given explicit consent to the inclusion of his child (the data subject) in a clinical trial, then upon attaining majority, the controller must make sure he still has a valid basis to process the personal data of the data subject. He must in particular consider obtaining the explicit consent of the data subject himself in order for the trial to continue, because sensitive data are involved.

On this issue, it must be remembered that the rights to data protection belong to the child, and not to their representatives, who simply exercise them.

5) – Competing interests: privacy and the best interest of the child

The principle of the best interest can have a double role. *Prima facie,* the principle requires that children's privacy be protected in the best possible way, by giving effect as far as possible to an infant subject's data protection rights. However, situations may arise where the best interest of the child and his/her right to privacy appear to compete. In such cases, data protection rights may have to yield to the principle of best interest. This is particularly the case with medical data, where, for example, a youth welfare service may require relevant information in cases of child neglect or abuse. Similarly, a teacher may disclose a child's personal data to a social worker in order to protect the child, either physically or psychologically.

In extreme cases, the principle of the best interest of the child can also come into conflict with the requirement for the consent of their representatives. The best interest must also here be preferred – for instance if the mental or physical integrity of the child is at stake.

---

[6] This right is a confirmation of the general right to privacy, enshrined in Art. 12 of the Universal Declaration, Art. 17 of the International Covenant on civil and political rights and Art. 8 of the European Convention for the Protection of Human Rights.

6) – Adapting to the degree of maturity of the child

Since the child is a person who is still developing, the exercise of their rights – including those relating to data protection – must adapt to their level of physical and psychological development. Not only are children in the process of developing, but they have a right to this development.[7] The way in which this process is managed in the legal system varies from state to state, but in any society children should be treated in accordance with their level of maturity.[8]

Where consent is concerned, the solution can progress from mere consultation of the child, to a parallel consent of the child and the representative, and even to the sole consent of the child if he or she is already mature.

7) – Right to be consulted

Children gradually become capable of contributing to decisions made about them. As they grow, they should be consulted more regularly about the exercise of their rights, including those relating to data protection.[9]

This duty of consultation consists of taking into account – though not necessarily submitting to – the child's own opinions.[10] This right to be consulted could apply to various different matters, such as geolocation, use of children's images and others.

B – Under the perspective of data protection

1) – Scope of the existing legal framework on data protection

The relevant Directives on data protection, i.e. 95/46/EC and 2002/58/EC, do not explicitly mention the privacy rights of minors. These legal instruments apply to all natural persons, but there are no specific provisions relating to issues particular to children. However, this does not mean that children do not have any right to privacy and that they fall outside the scope of the said Directives. According to the wording of the Directives themselves, they shall apply to any "natural person", and therefore include children.

---

7 UN Convention on the Rights of the Child – Arts. 27, 29.

8 Some legal systems implement this general principle distinguishing the periods before 12, between 12 and 16 and from 16 to 18.

9 UN convention on the rights of the child (Article 12), EU charter of fundamental rights (Article 24, N.1), Convention on personal relations concerning children (Article 6).

10 Such a *criterion* is clearly stated in the Recommendation of the Committee Ministers of the Council of Europe about the protection of medical data - Rec .nº R (97) 5, of 13 February 1997, nr. 5.5 and 6.3.

Given the Directive's limited personal and material scope, a number of questions as to the protection of children's privacy within the framework of the Directive remains. This is because most of the provisions do not take direct account of the particularities of children's lives. Problems arise with regard to the degree of individual maturity of a child as well as the requirement for representation in legal acts.

The data protection needs of children must take into account two important aspects. These are, firstly, the varying levels of maturity which determine when children can start dealing with their own data and, secondly, the extent to which representatives have the right to represent minors in cases where the disclosure of personal data would prejudice the best interests of the child. The following will deal with the question of how the existing rules of the Directive could best be applied to ensure that children's privacy is adequately and effectively protected.

2) – Principles of Directive 95/46/EC

a) Data Quality

The general principles on data quality provided for in Directive 95/46/EC must naturally be adequately adapted when applied to children.
This means:

a.1) Fairness

The duty to process personal data in accordance with the principle of fairness (Art. 6a) must be interpreted strictly when it concerns a child. As a child is not yet completely mature, controllers must be aware of this, and act with the utmost good faith when processing their data.

a.2) Proportionality and relevance of data

The principle set out in the Art. 6c) of Directive 95/46/EC provides that only adequate, relevant and non-excessive data can be collected and processed.

When applying the principles of Art. 6c), controllers should pay special attention to the situation of the child, as they must respect their best interests at all times.

According to Art. 6d) of the Directive 95/46/EC, "*data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data that are inaccurate or incomplete, having regard to the purpose for which they were collected or for which they are further processed, are erased or rectified"*.

In view of children's constant development, data controllers will need to pay particular attention to the duty to keep personal data up-to-date.

a.3) Data retention

In this regard, one must keep in mind the "*droit à l'oubli*" which covers any data subject including, *especially*, children. Art. 6e) of the Directive must be applied accordingly.

Because children are developing, the data relating to them change, and can quickly become outdated and irrelevant to the original purpose of collection. Data should not be kept after this happens.

b) Legitimacy

Directive 95/46/EC sets out fundamental principles in data protection which the Member States have to abide by and implement. With regard to the privacy rights of children, Art. 7 and 8 are of major importance as they state the criteria for making data processing legitimate.

First of all, processing can be allowed if the person concerned has given his unambiguous consent. The meaning of the word "consent" is clarified in Art. 2 (h) of the Directive.

In other words, it must be informed and free. However, consent is not mandatory in all cases. Indeed, processing can also be also legitimate if other legal requirements are fulfilled according to Art. 7 (b-f), for example, processing can also be allowed when a contract is signed.

In cases where representatives breach the privacy of their children by selling or publishing their data, the question arises as to how the right to privacy can be protected if the children themselves are not aware of the infringements. Children need a legal guardian, but in a case such as this, cannot exercise their rights. If the children are mature enough to detect a breach of their right to privacy, they should have the right to be heard by competent authorities, including the data protection authorities.

As to the other conditions in Art. 7 of the Directive that render the processing of data legitimate, the principles of the best interest of the child and of representation, have to be respected, as well. At a certain age, for example, children are able, by law, to enter into contractual obligations, e.g. in the field of employment. But those contracts can only be valid if consent has been given by the representatives. Prior to the conclusion of a contract, or during its performance, the other party may want to collect data on the child as an employee.

Representatives facilitate the data processing by giving their consent. Parents or guardians should make decisions on the basis of the best interest of the child. They should take into consideration the ways in which the disclosure of data could pose a threat to their child's privacy and vital interests, for example, by not disclosing medical data. There are other areas in which even children are allowed to decide independently from their representatives.

Regarding the condition in Article 7 e), it has to be pointed out that the principle of the best interest of the child may be classified as a public interest as well. This might be the case when the youth welfare service needs personal data of the child in order to take care of him/her. The provisions of the Directive may therefore be applied directly to these circumstances.

However, the question arises whether children who can in certain cases conclude legal acts without the consent of their representatives (in instances where they enjoy partial rights), can also give valid consent to the processing of their own data.

According to applicable local regulations, this might occur in cases of marriage, employment, religious matters etc. In other cases the child's consent might be valid on condition that the representative does not object. It is also clear that children's level of physical and psychological maturity must be taken into account, and that from a certain age they are able to judge matters related to them. This might be important in instances where the representative does not agree with the child but the child is mature enough to decide in his or her own interest, for example, in a medical or sexual context. Instances where the best interest of the child limits or even prevails over the principle of representation should not be neglected, and need further consideration.

The widest legitimacy ground refers to the legitimate interests of the controller or of a third party (Art 7 f), except where they are overridden by the interests or fundamental rights and freedoms of the data subject. On making this balance, special care must be taken in relation to the status of children as data subjects, using their best interests as a guide.

c) Data security

According to Art.17 of the Directive 95/46/EC, "*Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration unauthorized disclosure or access*" and specifies that:

"*Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.*"

Data controllers and processors should be aware that children's data require a high level of protection.

d) Rights of data subjects

d.1) Right to be informed

It should be pointed out that the consent requirement under the Directive goes hand in hand with the obligation to adequately inform data subjects (Art. 10, 11, 14).

The Working Party has already had the opportunity to address information requirements in several documents; in particular, the Opinion on more harmonised information provision (WP 100) and the Recommendation on certain minimum requirements for collecting personal data online in the EU (WP 43) should be taken into account as they provide clear guidance.

In the context of providing information to children, special emphasis should be put on giving layered notices based on the use of simple, concise and educational language that can be easily understood. A shorter notice should contain the basic information to be provided when collecting personal data either directly from the data subject or from a third party (Article 10 and 11). This should be accompanied by a more detailed notice, perhaps via a hyperlink, where all the relevant details are provided. As the Working Party has noted in its recommendation about online data processing, it is fundamental for the notices to be posted at the right place and time – i.e. they should be shown directly on the screen, prior to collecting the information. As well as being a requirement under the Directive, this is especially important as a tool to raise children's awareness of the possible risks and dangers arising out of online activities. Indeed, it might be argued that in the online environment, unlike in the real world, this is the only opportunity for children to be apprised of such dangers.

d.2) Right of access

The right of access is normally exercised by the representative of the child, but always in the interest of the child. Depending on the degree of maturity of the child, it can be exercised in his/her place or together with him/her. In some cases the child may also be entitled to exercise his/her rights alone.

When very personal rights are concerned (as for instance in the health field), children could even ask their doctors not to divulge their medical data to their representatives.

This might be the case if a teenager has given sexual data to a physician or a help line explicitly excluding the representatives from such information.

It might also be the case if the child does not trust his or her representatives and contacts the youth welfare service, for example, when consuming drugs, or feeling suicidal.

The question arises whether representatives may have access to such details, and whether the child may object. To assess whether the children's right to privacy prevails over the representatives' right to access, the interests of all parties involved have to be carefully balanced. In this balancing exercise, the best interest of the child is of special importance.

In the case of access to medical data, the appreciation of the practitioner might be relevant to assess the opportunity of access by the representatives.

National practice gives useful illustrations as well: in the United Kingdom, for example, teenagers above 12 are entitled to exercise their right of access alone.

In several countries, the right of access of representatives to the data of their teenager daughters is limited in cases of abortion.

As a general comment, the criteria for the conditions of access will be not only the age of the child, but also whether or not the data concerned were provided by the parents or by the child – which is also an indication of his/her degree of maturity and autonomy.

d.3) Right to object

Art 14 a) states that the data subject has the right to object the processing – at least in cases referred to in Art 7 e) and f) – on compelling legitimate grounds. These grounds can be particularly compelling when they concern children. It should also be recalled that data subjects are entitled in any case to object to the processing of their data for direct marketing purposes (Art. 14 b)).

III – At school

In this following section, the opinion will illustrate how the fundamental principles recalled above can be specified with regard to the school context. Indeed, the life of a child develops as much at school as within the family, so it is natural that several data protection questions arise in connection with the school life of children. These are questions of a varied nature, and raise correspondingly different problems.

1) – Student files

a) Information

Data protection questions relating to children (and also, sometimes, their families) can arise in connection with student files as early as at their enrolment at school. Indeed, there are countries where legislation permits school authorities to require forms, containing personal data, to be completed for the purpose of creating student files, computerised or others.

On forms such as these the data subjects should be informed that their personal data will be collected, processed, and for what purpose, who are the controllers, and how the rights of access and correction can be exercised. They must also be informed, when applicable, as to whom these data may be disclosed.

b) Proportionality

The data required must not be excessive: e.g. data about academic degrees of parents, their profession or labour situation are not always necessary. Data controllers must consider whether they are really needed. Special care should be taken because this information can be the cause of discrimination.

c) Non – discrimination

Some of the data contained in these forms can possibly cause discrimination, for example, data relating to race, immigrant status, or suffering from certain disabilities.

This information is usually collected to make sure that the school is aware of, and devotes the necessary attention to, pupils with cultural (for example, linguistic) or economic difficulties.

The principles of best interest and the purpose limitation principle should be the criteria in the processing of such information.

A very strict perspective must namely be applied in what concerns the registration of the religion of pupils; this can only be accepted when the nature (religious school) and administrative purposes justify it, and only to the extent strictly necessary. No superfluous deduction on the religion of the pupil should be drawn where data are only needed for administrative purposes (e.g. following a course on religion, indicating meal preference).

Information on the wealth and income of a child's family can also be a source of discrimination, but may be processed in the child's own interest, for instance, if the representatives ask for grants or reductions in school fees.

All data that might lead to discrimination must be protected by proper security measures, such as processing in separate files, by qualified and designated people, subject to professional secrecy, and other appropriate measures.

The consent to the processing of all data that can cause discrimination must be clear and unambiguous.

d) Principle of finality

d.1) Communication of data

There are cases where school authorities provide the names and addresses of their pupils to third parties, very often for marketing objectives.

This happens, for instance, when data are sent to banks or insurance companies which want to attract the pupils as their clients, or when student data are communicated to the local elected representatives. This constitutes a breach of the finality principle, as data intended for school aims are being used for incompatible purposes.

In accordance with Art. 6. 1) b) of Directive 95/46, children's data cannot be used for purposes incompatible with the one that justified their collection.

The issue here is not the problem of children being the addressees of marketing; this is a consumer protection problem. What is at stake is the prior collection of personal data, in order to send the data subjects marketing messages later. Such processing should always be subject to the prior consent of the representatives (and of the children, depending of their maturity).

In any case in which a marketing operation was considered as being legitimate and compatible, such processing should always be done in the least intrusive way.

In addition to the conditions mentioned above, if data of parents and/or pupils are requested by a third party for marketing purposes, their transmission should always be subject to the prior information and consent of the representatives (and of the children, depending of their maturity).

d.2) Access to data

The data contained in the student file must be subject to rigorous confidentiality, in accordance with the general principle of Directive 95/46/EC, Art 16.

The processing of data of a special nature must be subject to particular security requirements.

The following are examples of such kinds of data:

- Disciplinary proceedings
- Recording of violence cases
- Medical treatment in school
- School orientation
- Special education of disabled people
- Social aid to poor pupils

Access to data should be given to the representatives of the pupils (and to the pupils themselves, if they are already mature). Such an access must be strictly regulated, and limited to school authorities, school inspectors, health personnel and law enforcement bodies.

d.3) School results

Different countries have different traditions with regard to the publication of school results. There are countries with long established traditions of publishing results.

The purpose of this system is to allow comparison of results and facilitate possible complaints or recourse.

In other countries, even results are subject to the general rule of confidentiality applicable to data in the student file. In these cases, results can be disclosed to the representatives of the pupils exercising their right of access.

In any case, school results should be published only when necessary, and only after informing pupils and their representatives of the purpose of publishing, and their right to object.

A special problem concerns the publication of school results on the internet, which is a convenient way of communicating them to the interested persons. The risks inherent in this mode of communication demand that access to the data should only be possible with special safeguards. This might be achieved by using a secure website, or personal passwords assigned to the representatives or, when they are already mature, to the children.

The modalities of the right of access will be different, depending on the degree of maturity of the child. It is likely that in primary school, access will be exercised mostly by representatives, while in secondary school students will also be able to access the data by themselves.

d.4) Retention and elimination

The general principle whereby no data should be kept for longer than is necessary for the purpose for which it has been collected is applicable to this context as well. Therefore, careful consideration should be given as to which data from school files should be kept, either for educational or professional reasons, and which should be erased, for example, those concerning disciplinary procedures and sanctions.

2) – School life

Data protection questions emerge in connection with daily school life, in the following areas.

a) Biometric data – access to the school and canteen

Over the years, there has been an increase in access control to schools, for obvious reasons of safety. This access control involves collecting, at entry, biometric data such as fingerprints, iris, or hand contours. In certain situations such means may be disproportionate to the goal, producing an effect which is too intrusive.

In any case, the proportionality principle should be applied to the use of these biometric means as well.

It is strongly recommended that legal representatives have available to them a simple means of objecting to the use of their children's biometric data. If their right to object is exercised, their children should be given a card or other means to access the school premises concerned.

b) Closed Circuit Television (CCTV)

There is an increasing tendency to use CCTV in schools for security reasons. There is no recommended solution valid for all aspects of school life and for all parts of schools.

The capacity of CCTV to affect personal freedoms means that its installation in schools requires special care. This means that it should only be installed when necessary, and if other less intrusive means of achieving the same purpose are not available. The decision to install a CCTV system should be preceded by a thorough discussion between teachers, parents and pupils' representatives, taking into account the stated aims of the installation and the adequacy of the proposed systems.

There are places where safety is of paramount importance, so CCTV can be more easily justified, for example, at entrances and exits to schools, as well as to other places where people circulate - not just the school population, but also people visiting the school premises for whatever reason.

The choice of location of CCTV cameras should always be relevant, adequate and non-excessive in relation to the purpose of the processing. For instance, in some countries, the use of CCTV cameras outside of the school hours was considered as adequate regarding data protection principles.

On the other hand, in most other parts of the school, the pupils' right to privacy (as well as that of teachers and other school workers), and the essential freedom of teaching, weigh against the need for permanent CCTV surveillance.

This is so particularly in classrooms, where video surveillance can interfere not only with students' freedom of learning and of speech, but also with the freedom of teaching. The same applies to leisure areas, gymnasiums and dressing rooms, where surveillance can interfere with rights to privacy.

These remarks are also based on the right to the development of the personality, which all children have. Indeed, their developing conception of their own freedom can become compromised if they assume from an early age that it is normal to be monitored by CCTV. This is all the more true if webcams or similar devices are used for distance monitoring of children during school time.

In any case where CCTV is justified, the children, the rest of the school population, and representatives must all be informed of the existence of surveillance, its controller, and its aims. The information intended for children should be appropriate to their level of understanding.

The justification and the relevance of the CCTV system should be reviewed regularly by the school authorities to decide whether or not it should be maintained. The representatives of the children should be informed accordingly.

c) Health conditions

Data about pupils' health conditions are sensitive data. For this reason, their processing must strictly adhere to the principles of Article 8 of the Directive. Such data should only be processed by doctors, or those who directly "take care" of the pupils, such as teachers and other school personnel bound by professional secrecy ethics.

The processing of data of this kind depends either on the consent of the representatives of the children or on vital interests in emergency cases connected with school or educational life.

d) School websites

A growing number of schools create websites targeted at students/pupils and their families, and those websites become the main tool for external communications. Schools should be aware that disseminating personal information warrants more stringent observance of fundamental data protection principles, in particular data minimisation and proportionality; additionally, it is recommended that restricted access mechanisms are implemented with a view to safeguarding the personal information in question (e.g. login via user ID and password).

e) Children's photos

Schools are often tempted to publish (in the press or on the internet) photos of their pupils. Special attention should be drawn to the publishing by schools of photos of their pupils on the internet. An evaluation should always be made of the kind of photo, the relevance of posting it, and its intended purpose. Children and their representatives should be made aware of the publication, and prior consent from the representative (or the child, if already mature) should be obtained.

Derogations are acceptable in the case of collective photos, namely of school events, if, by nature, they do not permit easy identification of pupils.

f) Pupil's cards

For the control of access and the monitoring of purchases: Many schools are utilising pupils' cards not only to control access to the school, but also to monitor the purchases made by the children. It is questionable if the second purpose is completely compatible with the privacy of the child, especially after a certain age.

In any case, the two functions should be separated, as the second may raise privacy issues.

For the location of pupils[11]: Another means of control used in certain schools (whether with a card or not) is the location of pupils through RFID badges. In this case, the

[11] See WP 115 (adopted on November 25, 2005) on the principles relating to the localization of minors.

relevance of such a system must be justified with regards to the specific risks at stake, particularly where alternative methods for control are available.

g) Videophones in schools

Schools can play a crucial role in setting out precautions for the use of MMS, audio and video recording where personal data referring to third parties are involved, without the data subjects' being aware of it. Schools should warn their students that unrestrained circulation of video recordings, audio recordings and digital pictures can result in serious infringements of the data subjects' right to privacy and personal data protection.

3) – School statistics and other studies

In most cases, personal data are not needed to obtain statistics (nevertheless, it can happen in exceptional cases; for instance: when statistics are made on professional integration).

According to Art. 6 e) of the Directive, statistical results should not lead to any identification of data subjects, be it direct or indirect.

Studies are often conducted that use various personal data about pupils, obtained from more or less detailed questionnaires. The collection of this data should be authorised by the representatives (in particular if it is sensitive data), and the representatives should be informed of the purpose and the recipients of the study.

Furthermore, whenever it is possible to develop studies without identifying the children, that procedure should be followed.

IV – Conclusion

1) Law

This opinion shows that the provisions set out in the current legal framework, in most cases, effectively ensure the protection of children's data.

A prerequisite for effective protection of children's privacy is, however, that the provisions are applied in accordance with regard for the principle of the child's best interest. The application must take into account the specific situations of minors, and those of their representatives. Directives 95/46/EC and 2002/58/EC should be interpreted and applied accordingly.

In cases of conflicting interests, a solution can be sought by interpreting the Directives in accordance with the general principles of the UN Convention on the Rights of the Child, namely, the best interest of the child, and also by reference to the other legal instruments already mentioned.

Member States are encouraged to bring their laws into line with the above-mentioned interpretation by taking the necessary measures. Also, at Community level,

recommendations or other appropriate instruments dealing with this subject would be welcomed.

As stated earlier, this opinion contains only the general principles of privacy and data protection as relevant to children's data, and their application to the important field of education. Other specific areas could warrant separate study by this Working Party in the future.

2) Practice

This opinion sets out the general concerns and considerations when looking at data protection and privacy issues related to children. The Working Party has chosen the field of education as a first step to address this issue due to the importance of education in society. As can be seen, 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 the consequences of giving out personal data if not necessary.

If our societies are to strive for true culture of data protection in particular, and 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, the school 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 later 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 plans, according to the age of the pupils and the nature of the subjects taught.

It should never be the case that, for reasons of security, children are confronted with over-surveillance that would reduce their autonomy. In this context, a balance has to be found between the protection of the intimacy and privacy of children and their security.

Legislators, political leaders and educational organisations should, in their respective areas of competence, take effective measures to address these issues.

The role of data protection authorities is four-fold: to educate and inform, especially children and authorities responsible for the well-being of young people; to influence policy makers to make the right decisions as regards children and privacy; to make controllers aware of their duties; and to use their powers against those who disregard legislation or do not adhere to codes of conduct or best practice in this area.

An effective strategy, in this context, can be the formulation of agreements between DPAs, Ministries of Education and other responsible bodies, defining clear and practical terms of mutual cooperation in this area to foster the notion that data protection is a fundamental right.

Children should be made aware, in particular, that they themselves must be the primary protectors of their personal data. This is an area where the effectiveness of empowerment can be demonstrated.

Public consultation

The Article 29 Working Party invites those who handle children's personal data, especially teachers and school authorities, as well as the general public to comment on this Working Document.[12]

Done at Brussels, on 18 February 2008

For the Working Party
The Chairman
Peter SCHAAR

[12] Comments to this Working Document should be sent to: Article 29 Working Party - Secretariat - European Commission, Directorate-General Justice, Freedom and Security
Unit C.5 – Protection of personal data
Office: LX 46 06/80
B – 1049 Brussels
E-mail: Amanda.JOYCE-VENNARD@ec.europa.eu and to Kalliopi.Mathioudaki-Kotsomyti@ec.europa.eu;
Fax: +32-2-299 80 94

All comments from both public and private sectors will be published on the Article 29 Working Party's internet site unless respondents explicitly state that they wish to keep particular information confidential.