Protecting Vulnerable Data Subjects: Findings from a Survey of EU Data Protection Officials on the Use of Cloud Services in Organisations

A SafeGov.org Report

Table of Contents

Author: Jeff Gould (jeff.gould@safegov.org)

Publication date: September 23, 2013

Media inquiries: Kate Tellier (kate.tellier@safegov.org or +32 479908727)

Executive Summary

The use of commercial cloud services by public organisations in Europe is growing. While the benefits of cloud computing are indisputable, the public sector contains certain particularly sensitive or vulnerable user populations whose privacy requires special protection. Critical examples include civil servants employed by local or national governments and – the subject of particular emphasis in this report – children in schools[1].

The most widely used cloud services today are typically free or very inexpensive offerings designed as vehicles for online behavioural advertising aimed at individual consumers. SafeGov.org is concerned that by repurposing such advertising-driven services for users within organisations, cloud providers may deliberately or inadvertently expose these data subjects to online advertising, profiling or other forms of personal information processing that violate their rights under EU data protection laws. The risk is particularly acute in the absence of constraints on the contractual relations between data processors and data controllers that ensure the rights to information and consent of the data subjects in these organisational contexts.

In order to address this issue, SafeGov.org has undertaken a major research project to identify and analyse the privacy risks these data subjects face and to review possible solutions in the framework of European data protection legislation. In developing our views we conducted in-depth interviews with over a dozen representatives of European Data Protection Authorities (DPAs) as well as a number of European Commission officials involved in the development of data protection policy. We found wide support for the idea that vulnerable data subjects such as school children deserve special protection. We also found significant support for the idea that codes of conduct – as provided for in both the 1995 Data Protection Directive and the proposed General Data Protection Regulation (GDPR) – are an appropriate mechanism for providing such protection.

We note the considerable debate and disagreement around the draft GDPR. We strongly endorse the EU's ambitious and necessary effort to harmonise and modernise its data protection legislation, while recognising that the final form of this legislation remains at present uncertain. Nonetheless, we believe that whatever the final shape of the Regulation, existing disagreements should not overshadow the urgent measures that Europe must take to protect the online privacy of vulnerable public sector users.

In this paper, we focus on the protection of children using modern commercial cloud services in schools, though we believe our approach is applicable for other public sector user populations. Our extensive survey research into the use of cloud services by schools in Europe and other regions of the world[2] confirms that school authorities and parents clearly understand the powerful benefits

[1] We here define "public sector" in a broad sense to include schools of all kinds, both state-sponsored and private.

[2] See results from the SafeGov global series of surveys of cloud use in schools:
"SafeGov 2012 National Data Privacy in Schools Survey"
(www.safegov.org/media/43502/brunswick_edu_data_privacy_report_jan_2013.pdf)
"UK School Opinions of Cloud Services and Student Privacy"
(www.safegov.org/media/48269/safegov_ponemon_uk_school_survey.pdf)

that these technologies offer, while recognising the need for strong privacy safeguards. Our interviews with European data protection officials suggest that a consensus exists at least in broad outline that a regulatory approach based on codes of conduct can provide such safeguards. These dual findings are highly encouraging, and bode well for the future of safe and effective use of cloud computing in European schools.

On the basis of this research, we address the following Calls to Action to European data protection officials, schools and school authorities, parent associations and the cloud providers themselves:

- DPAs, the Commission, national education ministries, schools and parent associations must recognise that while free commercial cloud services provide great benefits to schools, they must be carefully regulated in order to prevent violations of data protection rights or the introduction of advertising into schools.
- DPAs, the Commission, national education ministries, schools and parent associations should embrace Codes of Conduct at the national level and possibly also at the EU level as a mechanism for insuring the data protection rights of school children. This framework could also be applied to other sensitive user populations of cloud services in public sector organisations, such as civil servants.
- DPAs should extend the current focus of their investigations of the consumer privacy policies of large Internet firms to address the specific scenario of data subjects who use cloud services in a collective context where the organisation serves as the data controller interacting with an outside data processor.
- All cloud service providers should review their privacy policies and associated practices and revise them as necessary to meet the standards of school online privacy discussed in this report, namely including a legally binding pledge not to conduct user profiling or data mining for advertising purposes under any circumstances when providing services to schools.

"Australian Parents' Views of Cloud Services and Online Privacy in Schools" (http://safegov.org/media/49377/safegov-australian-parents-survey.pdf).

Cloud Services Threaten the Privacy of Vulnerable Data Subjects

European officials have long recognised the profound impact that the Internet and the many applications it enables have on economic growth and innovation. The online services commonly referred to as "cloud computing" are the latest generation of these applications. They differ from previous generations not in their fundamental nature, but in their lower cost, their greater ease of use and their vastly simplified management process. The European Commission's September 2012 Communication to the Parliament and the Council entitled "Unleashing the Potential of Cloud Computing in Europe" offers a concise definition of these services:

- "Cloud computing" in simplified terms can be understood as the storing, processing and use of data on remotely located computers accessed over the internet. This means that users can command almost unlimited computing power on demand, that they do not have to make major capital investments to fulfil their needs and that they can get to their data from anywhere with an internet connection. Cloud computing has the potential to slash users' IT expenditure and to enable many new services to be developed.[3]

While almost any kind of computing application can be provided from "the cloud", the most widely used examples are web services such as email, social networking and online content creation. Many of the most popular of these applications began life as advertising-supported services provided to individual consumers at no cost. However, in recent years they have increasingly been adopted by companies, governments, schools, and healthcare providers as less expensive, more flexible alternatives to traditional enterprise IT systems. As we shall see, the use of cloud computing by organisations creates specific risks for the data subjects who belong to these organisations (employees, civil servants, schoolchildren, patients) – risks that are different and more serious than those encountered by ordinary consumers who use cloud services.

In this report we do not consider the whole range of cloud offerings, but focus only on email, document creation and online collaboration, because these are the services that are currently the most widely used by the user populations we are concerned with[4]. There are many indications that significant numbers of schools and public organisations in Europe are adopting these new cloud services, motivated by their ease of use, ease of deployment, and low (in some cases zero) cost. For example, a recent survey conducted for SafeGov.org by the Ponemon Institute reveals that 68% of UK schools are already using cloud services or expect to adopt them in the foreseeable future[5].

While the sophisticated consumer-grade cloud services such as email, online content creation and collaboration that several commercial cloud providers are now offering at no cost to European schools indisputably bring many educational benefits, they also carry important privacy risks that

[3] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf
[4] The most widely used cloud service that we do not consider here is infrastructure as a service (IaaS), which is the provision over the Internet of on-demand access to basic computing resources such as virtualised servers and storage.
[5] http://www.safegov.org/media/48269/safegov_ponemon_uk_school_survey.pdf

school officials and parents often fail to measure. These risks are especially acute for services that were originally designed as vehicles for online behavioural advertising and have been subsequently adapted for use in schools. Such repurposed services sometimes fail to establish a clearly demarcated frontier between technical infrastructure and user interfaces created for consumer advertising and an online environment appropriate for schoolchildren.

There are a number of areas where advertising-oriented cloud services may jeopardise the privacy of data subjects in schools, even when ad-serving is nominally disabled. Threats to student online privacy occasioned by the use of such services in the school environment include the following:

- **Lack of privacy policies suitable for schools:** By failing to adopt privacy policies specifically crafted to the needs of schools, cloud providers may deliberately or inadvertently force schools to accept policies or terms of service that authorise user profiling and online behavioural advertising.
- **Blurred mechanisms for user consent:** Some cloud privacy policies, even though based on contractual relationships between cloud providers and schools, stipulate that individual data subjects (students) are also bound by these policies, even when these subjects have not had the opportunity to grant or withhold their consent.
- **Potential for commercial data mining:** When school cloud services derive from ad-supported consumer services that rely on powerful user profiling and tracking algorithms, it may be technically difficult for the cloud provider to turn off these functions even when ads are not being served.
- **User interfaces that don't separate ad-free and ad-based services:** By failing to create interfaces that distinguish clearly between ad-based and ad-free services, cloud providers may lure school children into moving unwittingly from ad-free services intended for school use (such as email or online collaboration) to consumer ad-driven services that engage in highly intrusive processing of personal information (such as online video, social networking or even basic search).
- **Contracts that don't guarantee ad-free services**: By using ambiguously worded contracts and including the option to serve ads in their services, some cloud providers leave the door open to future imposition of online advertising as a condition for allowing schools to continue receiving cloud services for free.

With Europe clearly at the start of a broad wave of cloud adoption by schools, it is critically important to focus early in this process on these vital questions of privacy and data protection for users in schools.

Findings from Interviews with European Data Protection Officials

The findings and recommendations in this report are based on extensive interviews conducted by SafeGov.org with European data protection officials, including over a dozen representatives of Data Protection Authorities (DPAs) as well as senior representatives of the European Commission. The interviews were conducted in April and May of 2013 under a promise of anonymity and typically lasted one hour or more. Although the conversations covered a broad range of topics relating to data protection in Europe, the focus was on two key questions:

- Do vulnerable populations of data subjects, such as school children, require more protection when using cloud services than individual consumers?
- If so, what mechanisms in current and future European data protection legislation might provide such additional protection?

To summarise the results of our interviews, we found broad support for our initial view that vulnerable data subjects such as school children do in fact require extra protection. When we canvassed data protection officials for suggestions as to possible mechanisms for providing this protection, we also found that the majority endorsed the use of codes of conduct for this purpose[6]. As the interviews progressed, a clear picture emerged of the potential of such codes to mitigate the extra privacy risks that users face when they use cloud services as members of an organisation.

Findings on the Rights of Data Subjects in Organisations

The issue of the rights of data subjects inside an organisation that acts as a data controller has already been raised by European DPAs in the context of their ongoing investigation of Google's privacy policy. Specifically, the French DPA (CNIL[7]), acting on behalf of the Article 29 Working Party[8], has found that a data controller does not necessarily have the capacity to consent on behalf of its data subjects to the processing of their personal information by an outside cloud provider[9]. Although the CNIL's conclusion concerned one specific cloud service (Google Apps), the underlying

[6] Support for codes of conduct was broad but not unanimous. A minority of member-state DPAs expressed skepticism about the efficacy of voluntary codes and indicated a preference for mandatory legislation to govern the behaviour of cloud service providers in a school environment. However, these officials generally attributed their views to the specific historical experience of their countries and acknowledged that in the broader EU context such codes could be effective.

[7] Commission nationale de l'informatique et des libertés.

[8] The Article 29 Working Party consists of the member state DPAs, the European Data Protection Supervisor, and the European Commission. The group has an important advisory role and has been influential in shaping the interpretation and evolution of EU data protection law, but under the 1995 Directive all enforcement powers remain in the hands of the national DPAs.

[9] "For Google Apps end-users, the use of a Google Account is decided by the Google Apps customer (typically the company that employs the end-users): consent may therefore not be valid." CNIL, "Google Privacy Policy: Main Findings and Recommendations", October 16, 2012 (www.ip-rs.si/fileadmin/user_upload/Pdf/Article_29_WP/Google_Privacy_Policy_-_recommendations.pdf).

principle is clearly valid for the general case of any organisational data controller that contracts for the provision of cloud services to its data subjects. We believe that this principle is of fundamental importance and deserves much more attention from DPAs and the Commission as well as from data controllers and data subjects themselves than it has hitherto received.

A fundamental question that arises when schools adopt cloud services that process users' personal information is whether the students and their parents have been given an adequate opportunity to provide or withhold their informed consent. We found broad agreement that such informed consent is required under both the 1995 Data Protection Directive and the proposed draft of the GDPR. One official summarised the issue as follows:

- "There's a distinction to be made between sensitive user populations as data subjects (e.g. a school using a cloud service to process its pupils' data) and sensitive user populations as consumers of cloud services (e.g. a cloud-based gaming environment that specifically caters to children). In the former situation (sensitive user populations as data subjects), it's the data controller's responsibility to ensure compliance, and also to perform a prior risk analysis in order to establish that, for their specific data processing and their specific data subjects, the cloud service under consideration is a viable option and any risks to the data subjects are acceptable. In the latter situation (sensitive user populations as consumers of cloud services), it's up to the provider of the service to ensure compliance and to perform a prior risk analysis in order to offer the service in such a way that there are no unacceptable risks to the data subjects." (DPA 1)

A clear distinction must thus be made between situations where the responsibility for ensuring that the data subject's rights are protected falls chiefly on the data processor (consumer markets) and those where it falls on the data controller (organisational markets). The underlying principle at work here is the requirement for a risk-based approach that selects different degrees and kinds of protection according to different degrees and kinds of risk.

Findings on Codes of Conduct

Once the risk-based approach is embraced, the next question that naturally arises is what mechanisms are flexible enough to provide the different kinds and degrees of protection required by populations with distinct risk profiles. Identifying an adequate answer to this question is not simple. The seemingly obvious solution of requiring the data controller (school or employer) to seek the consent of its data subject members may in fact be unacceptable, because the imbalance of power between controller and subjects makes it inequitable. Can a family be said to have "freely" consented to the processing of a student's personal information by an outside cloud provider when the school that has contracted with this provider essentially tells the family it has no alternative? This problem was clearly identified by a data protection official we spoke to:

- "We believe that tracking and profiling for such purposes as online behavioural advertising require explicit consent. However, in the case of users in dependent relations (e.g. employees, students) we see only limited space for user consent. Consent must be based on free choice, but such a dependent situation usually is contrary to exerting such choice." (DPA 2)

What is needed therefore is a mechanism that constrains the actions of the data controller and in particular the choices it is permitted to make when contracting with outside cloud service providers. As we have suggested, codes of conduct are one such mechanism. Many officials told us that such codes are well suited to provide the specific protections required by vulnerable user populations. DPAs specifically endorsed the potential value of codes of conduct for protecting children from online advertising:

- "Specific codes of conduct or separate privacy policies may contribute to the protection of the personal data of users in sensitive populations. For instance, a specific code of conduct might be a useful approach to regulating advertising to children." (DPA 1)

Under existing and proposed EU data protection law, a code of conduct is a set of rules that a data controller or data processor voluntarily agrees to apply to itself, in exchange for an implied or explicit assurance from regulators that by so doing it will be considered to have fulfilled basic requirements for due diligence. Indeed, the fundamental value of a code of conduct is to provide a degree of assurance to all participants in the process – the data subjects, the data controller, and the data processor – that the subjects' privacy rights have been adequately protected.

Existing EU legislation is extremely flexible with regard to the ways in which codes of conduct may be developed and submitted for approval. A senior EC official explained the basic procedures as follows:

- "Both the Regulation and the 1995 Directive call for data protection measures to be linked to the risks. So on a case by case basis you may need additional protection, but the text of the Regulation won't specify the details of those measures. More risk needs more protection, but the Regulation will leave it to codes of conduct that may be developed by specific sectors or jointly with DPAs or then blessed by DPAs or perhaps the Commission (the final text of the Regulation on this point is still a matter for debate). The current Directive says that codes of conduct can be developed by a sector and then go to the national DPA which approves or disapproves for that one country. But it's also possible under the current Directive to go to the Article 29 Working Party. This has only happened a few times so far, but it could happen more often under the Regulation." (Senior EC Official A)

Several DPAs made the important observation that codes of conduct governing the relationship between cloud providers, data controllers and data subjects could be developed in two quite different ways. In the first case ("Option 1"), codes would be adopted as self-regulatory mechanisms by the cloud providers themselves (the data processors), committing them to follow certain standards in the provision of cloud services to vulnerable user populations.

- "Codes of conduct may be especially useful at the level of the controller-processor relationship, where the choice of the cloud provider is the responsibility of the customer who is the controller, who should choose a cloud provider that implements best practices. If the controller can choose between a provider who offers compliance with a code of conduct and another who does not, that could be an element of choice." (DPA 3)

In the second case ("Option 2"), codes of conduct would be defined by the data controllers themselves, for example by schools acting either on a national or EU basis, and would set minimum requirements for contracts with cloud providers.

- "Codes of conduct to protect schools are a good idea. The formal position of the EU is that the school is the controller, so they are responsible. But in practice there will be pressure on DPAs to come up with criteria that a school or university could use to say that they have done their due diligence on the cloud provider, e.g. they respect certain standards. We understand that schools won't have the capacity to deal with a Microsoft or a Google, so DPAs will be under pressure to come up with codes of practice. DPAs will be reluctant to say this or that cloud provider is approved. But DPAs can approve certain codes of conduct or third-party certifications." (DPA 4)

A concern about industry-sponsored codes of conduct (Option 1) is that the imbalance in bargaining power between large multinational cloud providers and small data controllers such as schools could result in policies that are unfair or ineffective:

- "Maybe small data controllers like schools won't have enough power to negotiate with the likes of Google, so codes of conduct might not work. It may be preferable to have written contracts and binding legal documents." (DPA 5)

However, while legislation may be an appropriate avenue to pursue in some member states, codes of conduct defined and adopted by schools themselves could do much to alleviate concerns about the imbalance of power between processors and controllers. This is particularly so if the codes win the support of DPAs, national education authorities and interested third parties such as parent groups and privacy advocates. We note that both the Commission and the Council of Ministers have expressly endorsed the use of codes of conduct in such contexts:

- "Because of the power disparity between large multinational processors and small controllers such as schools, it can be reasonably expected that DPAs will address this issue. The Ministers have directed that these codes of practice be incentivised." (DPA 4)

DPAs also underscored the fact that significant cultural variations exist in Europe regarding the concept of privacy. These variations naturally influence the view that different countries have of codes of conduct.

- "Privacy is something that is a cultural good, it's a very sensitive matter that can't be easily measured." (DPA 6)

However, even skeptics acknowledge that the harmonisation implied by the GDPR could pave the way to broader use of codes of conduct:

- "Codes of conduct are more an English way of thinking, but their use will increase in the future." (DPA 7)

Several respondents observed that it would be legally possible under the draft GDPR to establish codes of conduct on a European level by submitting them for validation to the Commission or the proposed European Data Protection Board (successor to the Article 29 Working Party). But many also noted that education remains largely a national matter subject to diverse rules and customs, and that national codes of conduct approved by the local DPAs would be more likely to succeed.

- "It would be difficult to have codes of conduct for schools other than on a national basis, because school systems are so different, it's still a national thing." (DPA 8)

Crucially, the DPAs reminded us that a code of conduct would have to be approved not only by the processor and the controller, but also by the relevant national DPAs and ideally – rejoining here the key concept of consent – by the data subjects themselves:

- "Codes of conduct are always a good idea, but they need to be agreed not only by the data controller but by all the different actors of the processing, e.g. the DPAs, the data subjects themselves such as students and others who play a role in the processing. And this agreement needs to be approved by a DPA." (DPA 9)

Findings on the Importance of Data Subject Consent in Organisations

The next issue to explore is the nature of user consent required when cloud services process personal information. According to European data protection law, profiling of users for commercial purposes requires explicit consent. A senior EC official framed the issue as follows:

- "If data have been collected for certain purposes, what about secondary purposes, are they compatible? If it's for statistical analysis then compatibility is much easier, but if it is truly to get as close as possible to the individual and is going to impact on that individual's life, then please face reality that this is probably subject to many more safeguards and in the end may well require very specific consent." (Senior EC Official B)

This view echoes the conclusions of the recent Article 29 Working Party paper on purpose limitation:

- "When an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers […] free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible. Importantly, such consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research."[10]

One prominent issue in the debate over the draft GDPR has been the choice between the notions of "unambiguous" and "explicit" consent. The former, present in the 1995 Directive, is a weaker type of consent that may often be implicit. A common example of implicit consent is when a consumer clicks through the log-on page of a web service containing a link to a lengthy and complex privacy policy that the user hasn't studied carefully or perhaps hasn't even read at all. The change from "unambiguous" to "explicit" proposed by the draft GDPR introduces a kind of consent that is clearly stronger, because it removes the possibility that consent can be purely implicit. The statement by the Article 29 Working Party cited above suggests that even under the 1995 Directive certain kinds of personal information processing, such as that required for behavioural advertising, do in fact require explicit rather than merely unambiguous consent. However this view is unpopular in certain circles and has been lobbied against by a number of large Internet advertising firms.

[10] Article 29 Working Party "Opinion on Purpose Limitation", April 2, 2013 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf).

Even in the case of cloud providers that engage in profiling and tracking of individual consumers for purposes of behavioural advertising, some argue that when consumers continue to use a service after having been informed that the provider is profiling them, they can be assumed to have consented to this processing. The argument is reinforced when the service is a sophisticated web application such as email or online document creation that would have to be paid for in an enterprise environment but is offered free to consumers. The "user profiling in exchange for free services" business model is arguably the foundation of the modern consumer web, and European data protection officials are understandably reluctant to embrace regulatory principles that might make such a model unworkable. One official observed that the requirement for "explicit" consent, when properly understood, does not jeopardise this model:

- "Adding the word 'explicit' on consent won't mess up business models. People say that requiring explicit consent will mean that they will have to ask for explicit consent for every operation. But that's not the case… All we're saying is that you need consent in the same places as before but now it has to be made explicit. This has been presented as cataclysmic revolution, but it's not. It doesn't affect businesses destructively as it's sometimes presented." (Senior EC Official C)

Some legal scholars have challenged the idea that using a free web service which comes with the implicit assumption of profiling should be treated as a simple economic transaction. According to modern theories of behavioural economics and transaction costs, consumers cannot be assumed to be perfectly rational actors, but must operate under certain cognitive constraints that make it difficult for them to understand particularly complex transactions, and therefore require additional regulatory protection[11].

We do not wish to take sides on the question of how targeted online consumer advertising should be regulated or on the broader debate over the many amendments that have been proposed to the draft GDPR. We observe simply that those who endorse a risk-based approach must logically acknowledge that both forms of consent – unambiguous or explicit – can be appropriate in certain circumstances. The question of which one should apply in a given case must depend on the kind and degree of risk present. It is very difficult to formulate the choice in general terms, because there is an almost infinite variety in the possible relationships and associated balance of power among data processors, data controllers, and data subjects, as well as in the degree of vulnerability of the latter.

Children who use a cloud service contracted for by their school face a double imbalance of power: on the one hand between the data subject and the organisation serving as the data controller (the students may have little real option but to use the cloud service that has been selected by their school), and on the other hand between the data controller and the processor (the school by itself has little ability to influence the business model or contractual terms of a large multinational Internet firm). Moreover, if the cloud service chosen by the school derives from a consumer service whose business model is user profiling and behavioural advertising, it is legitimate to ask if such practices will carry over from the consumer market to the school environment. Whether the school children are actually profiled or targeted with advertising are questions that must be answered on the basis of factual investigation. But the risks are undeniably real and must be accounted for in the regulatory framework that governs the use of cloud services in such situations. This is why we

[11] Whittington and Hoofnagle, "Unpacking Privacy's Price", North Carolina Law Review, May 2012 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2059154).

believe that some form of consent by data subjects (school children and their parents) is an essential requirement for the safe use of commercial cloud services in schools and, by extension, other public sector institutions where a significant imbalance of power exists between data processors, controllers, and subjects.

A clear conclusion from the findings is that schools and other institutions that act as data controllers must agree to abide by certain rules when they contract with commercial cloud service providers. As we have suggested, codes of conduct are an appropriate mechanism for defining such rules. As observed by a respondent:

- "Data controllers must abide by the law. If they want to use a service from a processor this must be stipulated in a contract. The processor cannot have more power than the instructions of the controller, the processor cannot use the data for their own purposes. This is often a problem with large cloud providers. If a controller accepts certain terms and conditions from a processor, this is not sufficient under the law to protect the controller from the requirements of the law. We have a great imbalance of power between cloud providers and cloud users. This is not something that the users themselves can solve, they need help of third parties. There is a big difference between using cloud as an individual consumer or as a member of an institution such as a school." (DPA 10)

A Proposal for Codes of Conduct for Cloud Procurement in Schools

An effective response to the problem of schoolchildren's online privacy in cloud services must address all of the issues identified in this report. Based on our extensive conversations with European data protection officials and our research into the use of cloud services by schools in Europe and other regions[12], we find strong support for the view that codes of conduct can provide an effective mechanism for implementing such a response. Existing and proposed European data protection legislation allows for considerable flexibility in elaborating such codes. Given the great variety of EU member-state educational systems, this report does not propose a complete draft text for a possible code of conduct to regulate cloud services in European schools. However, we can identify a certain number of general procedural and institutional requirements, as indicated below.

- Codes must be approved at a minimum by the DPA(s) of the member state(s) in which they apply.
- If intended to function across multiple member states, codes can be submitted for validation to the Article 29 Working Party or the future European Data Protection Board.
- Codes of conduct are far more likely to be effective if they have strong support and sponsorship from national, regional or local parent associations, since they represent the children who are the primary data subjects. Indeed, such associations might play a role in defining appropriate content for the codes, in collaboration with school authorities and other concerned parties.
- Considering the imbalance of power between large multinational Internet firms (data processors) and schools acting as data controllers, industry self-regulation is not sufficient when the data subjects are children using commercial cloud services in the school environment[13]. Therefore effective codes of conduct would ideally be adopted by the schools themselves and/or the relevant education authorities (national or local).

Codes of conduct as described here should be understood as a mechanism for helping schools to define their responsibilities in the selection and management of commercial cloud services. For example, they might contain "model clauses" that schools or educational authorities will require cloud providers to include in their contracts. Such model language would thus specify the basic rules governing the permissible terms of service between cloud providers and schools. At a minimum they should include the following "baseline" elements:

- A privacy policy that addresses the concerns of schools and parents by containing a legally binding pledge not to conduct user profiling or data mining for any

[12] See the research cited in footnote 1 above.
[13] This observation does not preclude the relevance of industry self-regulation for other sectors and use scenarios where data subjects are less vulnerable.

advertising-related purposes. Such a policy could be tailored specifically for schools, or it could be a more general policy[14]. Schools and other public sector institutions acting as data controllers and the data subjects who belong to these organisations must not be forced to accept inappropriate consumer privacy policies.

- A clear and explicitly demarcated separation between core ad-free services and non-core ad-based services, both at the level of underlying technical infrastructure (for example, data mining algorithms) and of user interfaces. The latter should not enable access to ad-driven services from the core ad-free services provided for educational purposes.
- Complete disabling of all data mining and ad-targeting functions in cloud services provided to schools. Ad-targeting and data mining should not be allowed even as options in a school environment.
- A contractual pledge that online advertising as well as associated data mining and user profiling methods will not be enabled in the cloud service at any time. Contracts must make explicit that cloud providers who enter the educational market by offering free or subsidised services cannot impose advertising as a condition for establishing or subsequently renewing contracts on such preferential pricing terms[15].

Finally, we suggest that codes of conduct which place strict and explicit constraints on allowable personal information processing by cloud providers may offer a solution to the practical issue of obtaining consent from data subjects. If schools adopt codes of conduct for the procurement of cloud services that require providers to obey simple baseline rules such as those described above, and if children and their families are adequately informed of these rules, DPAs should have sufficient grounds for deeming both the data controllers and the data processors to be in compliance with data protection law.

[14] Some cloud providers have attempted to argue that a ban on data mining of user content by cloud providers could prevent legitimate and beneficial activities such as scanning emails for malware or spam. But appropriate privacy policies and terms of service can easily be structured to permit such protective activities while forbidding other forms of data mining or user content scanning undertaken for commercial purposes.
[15] SafeGov does not endorse or recommend any particular cloud services or brands over others. Our recommendation rather is that all cloud service providers should review their privacy policies and associated practices and revise them as necessary to meet the standards of school online privacy discussed in this report.

Appendix 1: Codes of Conduct in Current and Proposed EU Data Protection Legislation

Codes of Conduct in the 1995 Data Protection Directive

- Article 27
- 1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.
- 2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.
- Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.
- 3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

Codes of Conduct in the draft General Data Protection Regulation

- Article 38
- Codes of conduct
- 1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:
- (a) fair and transparent data processing;
- (b) the collection of data;
- (c) the information of the public and of data subjects;
- (d) requests of data subjects in exercise of their rights;
- (e) information and protection of children;

- (f) transfer of data to third countries or international organisations;
- (g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;
- (h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.
- 2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.
- 3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.
- 4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).
- 5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

Certifications in the Draft General Data Protection Regulation

- Article 39
- 1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.
- 2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.
- 3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Appendix 2: About SafeGov.org

SafeGov.org is an international forum for IT providers and leading industry experts dedicated to promoting trusted and responsible cloud computing solutions for the public sector. By fostering a more comprehensive understanding of cloud technologies, including their benefits, capabilities and limitations, SafeGov.org works to empower public sector users to make well-informed procurement choices from the growing universe of marketplace offerings.

SafeGov.org will:

- Propose solutions, best practices and guidance to ensure that public sector customers can gain the advantages of new cloud offerings while mitigating risk.
- Provide detailed information that governments and public institutions need to make complex decisions about shifting enterprise services to the cloud.
- Provide a comprehensive platform for leading experts and analysts to discuss issues affecting the broader cloud sector.
- Help foster healthy discussions of innovations and advancements in cloud computing by tracking policy developments, news coverage, and expert analysis and research.
- Promote open competition and safe, secure, and responsible IT practices.

The following principles are a foundation for this forum:

- **Data storage and integrity:** Government and other public sector users have the right to know how and where their data is stored and that it is stored without compromising data integrity.
- **Cloud architecture choice:** The right for public sector customers to choose a cloud architecture that best meets their needs.
- **Accurate vendor representations:** The commitment of vendors to clearly and accurately represent their capabilities, costs and ability to conform to public standards and legislation.
- **Security and privacy:** The top priorities for any cloud solution should be to provide maximum security and well-defined privacy policies that reflect the interests of government and other public sector customers.
- **Level playing field:** The need for open competition based on well-defined implementation and procurement policies.

For more information please visit: www.safe.gov.org or contact Jeff Gould at jeff.gould@safegov.org.