APPENDIX H

Broad Jurisdictional Report for the European Union

CONTENTS

Context

This report examines the broad position to date regarding the use of Privacy Impact Assessments (PIAs) or PIA-like processes within the Member States of the European Union/European Economic Area. This does not purport to be an exhaustive examination of the 27 EU Member States; rather it looks at the existing state of play across the EU generally.

It may perhaps come as no surprise to discover that the use of 'Privacy Impact Assessments' has received relatively minor attention within the EU. An academic literature search generates virtually no material in the English language focused on PIAs in EU Member States; a practitioner literature search does no better. There are occasional mentions; suggestions in passing that the EU might formally adopt some form of PIAs; but no sustained or detailed examination of the European 'state of the art' in English.

There, of course, lies one of the stumbling blocks to this assessment: PIAs as a concept have largely been developed in the Anglophone world – with countries such as New Zealand, Australia and Canada taking the lead. This does not, however, mean that other non-Anglophone countries are not engaged in similar exercises, or are not already working to the same ends; rather it may mean that they simply call that process of assessing privacy risks in advance of engaging in new, or re-engineering old, projects and practices involving personal data, by some other name than PIAs. Indeed, it is entirely possible that they've been doing similar assessment for so long that its rationales and goals are no longer an area of controversy for academics or practitioners.

We are, after all, a union of nations who, in the process of implementing Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Data Protection Directive),[1] managed to differ as to our understanding of the meaning of such fundamental data protection definitions as 'data controller,' 'data processor,' 'sensitive data,' 'anonymous data,' 'consent,' 'third party,' 'establishment,' and 'equipment.' In that light, the fact that we might fail to come to a common usage of the term 'PIA' seems hardly surprising, not least given the fact that even in those jurisdictions where the term is used, its definition and underlying understandings are rarely entirely uniform.

In short then, this is a study less concerned with obtaining a view of whether public or private sector bodies in the EU Member States make use of a tool called a 'PIA', than it is with eliciting whether legislators, regulators and public or private sector bodies in the EU Member States are open to, or already engaging with, PIA-type processes.

Legislative and Policy Framework

While there are a number of other EU Directives that contain data privacy elements including the Distance Selling Directive,[2] the E-Commerce Directive[3] the Electronic Signatures Directive,[4] and the Electronic Communications Data Protection Directive,[5]

1 Directive 95/46/EC, 1995 O.J. (L 281) 31-50.

2 Directive 97/7/EC, May 20, 1997, On the Protection of Consumers in Respect of Distance Contracts, 1997 O.J. (L 144) 19-27.

3 Directive 2000/31/EC, June 8, 2000, On Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1-16.

4 Directive 1999/93/EC, Dec. 13, 1999, On a Community Framework for Electronic Signatures, 2000 O.J. (L 013) 12-20.

Directive 95/46/EC provides the broad framework upon which the Member States of the EU (and the EEA States) have developed their data privacy regimes.

The Directive provides that Member States should have an independent supervisory authority, or authorities authorised to receive and investigate complaints. It further requires that the supervisory authority or authorities should have effective powers of intervention, including that of delivering opinions before processing operations are carried out. While the Directive is silent on the issue of 'Privacy Impact Assessments,' in order to enable the supervisory authority or authorities' power of pre-processing intervention, Article 20 of the Directive requires that processing operations likely to present specific risks to the rights and freedoms of data subjects should be examined prior to their start – which the Directive describes as 'prior checking'.

> **Article 20**
>
> **Prior checking**
>
> 1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.
>
> 2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.
>
> 3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

However, as Member States are given the discretion to determine which activities present a specific risk to the rights and freedoms of individuals and thus require prior checking, the extent to which this provision is clearly incorporated into law by Member States and acted upon as policy by their supervisory authorities varies. For example, 'prior checking', in certain circumstances, was clearly envisaged by the UK Government in its paper describing the Government's proposals for implementing the Data Protection Directive:

> **Prior checking**
> 5.13 The Government is considering which categories of processing operation should be subject to the prior checking system required by article 20. It wishes to limit them to the minimum consistent with the need to provide adequate protection for individuals in the light of the tight criteria set out in the Directive. No decisions have yet been taken, but the Government is currently considering whether there is a case for prior checking some processing operations involving data matching, genetic data and private investigation activities. The proposed prior checking mechanism is described in paragraph 6.10.[6]
>
> […]
>
> **Prior checking**
> 6.10 Under the present law processing may lawfully begin once the application for registration has been made. The new law will preserve this provision for the great majority of processing. However, those operations subject to prior checking (see

[5] Directive 2002/58/EC, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37-47.

[6] *Data Protection: The Government's proposals.* Home Office CM3725, (1997) Chapter 5: Notification./Registration.

> paragraph 5.13) will not be allowed to start until they have been checked by the supervisory authority. The supervisory authority will be required to carry out that check and give its opinion to the controller within, say, 15 working days of receiving the application. The opinion may take the form of a notification to the controller that the supervisory authority is minded to issue an enforcement notice; or a statement to the effect that it does not intend to take any further action in the context of the prior checking exercise. In either case, the processing may go ahead. If the controller decides to go ahead, he will of course be at risk of subsequent challenge from the supervisory authority for any breach of the Act. [7]

Section 22 of the UK Data Protection Act 1998 provides for a version of 'prior checking' by requiring that, as part of the notification process, certain processing might be assessed by the Information Commissioner for compliance with the provisions of the Act before the processing begins – preliminary assessment. The type of processing must specified in an Order made by the Secretary of State, if it is considered that processing would be particularly likely:

- to cause substantial damage or substantial distress to data subjects; or
- otherwise significantly to prejudice the rights and freedoms of data subjects.

Controllers wishing to process material in the preliminary assessment categories would be required to notify the Commissioner as with any other processing. They would then have to wait for a period of up to 28 days before starting processing to permit the Commissioner to give an opinion about likely compliance with the Act. In its White Paper of July 1997 the UK government identified 3 possible categories of processing that might be covered by 'preliminary assessment':

- data matching;
- processing involving genetic data;
- processing by private investigators.[8]

However, to date, no order has been yet been made in the UK, and the previous UK Information Commissioner suggested that "no 'assessable processing' should be designated".[9]

As outlined below, other Member States (and indeed the EU itself) have been more inclined to adopt a "prior check" or "prior authorisation" regime for particular types of processing.

Prior Checking in the European Union

In most cases, where Member States have implemented 'prior checking', the primary legislation defines the categories of processing operations that will be subject to prior checking, but sometimes the law provides that secondary legislation will define which processing operations should be subject to prior checking. The degree to which prior checking is used across the Member States varies widely. Table 1 is drawn from the following sources, the Article 29 Working Party's *Vademecum on Notification*

---

7 *Ibid*. Chapter 6: Enforcement.

8 *Data Protection Act 1998: Consultation Paper on Subordinate Legislation*, Home Office (1998), para. 20.

9 Cited in: Foundation for Information Policy Research, *Children's Databases – Safety and Privacy: A Report for the Information Commissioner* (March/August 2006) at p.187. http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_issues_paper_protecting_chidrens_personal_information.pdf.

Requirements; documentation available from the supervisory authorities' websites; academic and practitioner literature; and personal communications.

Table 1 Prior Checking uptake in the European Union Member States

Country	Prior checking or prior authorisation or permit required	Legislation, if applicable.
Austria	Processing sensitive data Processing data concerning offences and criminal convictions. Processing data to obtain information on a data subject's creditworthiness All "interconnections" between files (databases). All "combinations" of data (data matching, results of data sharing).	s.18, Act Concerning the Protection of Personal Data 2000 (Datenschutzgesetz 2000)
Belgium	No prior checking as envisaged under Article 20, Directive 95/46/EC.	N/A
Bulgaria	Several sources suggest Bulgaria does not have prior checking as envisaged under Article 20, Directive 95/46/EC.[10] Art.15 & 16 Bulgarian Personal Data Protection Act refer to some form of prior checking.	Possibly Art.15 & 16 Bulgarian Personal Data Protection Act
Cyprus	No prior checking as envisaged under Article 20, Directive 95/46/EC.	N/A
Czech Republic	Not known[11]	N/A
Denmark	Processing sensitive data Processing data concerning offences and criminal convictions. Use of files excluding individuals from a right or benefit of contract (blacklists). Processing data to obtain information on a data subject's creditworthiness Processing for the purpose of professional assistance in connection with staff recruitment Processing for the purpose of operating legal information systems.	s.50, Act on Processing of Personal Data
Estonia	No prior checking as envisaged under Article 20,	N/A

[10] See Beyleveld, D., Townend, D., Rouillé-Mirza, S. & Wright, J. (eds.) (2004). *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*. Ashgate at p.187; Commission Staff Working Document, *Bulgaria - May 2006 Monitoring Report* COM (2006) 214 final, p.19.

[11] In the Article 29 Working Party's *Vademecum on Notification Requirements* (03/07/06) it stated that the Czech Republic legislation does provide for prior checking, but it is currently not possible to verify this from available documentation.

	Directive 95/46/EC.	
Finland	No prior checking as envisaged under Article 20, Directive 95/46/EC.	N/A
France	Processing of the national identification number ("NIR", or social security number) Use of sensitive data (with exceptions) Interconnection of files held by different controllers for different purposes; Processing operations with a purpose to select individuals for the benefit of a right, of a service or of a contract when they are not excluded from this benefit by law or regulation, e.g. files which list the names of bad debtors, used to avoid the granting of credit to individuals who have occasionally failed to pay their debts; and more generally all forms of "blacklists"; Processing operations on biometric data that are necessary to control the identity of individuals, Processing operations on genetic data, Processing operations on criminal data, Processing personal data concerning offences and criminal convictions.	Art.25, Data Protection Act (Loi Informatique et Libertés) 1978 as amended France effectively had a system of prior checking before implementation of the EU Directive, where the public sector was subject to prior checking procedures
Germany (Federal)	Where automated processing operations pose particular/specific risks for the rights and liberties of the data subjects, especially • use of sensitive personal data or • where the purpose of the processing of personal data is to evaluate the data subject's personality including his abilities, his performance or his behaviour, unless a legal obligation applies or the data subject's consent has been obtained or the collection, processing or use furthers the object of a contractual relationship or a quasi-contractual relationship of trust with the data subject.	s.4d Federal Data Protection Act (Bundesdatenschutzgesetz)
Germany (Land Berlin)	The Land Berlin has similar rules to those of the German Federal data protection law, but requires prior checking in order to detect possible as opposed to specific risks to informational self-determination. The wording of this legislation resembles most closely that of PIA processes.	s.5 (3) Berlin Data Protection Act (Berliner Datenschutzgesetz)
Greece	Processing sensitive data All "interconnections" between files. All "combinations" of data.	Arts. 7-8, Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended)

Hungary	No prior checking as envisaged under Article 20, Directive 95/46/EC.	N/A
Ireland	Provided for, but categories of data not defined in primary legislation, no secondary legislation to date	s.12A, Data Protection Act
Italy	Processing likely to present specific risks to data subjects' fundamental rights and freedoms and dignity on account of the nature of the data, the arrangements applying to the processing, or the effects the latter may produce.	s17, Legislative Decree no. 196 of 30 June 2003 Personal Data Protection Code
Latvia	It appears that all processing is potentially subject to prior checking.[12]	Art.22(2), Personal Data Protection Act 2000
Lithuania	Processing of sensitive personal data by automated means Processing of public data files by automated means Processing carried out by a data processor on behalf of a data controller of the information systems of state registers or state and municipal institutions Processing of personal data in the course of scientific research on condition without the consent of the data subject Processing of personal data to evaluate of a person's solvency and to manage their debt Processing of personal data for the statistical or research purposes where data subjects are not informed	Art.26, Law on Legal Protection of Personal Data
Luxembourg	Most data processing operations related to sensitive data, video-surveillance, surveillance in the workplace by the employer, interconnection of data, use of personal data for other purposes than those for which they have been collected, data processing related to credit and solvency of the data subjects.	Art.14, Loi sur la protection des données (as amended)
Malta	Processing of personal data that involves particular risks of improper interference with the rights and freedoms of data subjects, categories of data not defined in primary legislation.	s.34 Data Protection Act 2003
Netherlands	Processing a number identifying persons for a purpose other than the one for which the number is specifically intended with the aim of linking the data together with data processed by other responsible parties, unless otherwise permitted. Recording data on the basis of data controller's own observations without informing the data subjects thereof. Processing data on criminal behaviour or on unlawful or objectionable conduct for third parties other than under	Art. 31, Personal Data Protection Act 2000

[12] According to Beyleveld, D. et al; supra at p.180.

	the terms of a licence issued under the Private Security Organisations and Investigation Bureaus Act.	
Poland	Data filing systems containing the following data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade-union membership, as well as data concerning health, genetic code, addictions or sex life and data relating to convictions, decisions or penalty, fines and other decisions issued in court or administrative proceedings.	Art. 46a Act of 29 August 1997 on the Protection of Personal Data (as amended)[13]
Portugal	Processing sensitive data Processing personal data concerning offences and criminal convictions. Processing of personal data relating to credit and the solvency of the data subjects The combination of personal data not provided for in a legal provision	Art. 28, Protection of Personal Data Act 1998 (Lei da Protecção de Dados Pessoais)
Romania	No prior checking as envisaged under Article 20, Directive 95/46/EC	N/A
Slovakia	Processing of personal data for protection of statutory rights and legitimate interests of the controller or the third party without data subjects consent Some types of processing of biometric data	s.27, Act No. 428/2002 Coll. on Protection of Personal Data
Slovenia	Not known	N/A
Spain	No prior checking as envisaged under Article 20, Directive 95/46/EC.	N/A
Sweden	Government can issue regulations providing that processing of personal data that has particular risks of improper interference with the rights and freedoms of data subjects shall be notified for preliminary examination. Regulations have been issued by the Government in: • the Personal Data Ordinance (processing of personal data concerning hereditary disposition derived from genetic investigation) • the Police Data Ordinance, • the Ordinance on personal data processing by tax authorities' when assisting in criminal investigations • the Ordinance on personal data processing in the Customs' activity regarding fight against crimes	s.41, Personal Data Act

[13] This is the position stated in the Article 29 Working Party's *Vademecum on Notification Requirements* (03/07/06), but it is difficult to verify from available documentation.

UK	Provided for, but categories of data not defined in primary legislation, no secondary legislation to date.	s.22, Data Protection Act 1998

The Differences between Prior Checking and PIAs

Some of these forms of prior checking may require data controllers wishing to engage in relevant processing to undertake a similar style and degree of analysis of new or adapted projects and processes as is found with the Privacy Impact Assessments. However, use of prior checking is usually limited to specific circumstances whether there is either:

- processing of certain types of sensitive data (as defined in the Directive);
- processing of other critical personal data (e.g. national identity numbers, biometric data, personal financial information, data used for 'blacklisting');
- data matching/data sharing.

Among the apparent exceptions to this rule are Latvia, where from the translated text of the Latvian Personal Data Protection Act 2000, it appears that all new data processing is potentially subject to prior checking, and the German Land of Berlin. The latter's prior checking mechanism in s 5(3) of the Berliner Datenschutzgesetz (BlnDSG) translates approximately as:

> (3) Before a decision on the use of, or a significant change in, automated data processing, appropriate technical and organisational measures should be determined on the basis of a risk analysis and a security evaluation. Where the data is processed is for employment purposes, is subject to official secrecy, or collected for the prosecution of criminal offences, a preliminary inspection of potential dangers to the right to informational self-determination is required. Where, despite the use of practicable security measures, unacceptable risks remain which cannot be overcome by [appropriate technical and organizational measures] and the [confidentiality, integrity, availability, authenticity, nature and author of revisions, or transparency] guaranteed, the processing should not take place. [14]

This appears broader in scope than the basic prior checking provisions found in other jurisdictions, including that of the German Federal Data Protection Act (Bundesdatenschutzgesetz), and appears to bear closer similarity to the PIA processes reviewed elsewhere in this Study, in terms of the expectation of the use of risk and security analyses prior to the adoption of new or revised forms of data processing, and the preemptive consideration of appropriate mitigation strategies.

[14] (3) Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung der automatisierten Datenverarbeitung sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln. Dazu gehört bei Verfahren, mit denen Daten verarbeitet werden, die einen Berufs- oder besonderen Amtsgeheimnis unterliegen oder die zur Verfolgung von Straftaten und Ordnungswidrigkeiten erhoben werden, eine Vorabkontrolle hinsichtlich möglicher Gefahren für das Recht auf informationelle Selbstbestimmung. Entsprechend der technischen Entwicklung ist die Ermittlung in angemessenen Abständen zu wiederholen. Soweit trotz der realisierbaren Sicherheitsmaßnahmen untragbare Risiken verbleiben, die nicht durch Maßnahmen nach den Absätzen 1 und 2 oder eine Modifizierung der automatisierten Datenverarbeitung verhindert werden können, darf ein Verfahren nicht eingesetzt werden.

Elements of the French 'prior checking/assessment' process also relate to elements of a PIA process, not least in the ability of the public to access notification information, the details of decisions made by CNIL with regard to the conditions required if 'risky' processing is to be allowed, as well as the reasons why 'risky' processing has not been allowed. However, in CNIL's 'prior checking' regime both the risk assessment and the publicity are facilitated by the supervisory authority rather than by the organisation carrying out the processing.

In general, across the Member States using 'prior checking' or similar mechanisms, such as 'prior authorisation' and licensing, the scope of such 'prior checking' appears to be narrower than that of PIAs, where the tendency is for a holistic privacy risk assessment rather than a basic assessment of compliance with data protection law, to be undertaken.

Previous work undertaken for the UK Information Commissioner, including the Foundation for Information Policy Research's *Children's Databases – Safety and Privacy: A Report for the Information Commissioner,* written in 2006,[15] has suggested that the UK should reconsider its current position on 'prior checking' for certain categories of personal data processing. It is suggested here that encouraging the widespread use of PIAs could:

- facilitate the process of 'prior checking' by allowing the supervisory authority to draw upon the results of PIAs incorporated into organisational processes, such as Threat Risk Assessments for new or redesigned projects;
- broaden the pool of organisational privacy understanding and expertise such that organisations will be more readily aware of the need for 'prior checking' when it is appropriate, and better able to supply the supervisory authority with appropriate information about the project/process for an appropriate prior checking assessment or decision to be made efficiently.

It is clear, however, that while supervisory authority 'prior checking' in specific circumstances has its place in a data privacy regime, in most circumstances that process is not currently synonymous with the PIA process, as it is understood in jurisdictions, such as Canada, Australia, and New Zealand.

Adoption of PIAs in the European Union Member States

While some form of 'prior checking' is provided for in legislation, and sometimes actively used, in at least 16 of the Member States, the use of PIAs of the type reviewed by this Study,in jurisdictions such as Canada, Australia, and NZ appears rare. Two Member States that have begun to explore this avenue are Finland and Ireland. Both are at a very early stage in their development work.

The Office of the Data Protection Ombudsman, Finland, has begun preliminary work on developing a PIA questionnaire, and early indications are that both public and private sector organisations would be expected to undertake PIAs, although it is unclear whether this would be at the discretion of the organisations, or whether it would be compulsory. The suggested Finnish model seems to be largely based upon, and to resemble the PIA models found in Canada, Australia and NZ.

In Ireland, the Irish Data Protection Commissioner's Office has developed policy guidance in relation to biometrics in the workplace and schools where they recommend

[15] Supra at n.9.

undertaking a Privacy Impact Assessment. The Office does not offer a template per se, but in the context of biometrics has provided a list of a range of issues that could be considered in a PIA (see below). The Data Protection Commissioner's Office integrates the undertaking of a PIA into advice it issues to organisations where it would be of benefit, and suggests that this has led to increased awareness of the need to take privacy concerns into account in decision-making processes.

> Irish Data Protection Commissioner's Office, *Biometrics in the workplace*[16]
>
> **[…]**
>
> **8. Privacy Impact Assessment.**
>
> The Data Protection Commissioner cannot give a general approval or condemnation of biometric systems. Each system must be judged in respect of the situation in which it is used. A case-by-case judgement is required. With that in mind, the Commissioner encourages employers to take the above guidance into account if considering introducing any biometric system.
>
> Before an employer installs a biometric system, the Data Protection Commissioner recommends that a documented privacy impact assessment is carried out. An employer who properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Acts 1988 & 2003. This is an important procedure to adopt as a contravention may result in action being taking against an employer by the Commissioner, or may expose an employer to a claim for damages from an employee. Data protection responsibility and liability rests with the employer, not with the person who has supplied the system (except where that person also acts as a data processor on behalf of the employer).
>
> Some of the points that might be included in a Privacy Impact Assessment are:
>
> - Do I have a time management and/or access control system in place?
> - Why do I feel I need to replace it?
> - What problems are there with the system?
> - Are these problems a result of poor administration of the system or an inherent design problem?
> - Have I examined a number of types of system that are available?
> - Will the non-biometric systems perform the required tasks adequately?
> - Do I need a biometric system?
> - If so, why kind do I need?
> - Do I need a system that identifies employees as opposed to a verification system?
> - Do I need a central database?
> - If so, what is wrong with a system that does not use a central database?
> - What is the biometric system required to achieve for me?
> - Is it for time management purposes and/or for access control purposes?
> - How accurate shall the data be?
> - What procedures are used to ensure accuracy of data?
> - Will the data require updating?
> - How will the information on it be secured?
> - Who shall have access to the data or to logs?
> - Why, when and how shall such access be permitted?
> - What constitutes an abuse of the system by an employee?

[16] http://www.dataprotection.ie/docs/Biometrics_in_the_workplace./244.htm

- What procedures shall I put in place to deal with abuse?
- What legal basis do I have for requiring employees to participate?
- Does the system used employ additional identifiers (e.g. PIN number, smart card) along with the biometric?
- If so, would these additional identifiers be sufficient on their own, rather than requiring operation in conjunction with a biometric?
- How shall I inform employees about the system?
- What information about the system need I provide to employees?
- Would I be happy if I was an employee asked to use such a system?
- How will I ensure that employees who are unable to provide biometric data because of a disability, for example, are not discriminated against by being required to operate a different system, or otherwise?
- What is my retention policy on biometric data?
- Can I justify the retention period in my retention policy?
- Do I have a comprehensive data retention policy?
- Have I updated this policy to take account of the introduction of a biometric system for staff?

As such, the development of PIAs in the Member States is at a relatively early stage. While there is interest in the concept of PIAs and the role that they could play within national data protection regimes and in privacy protection more widely, there are currently no completed tools, and there are limited legislative or policy frameworks in place to support their use. In most Member States it appears that the scope of 'prior checking' and similar functions in national legislation would not extend to justifying the broad introduction of PIAs, particularly as a compulsory requirement. As such, it is likely that where Member States' supervisory agencies wish to see PIAs adopted as part of their national data protection regime, this will develop out of persuading public and private sectors to adopt PIAs as an issue of policy rather than via legislation. In the public sector, the desire for accountability, efficient management and effective incorporation of Threat/Risk Assessments into key decision-making processes should aid in uptake. The fact that major European corporations such as Philips, Vodafone and others have adopted such strategies, and that these are seen as potentially conferring competitive advantage, may mean that at least some parts of the private sector will also be open to such developments

Research

In completing this report, the following individuals were interviewed or contacted for specific information:

Berlin Office for Data Protection and Freedom of Information
Berliner Beauftragter für Datenschutz und Informationsfreiheit

- Alexander Dix, Commissioner

Dutch Data Protection Authority
College Bescherming Persoonsgegevens (CBP)

- Dr. Lynsey Dubbeld

Irish Data Protection Commissioner's Office

- Ciara M. O'Sullivan

French Data Protection Authority
La Commission Nationale de l'Informatique et des Libertés (CNIL)

- Marie Georges, Counsellor for the President for Advanced Studies, Development and Cooperation.

The Norwegian Data Inspectorate

Datatilsynet

- Astrid Flesland, Senior Legal Adviser

Finnish Office of Data Protection Ombudsman
Tietosuojavaltuutetun toimisto

- Reijo Aarnio, Data Protection Ombudsman

In addition, documents provided by these individuals and found on websites were reviewed. These included:

- National legislation and unofficial translations
- Webpages describing prior checking processes

Additional materials

Foundation for Information Policy Research, Children's Databases – Safety and Privacy: A Report for the Information Commissioner (March/August 2006)
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_issues_paper_protecting_chidrens_personal_information.pdf/

Article 29 Working Party, Vademecum on Notification Requirements (03/07/06)
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2006-07-03-vademecum.doc.

Beyleveld, D., Townend, D., Rouillé-Mirza, S. & Wright, J. (eds.) (2004). *Implementation of the Data Protection Directive in Relation to Medical Research in Europe*. Ashgate.

D. Korff. "Study on Implementation of Data Protection Directive – Comparative Summary of National Laws" (2003)
http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf