EUROPEAN COMMISSION REVIEW OF THE EU DATA PROTECTION DIRECTIVE (DIRECTIVE 95/46/EC)

COMMENTS BY IMS HEALTH

IMS HEALTH

IMS HEALTH collects data from hospitals, general practice and pharmacies across the European Community. Our complex databases have formed a valuable resource to understand the delivery and dynamics of patient care in Member States, these being used by industry, governments, regulatory bodies, academic institutions and patient organisations.

The company respects the privacy of individuals about whom it processes information, and strives to ensure that personal data is processed in accordance with legal requirements and internationally accepted standards of good practice. This approach is adopted in respect to all types of personal information processed by the company, including product information relating to patients and health care professionals, data relating to our customers and potential customers, and information about company employees, contractors and other internal stakeholders. [IMS HEALTH does not collect patient data in identifiable form.]

GENERAL COMMENTS

IMS HEALTH supports the spirit behind, and much of the existing content of, Directive 95/46/EC. However, IMS agrees with the many voices, within the business community and elsewhere, which are calling for a meaningful review of the Directive, leading to an actual change in the text of the law itself. Implementation of the Directive over the last 3 to 4 years has highlighted a number of problems with the legislation. In particular, certain requirements in the Directive place obligations on data controllers which are significantly disproportionate to the rights and freedoms of individuals being protected. Indeed, in some cases, including the one relating to the process of anonymisation which we set out below, the law as it stands actually has the potential to undermine the privacy rights of individuals.

We agree with many of the suggestions for changes to the Directive which have recently been proposed by business and representative bodies. We support, for example, the clarification of the rules on applicable law in Article 4, and the simplification or even abolition of the regulatory notification requirements, which seem to many data controllers an excessive obligation when processing of personal data has nevertheless to be fair and lawful. We also support the creation of a 'balance of interests' test to allow data controllers to transfer personal data to outside the EU without recourse to formal adequacy procedures in circumstances where individuals' rights and freedoms are clearly not threatened, for example, where basic personal information is securely and confidentially shared within a multi-national company.

We appreciate that the Commission will receive a substantial number of replies to their consultation process. We have therefore decided to concentrate on two specific issues that are particularly relevant to the health sector.

ISSUE 1: ANONYMISATION OF PERSONAL DATA

The anonymisation of personal data is, of course, a process which fundamentally supports the privacy of the individual, allowing valuable information about individuals to be processed without reference to identifying features, thus ensuring that the data can be legitimately used without presenting a threat to the rights and freedoms of those individuals. Anonymisation forms the basis of many innovative privacy enhancing technologies in the health, Internet and other sectors. Many organisations process anonymised data for the purposes of legitimate and valuable scientific and market research.

A strict and literal interpretation of certain provisions of the Data Protection Directive 95/46/EC as currently drafted has the potential to actually threaten the advancement of anonymisation as a practical concept.

The Definition of "Personal Data"

Firstly, an issue arises from how personal data is defined. The term is defined in Article 2 of the Directive as "any information relating to an identified or identifiable natural person…". Where this definition is transposed unqualified into a Member State's national law, there is a possibility that the concept will be strictly interpreted by the regulator or the courts, in such a way that data will remain 'personal' and subject to the law if individuals remain in any way identifiable. The concept of personal data should rather be defined pragmatically, as per Recital 26 of the European Data Protection Directive. It should not be the case that to anonymise personal information, taking it outside the remit of data protection law, an organisation has to destroy the identifiers and be sure that there is no conceivable method, however unlikely in reality, by which the identity of individuals can be re-established. This is a highly impractical approach and extremely difficult to achieve in reality. It may for example require the destruction of valuable identifiable data sets residing outside the control of the anonymising organisation. The rights, freedoms, and legitimate interests of individuals can more than adequately be protected if data is anonymised in such a way that all means likely reasonably to be used to identify the said person will fail.

The value that can be gained in protecting individual privacy through de-identifying personal data is lost if the law makes it prohibitively difficult to anonymise the information. Organisations are discouraged from adopting this privacy enhancing technique, if in reality they have to apply the full provisions of the law to data which is for all practical purposes anonymous, but in law remains identifiable personal information. Further, organisations will decide that it is not worthwhile to continue their processing on the basis of anonymisation techniques, because to comply with the strict application of data protection law in this context will require an excessive outlay of resource.

The concept of anonymisation has been defined pragmatically, with reference to Recital 26, within the transposing law of some Member States of the European Union, for example:

- "Depersonalisation means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual." §3(6) Federal Data Protection Act 2001, GERMANY.

- "Personal data means data which relate to a living individual who can be identified:-
  - from those data; or
  - from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller…."
    S1(1) Data Protection Act 1998, UNITED KINGDOM.

However, in other cases, the qualifying principle present in Recital 26 is only mentioned in 'explanatory memoranda' accompanying data protection statute, or is based upon case law. In many cases, the principle has no foundation in national law at all. Even in countries where the contents of Recital 26 are reflected in transposing legislation, an overly strict interpretation can be applied. For example, in her 'Legal Guidance' on the Data Protection Act 1998, the UK Information Commissioner states that "true anonymisation may be difficult to achieve in practice" (s2.2.5). This view does not take account of the safeguards that data controllers are applying in practice, and does not reflect the pragmatism that lies at the heart of Recital 26.

The inconsistent application and interpretation in this area does not engender confidence amongst data controllers seeking to apply anonymisation techniques on a multi-national basis. Therefore, we suggest that the important qualifying criteria present in Recital 26 are reflected within the definition of 'personal data' itself. The inclusion of the relevant wording within the Articles of the Directive will lead to the consistent transposition of a fundamentally important principle into national law.

The Application of the Law to the Act of Anonymisation

The second point we would like to raise in this area relates to the application of the law to the actual act of anonymisation itself. Procedures and processes established to process data without reference to individual identity, to enhance privacy, should not be undermined by the blind application of data protection rules that in essence are designed to protect the processing of identifiable personal information. In particular, it may be the case that to actually anonymise personal information, in compliance with the Directive, the explicit consent of the individual has to be sought (sensitive personal data), or notice of processing provided to that person (personal data). This is because the concept of 'processing' under the Data Protection Directive is very widely defined. Although it may not have been the intention of those drafting the legislation, it is conceivable that this definition catches all conceivable processing activities, including the act of anonymisation itself.

It is certainly clear that those who drafted the Directive did not consider how this would negatively impact on the beneficial process of anonymisation. In particular, organisations are discouraged from adopting anonymisation as a privacy enhancing technique, when in reality they have to expend considerable effort and resource seeking unnecessary consents from individuals. It can also be strongly contended that data controllers will refrain from anonymising personal information, when they have to gain the individual's consent for processing anyway.

Some examples of how the law as drafted can adversely and unnecessarily impact business are:

- <u>Example 1: Software development</u>

A software supplier wishes to develop a new prescription dispensing system for community pharmacies. A community pharmacist agrees to help with the development and testing of the system. The pharmacist is asked to provide an anonymised sample data set for testing

purposes. The pharmacist strips all features relating to the patient and doctor [1]. Only the data on the drugs prescribed is sent to the software supplier. The software supplier uses the data supplied by adding unrelated pseudonyms. Despite the information being supplied offering no danger to personal privacy, a strict literal interpretation of the Directive would require that individual patient consent be sought for the anonymisation. In addition every doctor whose prescription had been dispensed by the pharmacy would need to be notified.

- Example 2: Process improvement

A leading high street travel and holiday company, under new management, rationalises its sales workforce, introducing a commission based compensation scheme. It purchases a new sales and marketing database with enhanced functionality. It decides that the data should be processed in an anonymised form centrally in the parent company for the new purposes envisaged (payment of sales commission and product performance analysis). All information identifying the customer is destroyed prior to transfer. The data sent, however, includes significant amounts of anonymous 'sensitive' information about customers, for example, relating to disability (access in hotels and apartments), sexuality (specialist holidays) and religious beliefs (pilgrimage locations). In theory, consent would be required to anonymise the sensitive data. Notice would have to be given in all other cases.

- Example 3: Business analysis

A large multi-national Business to Business communications service provider decides that its existing sales, marketing and customer service database needs updating with new contact details relating to prospective customers. It is decided that the 40% of the legacy data is completely out-of-date, much relating to ex-customers. These data include details about employees in customers' IT procurement and business development departments, information about their role and position, the budgets available to them, their contact details, the products they purchased, the service history, etc.. The company decides to archive the legacy data in a custom built data centre. It is decided that the data, although no longer of use for direct marketing, can be valuably used for various product and business analysis purposes. All identifying information relating to the individual employees, their contact details, etc is stripped from the data prior to transfer. Customer codes are removed. The data are being anonymised only to protect customer's identity. However, under a strict interpretation of the Directive, the company would be forced to contact each individual to advise that their data is to be anonymised.

Should the definition of ‘processing’ under the Directive 95/46/EC actually cover the act of anonymisation? Clearly the Directive does not apply to personal data rendered anonymous. Recital 26 states that “the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable”. A purposive view of this Recital leads one strongly to the opinion that the Directive should have no more application to the operation of anonymising data than to the use or disclosure of anonymous data. In fact, this is the exact view expressed by the judge, LJ Simon, in the UK court case Regina v Department of Health, ex parte Source Informatics Ltd[2].

It may in the end be for the European Court of Justice to rule on whether the act of anonymisation falls under the scope of Directive 95/46/EC, most likely through a reference for a

[1] An argument can actually be made that the data relating to such persons is never processed at all. The system just leaves this data behind.

[2] (2000) 1 All ER 786.

preliminary ruling by a national court. One of the clearest statements of the Court's general approach to the interpretation of Community law can be found in C.I.L.F.I.T v Ministry of Health[3], where it stated:

> "…every provision of Community law must be placed in its context and interpreted in the light of the provisions of Community law as a whole, regard being had to the objectives thereof and to its state of evolution at the date on which the provision in question is to be applied." (para. 20, emphasis added)

Over the years, the Court has gained a reputation for favouring a purposive or teleological approach to interpretation, rather than a literal approach. On this basis, it may be speculated that, given the facts in Source, the opinion expressed by Simon LJ could find favour were the Court of Justice required to deliberate. However, to alleviate the current legal uncertainty in this area, it would be preferable if the Directive clearly indicated that anonymisation is a technique specifically excluded from the scope of 'processing'. If the definition of 'processing' is to retain its current very wide application, then appropriate pragmatic exemptions from certain key principles of the legislation should be drafted to encourage data controllers to anonymise wherever possible

It is of particular note that the recently departed French Government indicated their support for creating a legislative environment in which anonymisation is encouraged. On 30 January 2002, during the debate in the French National Assembly on the draft law transposing the Data Protection Directive in France, the then Minister for Justice, Marylise Lebranchu, stated that the French Government wish to explore this issue with the French data protection regulator, the 'Commission Nationale de l'Informatique et des Libertés', prior to the bill progressing further through the legislative process. This commitment was in direct response to calls from Members of the Assembly that exemptions be made from the consent and notice requirements of the legislation for the process of anonymising personal data. It is notable that many of those making these calls were from parties which now form the governing majority within the French National Assembly. [The draft law is due before the French upper chamber, the Senate, in the Autumn of 2002.]

ISSUE 2: PROFESSIONAL DATA

Recent trends in the interpretation of data protection legislation in Canada have resulted in a distinction being drawn between 'personal information' and 'professional or work product information'. These trends acknowledge that, while information relating to, or about an identified or identifiable person, is worthy of privacy protection, such protection should not extend to information that concerns an individual functioning in his or her professional or work capacity. This distinction is based upon both an analysis of the rights that such legislation is designed to protect, as well as a recognition of the value of such information to the protection and furtherance of societal goals.

In Europe, Directive 95/46/EC defines 'personal data' to mean:

> "Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[4]

[3] Case 283/81, [1982] ECR 3415.

[4] Directive 95/46/EC , Article 2

This extremely broad definition would, on its face, appear to cover any information in which the name, or other identifying feature of an individual, appears.

Similarly the Canadian federal privacy legislation, the Personal Information Protection and Electronic Documents Act[5], contains a broad definition of 'personal information' to mean…

> "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organisation"[6]

On its face, this definition appears to the most part to encompass the same breadth of information as does that of 'personal data' in the Directive. However, in a recent finding in response to a complaint over the use of physician prescribing information by a health informatics company in Canada, the Federal Privacy Commissioner in that country interpreted it as follows[7]:

> "In my view, therefore, the meaning of 'personal information', while broad, is not so broad as to encompass all information associated with an individual.
>
> It is certainly difficult to discern how an individual prescription can constitute personal information about the physician who wrote it. While it can be revealing with regard to the patient – the nature of an illness or condition, for instance, and perhaps its severity – it discloses little or nothing about the physician as an individual. Indeed, a prescription is not normally treated as personal information about himself or herself by the prescribing physician. The patient is not enjoined to secrecy, remaining entirely free to show it to anyone at will or to leave it unattended in a public place.
>
> This is not surprising, because the prescription is not, in any meaningful sense, "about" the physician. It does not tell us how he goes about his activities, whether he is casual or formal, whether he works mornings or afternoons, whom he meets, where he goes, what views he holds, or any of the other myriad details that might constitute personal information. Rather a prescription is the outcome of the professional interaction between the physician and the patient: the physician meets the patient, carries out an examination, perhaps reviews the results of tests, and then issues a prescription. Hence, the prescription can perhaps most appropriately be regarded as a 'work product'. I find it to be information not about the physician, but about something once removed, namely the professional process that led to its issuance. [emphasis added]

Of course this ruling specifically relates to the processing of prescription related data. However, the argument has a wider application. The distinction between 'personal information' and 'professional or work product information' is one that has been advocated for a number of years by Dr. Ann Cavoukian, the Freedom of Information and Protection of Privacy Commissioner for the province of Ontario, Canada's largest. The Office of the Information and Privacy Commissioner of Ontario (the 'IPCO') has consistently decided that information about the activities undertaken by an individual in his or her employment, professional or official government capacity is not information about that individual and is therefore not personal information. The IPCO has therefore determined that there is an employment / professional

---

[5] S.C.2000, c.5.

[6] Ibid. s.2

[7] Available online at: http://www.privcom.gc.ca/wn_011002_e.asp. The finding is currently under appeal before the Federal Court of Canada.

exception to the definition of personal information. The IPCO approach is based on the view that the mere association of an individual's name with other information, whether in an official government, employment or professional capacity, does not automatically make the information personal information.[8]

Dr. Cavoukian's international stature in the global privacy community is well-known through, among other matters, her advocacy of privacy-enhancing technologies and co-authorship of academic papers on privacy with European Data Commissioners.[9] In Ontario, she has recently made the case to government that evolving privacy legislation must distinguish between the two types of information.

In her response to the Ministry of Health and Long-Term Care consultation on the Health Sector Privacy Rules, she stated:[10]

> "Similarly, we believe that the definition of personal health information should be drafted to ensure that information about the employment and business responsibilities, activities and transactions of individual health service providers is not included. This type of information may be used to objectively assess the quality of provider services and should be considered professional in nature rather than personal health information."

Similarly, in her Submission to the then Ministry of Consumer and Commercial Affairs in response to A Consultation Paper: Proposed Ontario Privacy Act, the Commissioner submitted that[11]:

> "Finally, to provide consistency with other legislation (i.e., the federal Privacy Act), and to avoid confusion, the legislation should stipulate that information about the employment and business responsibilities, activities and transactions of an individual is not subject to the privacy protection provisions of the legislation."

The Ontario government has recently released a Consultation Draft of the Privacy of Personal Information Act, 2002[12]. This Draft contains a definition of 'personal information' that excludes both 'organisational information' and 'professional identity information'. 'Organisational information' means "the name, title and contact information of an identifiable individual when it is used for the purpose of identifying the individual in an employment, business, professional or official capacity, including carrying on business from a dwelling, or for purposes related to the operation or functioning of an organisation". 'Professional identity information' means:

> "… the name, title, contact information and professional designation of an identifiable individual when it is used for the purpose of describing the professional or official

---

[8] See, for example, Orders P-1412 and Reconsideration Order R-980015 available online at: http://www.ipc.on.ca. These orders were issued under the Ontario Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c.F-31 in which 'personal information' is defined in s. 2 as "recorded information about an identifiable individual, including…"

[9] See, for example, Privacy-Enhancing Technologies: The Path to Anonymity (Volumes I and II): A Joint Project of the Office of the Information and Privacy Commissioner/Ontario and the Registratierkamer, The Netherlands available online at: < http://www.ipc.on.ca/english/pubpres/papers/summary.htm> and Biometrics and Policing: Comments from a Privacy Perspective. This is a chapter, contributed by Ontario Information and Privacy Commissioner Ann Cavoukian to the book, Polizei und Datenschutz - Neupositionierung im Zeichen der Informationsgesellschaft, a compilation of essays by international privacy and data protection experts. The book was released in conjunction with the Data Protection Authority of Schleswig-Holstein's 1999 Summer Academy available online at: < http://www.ipc.on.ca/english/pubpres/papers/summary.htm>

[10] Available online at: <http://www.ipc.on.ca/english/pubpres/reports/health00.htm>

[11] Available online at: <http://www.ipc.on.ca/english/pubpres/reports/ccrsub00.htm>

[12] Available online at: < http://www.cbs.gov.on.ca/mcbs/english/pdf/56XSMB.pdf>

> responsibilities of the individual and the manner in which the individual carries out those responsibilities, and includes a description of those responsibilities, but does not include any personal information of another individual."

In her response to the government on this Draft, the Commissioner has again articulated her support for the distinction[13]:

> First off, the IPC thinks the term 'professional identity information' is confusing and recommends changing it to 'professional information'. Secondly, while we think the exclusion of professional activities from the definition of personal information is essential in order to enhance professional accountability, we are concerned that the inclusion of the phrase, "the manner in which the individual carries out those responsibilities," could be interpreted to include human resource matters, such as an employee's performance appraisals. Therefore, the IPC recommends the government re-work this definition to make it clear employee human resources records are covered by the draft legislation. [emphasis added]

Representatives of both government Ministries involved in the preparation of the legislation, the Ministry of Consumer and Business Services and the Ministry of Health and Long-Term Care, have recently advised that, while they acknowledge that the definition in the Consultation Draft could be improved, they are committed to the policy distinction behind the definition

Finally, it is instructive to consider the approach taken by the Global Business Dialogue to this issue. The Global Business Dialogue (the 'GBD') is an organisation comprised of over 80 of the largest global corporations[14]. Its working group on e-commerce met last September in Tokyo to consider global issues related to electronic commerce. One of the issues considered was that of Consumer Confidence, which the Dialogue addressed in a paper entitled 'GBDe Personal Data Privacy Protection Guidelines'.

For the purposes of the guidelines, 'consumer' is defined as:

> "Any natural person who acts in his or her individual capacity for purposes outside his or her trade, business or profession and who is a customer or potential customer of a company's business."

The Guidelines further define 'Personal Data' of any Consumer to mean:

> "Any data collected online by the Company which can identify the Consumer or which, when easily combined with other available data, can identify the Consumer."

Although the Guidelines were developed for voluntary application to Internet commerce it is suggested that they may be used by any other businesses for which they may be relevant. In addition, the GBDe encourages all its members and all other businesses to utilise these Guidelines in the world-wide application of privacy data protection (applied in parallel and with due respect to any applicable law). The GBDe guidelines thus illustrate that major global businesses recognise and support the distinction between information about individuals acting in their individual capacity and that related to individuals acting within their trade, business or profession.

---

[13] Available online at: < http://www.ipc.on.ca/english/pubpres/reports/cbs-0202.htm>

[14] Information on the GBD and its members may be found online at: http://www.gbde.org/index1.html

In summary, both legislative and non-legislative organisations recognise that there is a difference between 'personal' and 'professional or work product information' that should be made from a policy perspective when defining the scope of privacy protection.

Article 1 of the Directive states, as one of its Objectives:

> "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data."

However, even within the context of protecting the 'fundamental rights and freedoms of natural persons', some data is acknowledged to be 'more sensitive' than others.[15]

Given this distinction between degrees of sensitivity with respect to different types of personal data under the Directive, it may well be questioned whether the definition of 'personal data' of necessity must be interpreted so broadly as to encompass all information by which an individual is identified or identifiable? The question obtains even more legitimacy if one considers that the definition applies only to 'natural' persons.

It may well be that, as has been the case in Canada, legislators and others involved in the development of privacy or data protection initiatives, initially failed to give adequate consideration to the potential implications of language that could, and in fact has been interpreted, to apply to all manner of information about individuals[16].

While individuals certainly expect a right to privacy with respect to factors specific to their physical, physiological, mental, economic, cultural or social identity, do they expect that the position they hold in the work force, their employment activities, their professional responsibilities should be subject to data protection legislation in the same manner as their personal opinions? Is such an expectation reasonable in the context of an individual's relationship with others in the work environment? Are an individual's privacy rights at issue when he drafts a report on a company meeting he has chaired looking at business trends? When an individual sends his superior an email that the negotiations on a particular business transaction are not going well, are personal privacy issues at stake? When a company creates a business client database of its key contacts and their corporate responsibilities, is such information of the nature that should be protected by privacy or data protection legislation?

It is suggested that the answer to all of these questions is in the negative. In the examples provided it is evident that the 'factors specific to the identity' of the individual are not at issue; in fact, they are irrelevant. The only thing that is relevant in this respect is that the information relates to a company representative, a business negotiator, etc.. It does not relate to, nor is it about these people as individuals, because of their specific identity as human beings. What is at issue is the fact that the individual represents the legal entity that is conducting business. Information is recorded relating to the actions or activities of the individual solely in that context.

---

[15] Paragraph 1 of Article 8 relating to the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life.

[16] The Director of Electronic Commerce Policy for Industry Canada, the Canadian government department responsible for the Personal Information Protection and Electronic Documents Act has publicly stated that it was not the intent of the government that the legislation apply to 'professional' or 'work product' information, thus supporting the finding of the Federal Privacy Commissioner in the case outlined above – reported in Murray Long, PrivacyScan, October 1, 2001, at p. 7

Accordingly, it is suggested that the policy rationale for affording privacy protection to information relating to natural persons functioning in their business or professional capacity should be debated. If it is agreed that the Directive should be limited in scope to the recognition of rights that are essential and specific to the individual as a human being, this should be reflected in an appropriate change to the definition of personal data in the Directive. Alternatively the inclusion of a new definition conceptualising information relating to work or professional life could be introduced, this being subject to appropriate derogations from the legislation. This new concept, perhaps termed 'professional information', could be defined as follows:

> "Information specific to the employment, business or professional responsibilities of a data subject, such as: name, job title, workplace contact details; description of activities and transactions he has engaged in carrying out those responsibilities; reports and other work products; where they are processed for work related purposes."

The definition would allow confidential information processed for human resource purposes to remain within the remit of the legislation. However, with appropriate exemptions being made, it would exclude data which in essence relates to the entity for which the data subject works, rather than the individual.