



Information Commissioner's Office

The Information Commissioner response to The Council of Europe's consultation on The Modernisation of Convention 108

Introduction

The Information Commissioner for the United Kingdom (ICUK) has responsibility for promoting and enforcing the UK Data Protection Act 1998 (DPA) and the UK Freedom of Information Act 2000. The Information Commissioner is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICUK does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The ICUK's response to this consultation is primarily based on the practical experience he has gained in regulating compliance with United Kingdom data protection law.

The ICUK agrees with the Council's assertion that the fundamental legal standards contained in Convention 108 remain valid. In particular, it is useful that the Council have highlighted that Convention 108 has a broader international application than European states. The ICUK also considers it particularly useful that the Council of Europe has published their position paper on modernising Convention 108 at the same time as other international data protection legal frameworks and standards initiatives are being consulted upon.

In the ICUK's opinion, an effective data protection framework must:

- be clear in its scope, particularly in the context of new forms of individual identification;
- protect the rights and freedoms of individuals whilst permitting the free flow of data;
- place clear responsibility and accountability on those processing personal data, throughout the information life cycle;
- ensure obligations for those processing personal data are focused on processing that poses genuine risk to individuals

- or society; rather than focusing on particular categories of data; and
- give individuals clear, effective rights and simple, cost-effective means of exercising them.

The ICUK hopes that this consultation exercise will eventually result in the development of data protection framework that has these features.

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

The ICUK would support continuing the drafting any modernised data protection framework in a technologically neutral way. This effectively provides a “future proofing” for any modernised Convention that can remain relevant even as technology progresses. To start to detail the type of technologies the standards might apply to in the future is to rely on the foresight of those drafting the Convention. Ten or even five years ago we could not have foreseen the impact of technologies such as biometrics, social networking, targeted behavioural advertising, near field communications or cloud computing. Writing a legal text that could ensure that comparable future developments are adequately covered is therefore an impossible task.

This is not to say that the ICUK cannot see a need to provide greater detail in the drafting of a modernised Convention. But this should focus on providing greater clarity around the fundamental concepts of data protection, rather than detailing the type of technologies that the Convention should apply to. A modernised Convention 108 should be a “living instrument” that can be applied to technology as it advances, rather than an instrument that has a progressively narrower application as new technologies come to the fore and current technologies become obsolete.

Any modernised legislative framework should continue to apply to both direct and indirect forms of identification. However, there is evidence of considerable uncertainty in the practical application of the current law to information that identifies people indirectly. A modernised Convention should open the way for a more realistic treatment of this sort of information. For example, it might require the security principle to apply to all forms of personal data, but acknowledge the practical difficulty involved in obtaining consent for the processing of, or the granting of subject access to, some information that identifies individuals indirectly. A simple ‘all or nothing’ approach to data protection requirements no longer

suffices, given the variety of information that can now fall within the definition of personal data. The requirements should be more clearly linked to the risk to individual privacy.

2. Should Convention 108 give a definition of the right to data protection and privacy?

The right to privacy is enshrined in several other Conventions and international agreements. Data protection applies the right to privacy to personal data, drawing out specific obligations on data controllers and specific rights for data subjects, including subject access, rectification and destruction and the right to object to certain processing.

While the ICUK does not see the need to provide another definition of the right to privacy or a right to data protection, he sees the value in being explicit about the strong links between Convention 108 and the rights enshrined in the European Convention on Human Rights, in particular those Article 8 rights to a private and family life, home and correspondence.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

The ICUK considers it vital that any modernised Convention retain the comprehensive coverage of scope. While the ICUK appreciates that other instruments, such as the EU Data Protection Directive, have explicitly excluded law enforcement and judicial authorities from their scope, the European Commission has now stated that it is considering extending EU data protection rules to the areas of police and judicial cooperation in criminal matters¹. UK data protection law already applies to these areas, albeit with appropriate exemptions which allow police and judicial services to operate effectively.

The current debate on the future of data protection is to broaden the scope to cover these areas, to adopt the comprehensive approach that has been a cornerstone of Convention 108 since its adoption in 1981. The ICUK supports this approach and his experience is that high standards of personal data protection are neither incompatible with, nor an impediment to, effective law

¹ See Chapter 2.3 of "A comprehensive approach on personal data protection in the European Union", a Communication from the European Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on 4 November 2010

enforcement and judicial services. It would be unfortunate if a modernised Convention abandoned the comprehensive approach.

4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0.)?

Other instruments exclude from their scope data processed by a natural person in the course of purely personal or household activity, such as the EU Data Protection Directive. The ICUK supports this notion.

However, the ICUK considers it vital that a better understanding is needed of what comes within the scope of purely personal or household activity. This is becoming an acute practical problem given private individuals' capacity to process personal data on the internet and to make it widely available to other individuals, for example, through social networking services. There are also questions about how far such an exclusion can be applied to the activities of private individuals on the internet. There are also significant practical consequences for data protection authorities in terms of the extent to which any modernised Convention may require them to regulate private individuals' online behaviour.

5. The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

The ICUK considers it vital that the collection of data is included in the definition of automatic processing, or at the very least data which is intended to be processed by automatic means is brought within the scope of any modernised Convention. This would bring the Convention in line with other national and international data protection instruments.

The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?

There can be a lack of clarity and certainty in determining which organisation is the "controller of the file" in relationships between organisations that process personal information. The complexity of modern business relationships means that there are endless

possibilities and the question of who takes ultimate responsibility for ensuring that personal information is processed in accordance with the law is often opaque. This is not helped by very general definition as to what constitutes a “controller”. The ICUK would support reviewing this definition.

In terms of whether there should be several criteria listed, and whether these criteria should be cumulative, the ICUK would again say that the complexity of modern business relationships could not have been foreseen 10 years ago. Rather than list criteria as to what constitutes a “controller”, the ICUK would see value in providing a better description as to what activities a controller of the file would undertake.

6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

With regard to the ICUK’s experience of definitions in the EU Data Protection Directive, it is clear that a simple distinction between a controller and a processor no longer reflects the complicated relationships that exist between organisations processing personal data. The definitions of “controller” and “processor” in Article 2 of the EU Data Protection Directive assume that there is always a clear distinction between those who determine the means and purpose of the processing and those who process on behalf of the controller. The definitions assume that a processor is an essentially passive entity, acting on behalf of a controller, with no independent influence over the way the processing takes place. This does not reflect the reality of current business practice where an organisation that at first sight appears to be a processor – typically a sub-contractor – may exercise considerable influence over the way the processing takes place and may, in many respects, act as a controller. This situation is made all the more difficult because subcontractors may outsource certain aspects of their work to other subcontractors. This can make it difficult to establish responsibility, for example, in enforcement cases.

An explicit accountability principle might help deal with controller-processor relationships that are difficult to define.

Protection principles

7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such a principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

The ICUK would support building proportionality more explicitly into any modernised Convention.

8. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

The relationship between these two aspects of fairness can be confusing. An emphasis on consent rather than transparency, or vice versa, can give a very different complexion to data protection regimes. It can confuse individuals and can cause great practical uncertainty for controllers. A new legislative framework should give a clearer indication of when consent is needed to legitimise the processing of personal data, and when it is sufficient for individuals to be merely aware that the processing is taking place. Consent should only be used to legitimise processing where individuals have genuinely free choice.

9. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

The ICUK has some doubt about the legal framework that involves the need to satisfy a condition to legitimise the processing of personal data, and an additional condition where sensitive personal data are involved. He believes that this can result in the artificial justification or restriction of otherwise unobjectionable processing and offers little meaningful protection to individuals. Indeed the predecessor to the current UK DPA, the Data Protection Act 1984, did not contain special provisions governing the processing of sensitive personal data. In practice this did not stand in the way of the proper protection of genuinely sensitive data, but provided more flexibility for business and the ICUK in the way this was delivered.

10. Convention 108 does not expressly mention compatibility in relation to purpose. In today's context, personal data is

commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

The ICUK would make two points here. The first is in relation to his approach to compatibility of purpose. The ICUK considers that much of the protection that is provided by the compatibility principle is provided by fairness and transparency about the purposes for which personal data are used. Both the EU DP Directive and the UK DPA make explicit reference to compatibility with "specified" purposes, which makes a strong link with transparency of processing operations. Often a breach of the compatibility principle is also a breach of the fairness principle.

The second point is that where the EU DP Directive and the UK DPA have a compatibility principle, both actually refer to further purposes not being incompatible with the specified purposes.

11. Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime : is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

The term 'biometric personal data' is perhaps misleading. Biometry involves capturing a piece of biological information, such as a measurement of a person's facial features, and using an algorithm to convert this into a biometric – put simply a set of numbers. A reader is then used to determine whether biological information presented to it on a subsequent occasion corresponds with the biometric already held in a database. This process is used to determine whether a person should be allowed to enter a building, for example. Therefore any new legislative framework needs to draw a distinction between the raw biological data from which a biometric is derived, and the biometric itself; the terms are sometimes used interchangeably.

The ICUK is not of the opinion that a physical or biological characteristic should necessarily be included within the definition of 'sensitive personal data'. Nor does he consider that the biometric itself should necessarily be considered 'sensitive'. This is because of the wide range of biometric systems in existence and their varying effect on individuals. The ICUK's view is that sensitivity arises from the overall nature of the processing operation, particularly its actual or potential effect on individuals, rather than just the nature of the information being processed.

12. A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

The application of data protection law to children raises a number of difficult issues for children, parents and those that process personal data about children. Some have suggested that in future data protection law could regulate the processing of children's data better, primarily by specifying an age at which childhood ends and adulthood begins, and by setting out specific requirements for the processing of data about children. However, we are sceptical as to what this would achieve in terms of the informational protection of children. This is because rules for defining a child vary across the world. In some countries there is a clear age limit, in others – such as the UK – there is no legal definition of a child. We do not anticipate a modernised Convention being able to harmonise this. The other problem is that different age groups of children, and indeed different individuals within those groups, can have very different levels of maturity and understanding. We envisage it being highly problematic to formulate a set of detailed data protection rules that are as applicable to a five year old as they are to a child in his or her teenage years, for example. The law should recognise that even relatively young children can understand simple low-risk propositions, for example, when they decide to provide their contact details when they sign up for an electronic newsletter.

We also note the formidable practical difficulties involved in setting up mechanisms for verifying a child's age or for obtaining parental consent; mechanisms that are relatively easy for a determined child to circumvent.

For these reasons we do not support the inclusion of detailed provisions that relate specifically to children. However, we think that the law should encourage initiatives such as industry codes of practice, setting out detailed rules for processing personal data about children in particular contexts – for example, marketing goods and services to specific age-groups.

13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of

security also include a right for data subjects to be informed of data security breaches?

It should be a prerequisite that in revising any of the current obligations on controllers, and in introducing any new obligations, those obligations have a substantive effect on the protection of privacy, and reduction of risk to the individual. New measures should not be introduced that add to the burden on data controllers but do not significantly add to the protection of the privacy of the individual.

The ICUK considers that, in the right circumstances, breach notification can significantly enhance data protection. However, the introduction of a general breach notification requirement must have a sound evidential base that demonstrates it will have a significant impact on the protection of personal data, and must be framed in such a way as to avoid becoming merely a way of complying on paper, with no substantive effect on information privacy in practice.

An alternative might be to require controllers to have a breach notification policy in place.

14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

The ICUK would reiterate that it is his view that sensitivity arises from the overall nature of the processing operation, particularly its actual or potential effect on individuals, rather than just the nature of the information being processed.

15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

The Information Commissioner would like to see a new, general requirement of accountability introduced. This would reinforce the responsibility of controllers for ensuring that personal information is properly protected in practice by requiring them to:

- take appropriate and effective measures to implement data protection principles; and
- be able to demonstrate, on request, that such measures have been taken.

The requirement would not impose any additional burden on controllers that take their responsibilities seriously, but would emphasise, on the face of the Convention, that data controllers have to take concrete measures to deliver effective data protection in practice. It would, through the transparency element, also assist DP authorities in targeting their activities on areas of genuine DP risk.

An accountability requirement would have to be scalable to the size of the organisation concerned and the risks of the processing of personal data they perform, so as not to impose any further unwarranted obligations on controllers. Whilst a large multinational might be expected to have measures in place such as relevant policies and procedures, a data protection official, privacy impact assessments and training programmes, a small or medium enterprise would not necessarily be expected to do any more than be able to explain the steps it has taken to identify and address any risks its business poses to the privacy of personal information. Accountability already features in some DP regimes including the OECD privacy guidelines and the APEC privacy framework. Its introduction as a principle in the Convention would promote global harmonisation of DP requirements and could contribute to reducing the administrative burden imposed by the current rules on international data transfers.

16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

The principle of privacy by design is implicit in the existing data protection principles - for example, the requirement that personal data shall not be excessive. However, an explicit privacy by design requirement would give a clear message to those designing, procuring and operating information systems that the processing of personal data must be done in the most privacy friendly way practicable.

Rights – Obligations

17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

The ICUK would support this as it is already covered in the right of access provided in both the EU DP Directive and the UK DPA.

18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

The ICUK can see some situations where the "right to oblivion" could work well in practice, such as where an individual wishes to delete their record from a social network, but these situations are limited. It is essential that individuals understand the nature and extent of their rights, and that those rights are framed in a way that is not misleading to the individual. The "right to oblivion" suggests possibilities that may not actually be available to the individual, or that in some cases could work against their fundamental rights and freedoms. It could also be technologically difficult for this right to be delivered in practice in some circumstances, such as when the information has been made publicly available on the internet.

19. Should there be a right to guarantee the confidentiality and integrity of information systems?

The ICUK would question the value of making this a "right" for the individual, as opposed to the greater value in strengthening the provisions of the principle of data security. How would individuals assert this right? More clarity is needed on the exact nature of this provision if it to be framed as a right to individuals.

20. Should a right 'not to be tracked' (RFID tags) be introduced?

This right will need some thinking through. Tracking happens using more than just RFID tags and to produce a right based on one type of technology seems to run contrary to the aim of keeping the Convention technology neutral.

21. Should everyone have a right to remain anonymous when using information and communication technologies?

There are three questions to ask in relation to the right to be anonymous. The first question is to whom the individual is anonymous. Is it their communications service provider, the websites that they visit, third parties engaged by the CSP or website, national authorities or other individuals with whom they may be communicating?

This leads to the second question. Where is providing this right technically possible? Traffic data has to be processed by the

communications service provider for billing purposes. Websites need to use cookies in some circumstances to provide interactive services to the individual.

The final question is where is this right desirable? For example, does an individual have the right to remain anonymous when using information and communications technologies to harass other individuals, to disrupt emergency services or break the law? The UK Privacy and Electronic Communications regulations place an obligation on telecommunications service providers to allow individuals to withhold their number from the recipient when making a call. However, the telecommunications service provider may override this right, in so far as it appears to the provider in question to be necessary, to trace malicious or nuisance calls. The right does not exist at all where the call is made to emergency services.

22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?

There are also significant practical consequences for data protection authorities in terms of the extent to which any new legislative framework may require them to regulate private individuals' online behaviour.

Connected to this, but of broader significance, is the need to balance a high standard of data protection against a strong upholding of the right to freedom of expression. In an age of online blogging, where should the line be drawn in any future Convention?

Sanctions and Remedies

23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

The ICUK would support both of these measures. In particular, the ICUK considers giving more scope to alternative dispute resolution to be of paramount importance. But there is a broader point. Organisations should also be encouraged to 'self-regulate' as far as possible, for example, by adopting sectoral codes or applying recognised standards for collecting and handling personal information. The ICUK has no doubt that effective self-regulation by organisations (perhaps backed up by some form of accreditation), and self-protection by well informed individuals, are important

elements of a modern data protection regime. A future framework should acknowledge and promote this.

With complaints handling, data protection authorities need the freedom to set up procedures to suit their resources and the local conditions. For example, it would be helpful if a modernised Convention provided a clear basis for data protection authorities to approve other complaint handling mechanisms, so as to be able to work with other relevant regulators or industry groups who may be able to achieve better or more cost effective results for individuals. The Commissioner has significant doubts as to the sustainability of a state of affairs where data protection authorities are expected to deal with every complaint about every aspect of the processing of personal information – particularly at a time when resources are being cut back.

Data Protection Authorities

25. How to guarantee their independence and ensure an international cooperation between national authorities?

Within the EU, data protection authorities are set up differently in the various member states and so are independent in different ways. In other countries, particularly those outside Europe who can now sign up to the Convention, the supervisory functions may be done by a separate authority or within an organisation. What is important is that the current Article 1(3) of the Additional Protocol (CETS 181, 2001) is extended to specify what is to be understood by independence.

For example, in Ireland the Commissioner is appointed by the government, but is independent in the exercise of his or her functions. In Canada, the Privacy Commissioner is an Officer of Parliament who reports directly to the House of Commons and the Senate. Both are considered independent supervisory authorities. In the UK, the ICUK considers the fact that his data protection work is funded by notification fees to be a crucial factor in his independence. This fee-based funding mechanism also ensures the ICUK has the necessary budget to fulfill his duties, which is particularly relevant in the current economic climate.

It might be helpful to update the additional protocol to specify that independence includes, for example, sufficient funding to carry out duties and obligations; independence in the exercise of functions; the freedom to set priorities and strategy; the head of the authority appointed by and reporting to the national Parliament or its equivalent.

With regard to international co-operation between authorities, the current provisions in Article 13(3)(b) of the Convention and Article 1(5) of the Additional Protocol are a barrier to authorities co-operating. This is because the provisions prevent the exchange of the personal data related to the issue that the authorities are co-operating to resolve. In the experience of the ICUK, most complaints that need co-operation with another authority to resolve involve exchanging the relevant personal data of the complainant. Without this information authorities cannot carry out the necessary checks and investigations to resolve the complaint.

The ICUK strongly recommends adding to or clarifying the articles mentioned above to ensure that supervisory authorities are able to co-operate fully, exchanging all necessary information including personal data, to ensure effective protection for individuals. To the ICUK's knowledge, all supervisory authorities have appropriate safeguards in their national law with regard to disclosures of information by staff. For example, in the UK it is a criminal offence for any ICO member of staff to disclose information relating to an identifiable individual obtained in the course of their duties to anyone outside the authority².

26. Should their role and tasks be specified?

The current data protection framework has resulted in many differences in the roles, remits and powers of national data protection authorities. What should the mixture of education, 'policing', complaints handling and policy activity? Whilst some degree of diversity between national data protection authorities is healthy and perhaps inevitable, the Commissioner recognises that the current situation can be confusing for data controllers that operate internationally – are they dealing with a tough policeman or a helpful educator in any particular country? It would be helpful if a future legal framework could do more to clarify what features and characteristics a modern data protection authority should have. In particular, the Information Commissioner is of the opinion that the role of the national authority as educator must be maintained as an explicit part of any modernised Convention.

Transborder data flows

27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further

² See section 59 of the DPA 98 for the details.

developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

28. Do we need to reconsider the notion of “transborder data flows” altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

This is one area that most needs to be amended to deal more realistically with current and future international dataflows. A modernised Convention should focus much more on risk assessment by the exporting data controller and should be clearer about data controllers’ responsibility, wherever they choose to process personal data. The ICUK has doubts about a concept of adequacy based substantially on the nature of the law in place in a particular territory. Adequacy should be assessed more in relation to the specific circumstances of the transfer and less on the adequacy or otherwise of the law of the country the recipient is established in. Clearly the law in place in the recipient country is a factor, but it should not be the principal means of determining the adequacy of a transfer.

The current system for determining whether a third country has an adequate level of data protection is slow and cumbersome, and only a few countries have to date achieved an adequacy finding. This system may still be part of the solution in the future legal framework, but it needs to be a quicker and simpler process. The Convention should also reaffirm the position that the test is adequacy, not equivalence. However, findings of adequacy should not be the only option; there need to be more flexible solutions for recognising the adequacy of organisations or sectors in non-adequate countries. For example, those signed up to recognised industry codes of practice, or self-regulatory systems. There is also a link here to the points made on accountability, with the possibility that properly accountable organisations in third countries could be deemed adequate for the transfer of personal data.

29. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

The ICUK favours a system under which methods of transfers, not transfers by individual businesses, are approved. Any approval of a

method of transfer (such as contractual clauses, BCR) should be underpinned by a legally established system of mutual recognition.

In terms of whether the public and private sectors have differing rules, this becomes ever more difficult in a world where the public sector increasingly engages the private sector to deliver services, and where public sector practice increasingly draws on private sector experience. The ICUK's experience suggests that having different methods to ensure adequacy is beneficial, but it should be left to the controller to determine which method they consider to be most appropriate for determining adequacy.

Role of the consultative committee

30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

While the ICUK considers this to be generally beneficial, the role of the consultative Committee must not place additional burdens on Member States and/or national authorities. There are several supra-national bodies in existence that may set standards, resolve disputes and monitor functions, and the European Commission's data protection strategy points to reforming the Article 29 Working Party to perform some of these roles.

Any revised role of the consultative committee must avoid duplication of effort or contradictory standards.

March 2011