The Information Commissioner's (United Kingdom) response to

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.

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 the DPA.

The ICUK welcomes the opportunity to respond to the European Commission's Communication on the future data protection strategy. The ICUK has been very active in this area over the last 2 years, with the publication of the RAND Europe review of the Data Protection Directive[1], which was commissioned by the ICO, through to the ICUK's response to the European Commission's consultation on the legal framework for the fundamental right to the protection of personal data. He was also involved in the Article 29 Working Party's joint contribution to the same consultation. The ICUK also responded substantively to the UK Ministry of Justice Call for evidence on the data protection legislative framework in October 2010[2].

Each of these contributions to the debate highlighted a number of aspects of Directive 95/46/EC (the EU Directive) which the ICUK considers need to be addressed to make any future legislative framework for the protection of personal data more effective. This response will lay out the ICUK position on the points raised in the Commission's communication.

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

- be clear in its scope, particularly in the context of new forms of individual identification;

[1] Available at: http://www.ico.gov.uk/~/media/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.ashx

[2] ICUK response available at http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Notices/response_to_moj_dpframework.ashx

- 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 law that has these features. The ICUK intends to provide a general response to the introduction and then to take each of the five key objectives outlined in part 2 of the Commission's communication and provide his response to each in turn.

Section 1. New challenges for the protection of personal data.

The ICUK welcomes the Commission's conclusion that the "core principles of the Directive are still valid and that its technologically neutral character should be preserved". The Commission's review has also identified a number of areas that have been identified as problematic and posing specific challenges. These are:

- Addressing the impact of new technologies.

In the ICUK's opinion, a future framework must deal better with the new forms of identification that are coming into being all the time, particularly in the online environment. It is clear that information such as IP logs held by search engines are being used to identify individuals and to take action affecting them, in contexts ranging from behavioural advertising to digital rights management or national security. It is clear that data protection safeguards ought to apply to this sort of information. However, we have to be realistic about how such information is treated under the law, what standards we expect those processing it to reach and what outcomes we are seeking for the individual. Whilst we may want this information to be kept secure and protected from inappropriate disclosure, it may be impossible in practice to grant conventional subject access to it or to expect individuals to consent to its processing. The ICUK hopes that a future framework will treat this sort of information realistically, perhaps recognising that a simple 'all or nothing' approach to the application of data protection requirements no longer suffices, given the breadth of information now falling within the definition of personal data.

- Enhancing the internal market dimension of data protection.

The ICUK welcomes greater harmonisation between the national regimes as they currently stand, and recognises that the divergence between regimes creates burdens for data controllers who are established in more than one Member State and confusion for those individuals who conduct their affairs in more than one Member State, for example in e-commerce or travel contexts. A benefit of greater harmonisation between data

protection regimes would be the possibility of greater mutual recognition between Member States.

One of the greatest burdens for data controllers is having to gain prior approval for certain processing operations in many Member States, be it for international transfers or in the context of prior checking of other processing operations. Often Member States are looking at the processing not just on the basis of the provisions of the EU Directive, but also on the basis of national data protection provisions that might have a basis in law that pre-dates the Directive, or on the basis of constitutional provisions for privacy that go further than the Directive.

These provisions were precisely the reason that the EU Directive was necessary, to provide a common, appropriately high level of data protection while facilitating the free movement of personal data within the EU. Any new legislative instrument will need to address the barriers to harmonisation and mutual recognition if it is to avoid the current burdens to business continuing.

The ICUK would also stress the need for reducing current provisions in the EU Directive that necessitate compliance on paper without actually contributing to effective protection for individuals. At the same time, introducing new obligations which do not in themselves increase the standard of protection for personal information should be avoided at all costs. Those who might not agree with high standards of personal data protection should not be able to portray the law as "unnecessary box ticking".

- Addressing globalisation and improving international data transfers.

This is one of the aspects of the EU Directive that most needs to be amended to deal more realistically with current and future international data-flows. 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 from the EU Commission. 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 future legal framework should also reaffirm the position that the test is adequacy, not equivalence.

- Providing a stronger institutional arrangement for the effective enforcement of data protection rules.

The ICUK welcomes the Commission's conclusion that the role of the national data protection authorities needs to be strengthened. There should also be some consideration as to how the ex-Third Pillar bodies can be better brought into the institutional framework of the Article 29 Working Party, particularly as the members of these bodies are drawn mainly from national data protection authorities.

- Improving the coherence of the data protection legal framework.

This is often characterised as "harmonisation" of the data protection regimes at national level. However, the ICUK considers that for there to be greater coherence of the data protection legal framework, there must also be an obligation of mutual recognition of the national data protection regimes between Member States. Mutual recognition is also important to the provision of stronger institutional arrangements for the effective enforcement of data protection rules.

Section 2. Key objectives of the comprehensive strategy on data protection

2.1. Strengthening individuals' rights

There is a question of how individuals in one Member State assert their rights and freedoms when information is being used in another Member State. Currently there is a level of co-operation between national data protection authorities, but this can be slow and cumbersome and does not fit well with either strengthening individuals' rights or improving the coherence of the data protection legal framework. Again, greater harmonisation and mutual recognition of data protection law between Member States would help, but a mechanism needs to be put in place to facilitate the handling of complaints across EU or EEA jurisdictions. This could be part of a wider review of the role and functions of the Article 29 Working Party.

The ICUK broadly welcomes the proposal to increase transparency as part of a revised data protection legislative framework. However, he has some questions about how some of the particular suggestions will work in practice.

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 a future Directive 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 EC. 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 new data protection directive 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 in a new Directive. 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.

The ICUK considers that much more can be done to harness technology to deliver improved rights for individuals, for example, online access to their personal information. Again, a future framework should do more to update and strengthen individuals' rights, particularly in terms of subject access and the way increasingly complex information systems are explained to the public.

The ICUK welcomes the proposal to clarify the rules on consent as there is confusion about consent under the current legislative framework. This takes the form of confusion between transparency and consent, confusion as to whether consent can be opt out, as well as opt in, and a common misunderstanding that consent is always necessary before processing of personal data can begin. The confusion about consent exists for both data controllers and data subjects.

Articles 10 and 11 of the EU Directive deal with information given to the data subject, commonly referred to as transparency; Article 7 refers to consent. In addition, Article 6 of the Directive says that personal data must be processed fairly and lawfully. There is general acceptance among data protection authorities that fairness has two main elements: transparency and consent. However, 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 across Europe, can confuse individuals and cause great practical uncertainty for data controllers. In many cases it is not clear where consent is necessary or where transparency suffices. This can lead to unrealistic presumptions about the degree of control that individuals should enjoy, perhaps in cases where choice may not be a realistic option or where individuals may neither expect nor want to choose.

This can be a particular issue in justice, home affairs, law enforcement and other public sector contexts. Any future legal framework should be realistic about the extent of choice that individuals can actually have and the degree of choice they actually want. In online contexts it is particularly important, therefore, that browser and website defaults are set in a way that balances functionality and privacy protection appropriately. A requirement for consent can be an important protection for individuals but it should be reserved for situations where an individual genuinely has a free choice as to whether or not to agree to the processing of their personal data.

Any new legislative framework should be clear about what consent actually entails, and whether and when explicit consent is necessary. In particular, the Commission should consider the issue of whether separate 'informational' consent is required where the processing of personal data is necessary for a service or transaction that an individual has entered into voluntarily. The Commission may be aware that the Key Provisions Subgroup of the Article 29 Working Party is currently working on an opinion on consent.

Consent is of particular relevance when we consider the "right to be forgotten". It is important that the Commission is clear about the extent to which this right can be effective in practice, as it could have a very limited application. In many cases, in particular where personal data are being used by public authorities, there is a legislative basis for the processing and the right to object, as currently exists, is limited. Where an individual has provided consent and this is the sole condition for making processing of personal data legitimate, then this can be withdrawn. However, in some cases, such as where the personal data are processed for the purposes of direct marketing, current good practice would require the data controller to keep a record of those individuals who do not wish to receive marketing, so that any marketing lists obtained after the objection has been received can be checked against this record. It is important that the future legal framework does not mandate deletion of personal data where suppression is what actually delivers privacy protection or rights for individuals.

The ICUK can see some situations where the "right to be forgotten" 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 be forgotten" 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. The ICUK therefore welcomes the Commission's proposal to clarify the "right to be forgotten".

The treatment of "sensitive" or "special categories" of personal data is an area of the legislative framework that the ICUK considers does not work well in practice. The categorisation was clearly an attempt to afford special protection to the sorts of data that could have the most negative impact on individuals if used inappropriately. For example, information about trade union membership has been used against individuals living under the various totalitarian regimes that have existed in Europe. Although the rationale for categorising certain types of data as "sensitive" is easy to understand, there are several practical problems.

First, the Directive's special categories of data may not match what individuals themselves consider to be 'sensitive'. To use the example above, many trade unionists living in relatively stable, democratic

societies probably wouldn't consider information about their membership to be sensitive, or believe that its existence leaves them open to particular threats, despite this information being misused in certain circumstances, such as the Consulting Association's vetting database[3]. However, many individuals would probably consider their personal finances or, in some circumstances, information about their location to be very sensitive. This shows that there can be a mismatch between what the law says and what people believe to be "sensitive". The difficulty with defining a set list of categories of what constitutes "sensitive personal data" is that it is a very subjective judgement, based entirely on the cultural or social mores at the time. This can lead to certain categories of data which might otherwise be considered sensitive falling outside the definition of sensitive personal data. There is also the danger that the list may be different in jurisdictions outside the EU, leading to multinationals to cope with different lists of sensitive personal data in a range of countries.

Just one example of this can be found in a draft discussion Bill that was put forward in the USA earlier this year[4]. This Bill defined "sensitive information" by a list of categories, some of which overlapped with those categories in the current EU legislative framework. However, other categories, such as precise geolocation information and financial data, were counted as "sensitive" (as an aside, biometric data was not considered to be "sensitive" in the draft Bill). This demonstrates the difficulty in defining "sensitive personal data" as a list of categories, as opposed to defining it against the impact, or potential impact, of the processing of the data has on the individual.

Second, there is the issue of context. As it stands, certain types of data are deemed to be special regardless of what the precise information is, who it is held by or what it is used for. Clearly, many individuals would consider their health data to be sensitive, but is a record kept in a manager's file recording that an employee was absent from work because he or she had a cold particularly sensitive in any real sense?

The way the EU Directive is structured means that where special categories of data are involved, their processing is prohibited unless one of a number of conditions applies. This has led to cases where legislation has had to be created in Member States to provide an explicit legal basis for carrying out otherwise unobjectionable processing. This has happened several times in the UK, and, we gather, in other countries too. The ICUK's view is that the rigid categorisation of special categories of data is not an effective way to allow acceptable processing but prohibit the unacceptable. We need a more flexible and contextual conception of

[3] For further information, see the enforcement notice issued by the Information Commissioner to the Consulting Association, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/notices/tca_enforcement_notice.pdf

[4] A Draft of a Privacy Bill was presented before the House of Representatives in the USA on 4 May 2010 by US Representatives Rick Boucher and Cliff Stearns. A full draft of the Privacy Bill can be found at http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf

sensitivity, which could, depending on the circumstances, extend to any type of personal data.

The ICUK suggests a definition based on the concept that information is sensitive if its processing could have an especially adverse or discriminatory effect on particular individuals, groups of individuals or on society more widely. Any future definition might state that information is sensitive if the processing of that information would have the potential to cause individuals significant damage or distress. Such an approach would allow for flexibility in different contexts, so that real protection is given where it matters most. In practice, it could mean that the current list of special data categories remains largely valid, but it would allow for personal data not currently in the list to be better protected, for example financial data or location data. Or, more radically, the distinctions between special categories and ordinary data could be removed from the new framework, with emphasis instead on the risk that particular processing poses in particular circumstances.

It is important to give a message to data controllers that a simply binary (special categories – the rest) approach is not good enough, and they must consider the context in which they hold information and the risk this poses to individuals. In the context of a revised legal framework national data protection authorities or EU-level bodies, such as the Article 29 WP, could produce guidance with examples that could help organisations to assess genuine sensitivity in various contexts. Regulation of misuse of "sensitive" data in this way would be in line with the ICUK's current risk-based approach to regulation.

The implementation of the current EU Directive 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 be? Whilst some degree of diversity between national data protection authorities is healthy and perhaps inevitable, the ICUK 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 ICUK is of the opinion that the role of the national authority as educator must be maintained as an explicit part of any new legislative framework.

There is also a need to be realistic about the functions data protection authorities are expected to carry out, against a backdrop of limited resources and increasing demand for their services. Again, a future framework could do more to help data protection authorities to focus on areas of particular privacy risk, rather than requiring them to 'police' every aspect of the processing of personal information. As explained above, a future framework should encourage data protection authorities to focus more on outcomes, rather than encouraging them to see compliance with the law as an end in itself, even where non-compliance does not put privacy significantly at risk.

Finally there is a need for any new EU data protection legislation to recognise that it is not always the data controller that is responsible for breaches of data security or privacy of the individual. It is well documented that often it is individuals working for the organisation who, either through malign intent or by mistake, act against robust policies and procedures put in place by the data controller to protect personal information. In the UK, this is dealt with by provision in the DPA to prosecute those individuals who knowingly or recklessly obtain or disclose information without the consent of the data controller. But even in the UK, the maximum sanction for this offence is a fine. This situation has come in for some criticism in the Courts and the ICUK and his predecessors have been advocating the introduction of custodial sentences for some time. Should the Commission be considering the introduction of criminal sanctions as part of a new legislative framework then consideration must be given to the introduction of sanctions that are a real deterrent to the unlawful trade in personal information and that can be applied against individuals who are acting maliciously.

2.2. Enhancing the internal market dimension

The ICUK welcomes the fact that while the Commission's proposal seeks to enhance the protection of personal privacy in data processing, it also sees the value in enhancing the internal market dimension of the data protection legislative framework. However, the ICUK is disappointed that the Commission has not included any undertaking to examine the definitions of "data controller" and "data processor" as they exist in the current EU Directive. This may be difficult but that does not mean it should be avoided.

There can be a lack of clarity and certainty in determining which is the "data controller" and which is the "data processor" in relationships between organisations that process personal information. The complexity of modern business relationships means that there are numerous 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 definitions as to what constitutes a "controller" or "processor" in the EU Directive. One area of confusion is what is meant by determining the "means" of processing. The ICUK sees the revision of the legislative framework as an opportunity to remove uncertainties surrounding definitions.

It should be a prerequisite that in revising any of the current obligations on data 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. Possibilities mooted in the Commission's communication include the mandatory recruitment of a data protection officer, obligations to carry out a data protection impact assessment, the promotion of privacy enhancing technologies and mandatory breach notification.

The ICUK considers that, in the right circumstances, these possibilities can significantly enhance data protection. However, the introduction of any of these measures, either individually or collectively, will increase the burden of data protection law on the data controller. As such, there must be a sound evidential base that demonstrates that each of these measures will have a significant impact on the protection of personal data, and they must be framed in such a way as to avoid becoming merely ways of complying on paper, with no substantive effects on information privacy in practice.

It is also important that the Commission approaches each of these proposals flexibly, determining where the maximum benefit to individuals can be drawn for the least burden on data controllers. For example, the Commission may wish to consider placing an obligation on certain categories of data controller to have a publicly available breach notification policy, rather than mandatory breach notification, or place an obligation on data controllers to consult with national data protection authorities at the beginning of projects which might present substantial risks, rather than mandate a data protection impact assessment in every case.

As already stated, the ICUK considers that harmonisation is an important step in reducing the burdens on data controllers, but this is in itself not sufficient to reduce the burdens on data controllers unless it is accompanied by an obligation of mutual recognition on Member States.

While the ICUK welcomes the proposal to reduce the administrative burden of notification by data controllers, he would urge caution in how this is done in practice. In the UK, notification of data processing by data controllers also attracts a fee, which is paid directly to the ICUK to fund data protection supervision. This effectively makes the ICUK's supervision of data processing self-funding, and underpins the independence of the ICUK as he does not need to rely on funding from the UK Government. Any new proposals on notification must leave this possibility open at national level.

The Article 29 Working Party is currently preparing an opinion on possible new notification regimes which is due to be published later this year. The ICUK would encourage the Commission to examine this opinion as part of their consideration of any new notification regime. In particular, we urge the Commission to consider how it can best strike the balance between an administratively 'lite' notification system and one that provides genuine benefit to individuals, regulators and others.

The ICUK would like the Commission to consider a fee-based funding model for all data protection authorities, which would facilitate independence and ensure they have sufficient resources to carry out their tasks, including those that will be required under the new legal framework. It is not essential though that any fee-based model is directly linked to the current notification obligations.

The fee would be based on the 'polluter pays' principle, in that those processing personal data are the ones who make it necessary for there to be a system of supervision, regulation and advice and guidance services provided by data protection authorities, and they therefore are the ones who should pay for it. There are various mechanisms to collect a fee – in conjunction with registration; or by introducing a requirement for a 'licence' for an organisation to process personal data.

The experience of the ICUK has shown that the fee-based funding model works. It strengthens the data protection authorities' independence from Government. The fee-based funding model substantially reduces the risk of government interference in how the data protection authority operates, sets its priorities, and allocates its resources, including the ability to recruit staff.

This model also means the ICUK has been spared reductions in funding for its data protection work, in contrast to its freedom of information work which is funded by a government grant which is being reduced. The ICO continues to be relatively well funded for its data protection work. This model undoubtedly allows the ICUK to raise more revenue than it would receive if it had to rely on Government funds. An increase in budget through using this model would allow data protection authorities to achieve far more and ultimately to be more effective, and would allow them to continue their role and tasks without being unduly affected by the financial position and priorities of their national government.

While data protection authorities would need to administer this fee, which will take human and financial resources, the costs could be kept to a minimum through online and automated systems, such as direct debit payment of fees. In any case the increase in overall budget from the fee model would more than cover these additional costs.

Of course it is also important that should the future legal framework not explicitly provide for the possibility of a fee-based funding model, it should certainly not preclude it. Were it to do so, those data protection authorities currently relying on fee income would be likely to suffer damaging reductions in their funding and a lessening of their independence.

Finally, the ICUK welcomes the communication discussion on the introduction of an examination of the "accountability principle". It is important that an accountability principle does not become an unwarranted bureaucratic burden on data controllers. The accountability principle should be based on the assumption that data controllers must have the freedom to design their own approach to compliance – legislation should merely set the standards they have to achieve and not prescribe in detail how this should be done. The ICUK strongly supports the concept of accountability becoming part of the data protection legislative framework, but the law must be clear on what such a principle is there to achieve.

The accountability requirement should not impose any additional burden on data controllers that take their responsibilities seriously, but should

emphasise, on the face of the legislation, 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 data 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 sized 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 DP regimes outside Europe including the OECD privacy guidelines, the APEC privacy framework, and Canada's PIPEDA law. Its introduction as a principle in the EU legal framework would promote global harmonisation of DP requirements and could contribute to reducing the administrative burden imposed by the current rules on international data transfers.

2.3. Revising the data protection rules in the area of police and judicial cooperation in criminal matters

The ICUK welcomes the proposal to consider the extension of general data protection rules to the areas of police and judicial cooperation in criminal matters. UK data protection law already applies to these areas, albeit with appropriate exemptions which allow police and judicial services to operate effectively.

The ICUK will respond more substantively to the proposed consultation on these matters in 2011. However, the ICUK would point out in the meantime that the basis of the revision should recognise where the subsidiarity principle should apply. Any new supervisory arrangements should distinguish between those ex-third pillar systems that have their own specific data protection provisions(lex speciales) and that extend to databases that exist in each Member State with domestic data controllers, (e.g. the Customs Information System), and those arrangements where the subsidiarity principle does not apply, such as those bodies that are European institutions and have processing activities that are more suited to a single European level regulator (e.g. Europol).

A related point is that any review should recognise that there is no single "European" way of supervising the processing of personal data in the areas of police and judicial cooperation in criminal matters. Each of the current means of supervision, be it a formal joint supervisory body, an obligation of coordinated supervision, or a single supervisor, have their advantages and disadvantages. The review should recognise this and not necessarily aim for a "one size fits all" approach.

2.4. The global dimension of data protection

This is one of the aspects of the EU Directive that most needs to be amended to deal more realistically with current and future international data-flows. A future framework 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.

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 from the EU Commission. 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 future legal framework should also reaffirm the position that the test is adequacy, not equivalence. However, EU Commission 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.

To the extent that the current provisions of Article 26(2) of the Directive, which relate to authorisations of transfers where the controller determines there are adequate safeguards, and which reference contractual clauses, are retained, the ICUK suggests adding the option for the Article 29 Working Party to approve other mechanisms. 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.

2.5. A stronger institutional arrangement for better enforcement of data protection rules

The ICUK welcomes the Commission's proposal to strengthen, clarify and harness the role and function of the Article 29 Working Party. In particular, the proposal that the Article 29 Working Party becomes a more transparent body is welcome.

There are a number of points that need to be kept in mind when re-examining the role and function of the Article 29 Working Party, and the role of the national data protection authorities as Working Party members. Independence of national data protection authorities is one important aspect of their function and should not be compromised in any new framework. Whilst the ICUK supports the idea that the Article 29 Working Party should have a greater coordinating role, it is important that this is focussed on issues that have a significant cross-border dimension and that

it does not compromise the independence of national data protection authorities.

Another important aspect to consider is how the current arrangements for supervision of data protection in the areas of police and judicial cooperation in criminal matters become part of any stronger institutional arrangement for better enforcement of data protection laws.

Finally, at several points in this submission the ICUK has made the point about mutual recognition being an important part of any new data protection regime. This has been relevant to a number of areas but is of particular relevance to having a stronger institutional arrangement for better enforcement of data protection rules. An obligation of mutual recognition would facilitate cross border co-operation between national data protection authorities, as it would allow certain authorities to become lead authorities in cross-border investigations.

Issues not raised in the Commission communication

The ICUK is disappointed that there was no mention in the communication about clarifying the scope of any new data protection legislation. For example, there was no discussion on clarifying the rules surrounding the use of data for domestic purposes, of particular importance in an online world.

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 law?

The ICUK was also surprised that the communication made no reference to the importance of codes of practice or other forms of soft law. In considering the future legislative framework, the ICUK would hope that the overarching legal instrument, whether a Directive or a Regulation, is pitched at a high level and based on general principles. Matters of more detail, for example any provisions relating to the processing of data on children, are best left for development in the context of softer law where they can be given more in-depth consideration and the needs, legal systems and cultures of different Member States can be taken fully into account. If the Commission is serious about achieving greater harmonisation without imposing disproportionate burdens on businesses and others, soft law, whether in the form of codes of practice or perhaps opinions of the Article 29 Working party that carry some legal weight, is a realistic way to achieve this. For example, the Commission will be well aware of the important, but difficult work that the Article 29 Working Party has done in developing opinions to help harmonise the application of the definitions in the existing Directive. The ICUK hopes that the Commission will take a suitably imaginative approach to the form of the future legislative framework.

Conclusion

The ICUK is grateful to the Commission for providing an opportunity to comment on the communication well in advance of the publication of proposed legislation in 2011. The ICUK will continue to feed into the Commission's thinking as it develops and will continue to contribute to the development of new data protection legislation through his role on the Article 29 Working Party and through further consultations proposed by the Commission throughout 2011.