

The future of data protection in the EU Briefing from the UK Information Commissioner's office

This briefing is to inform stakeholders about the upcoming proposed changes to the EU data protection legal framework and the ICO's views on some of the expected proposals. The European Commission has indicated they will publish their proposal by the end of January 2012 and this briefing outlines what the ICO would like to see in any future legislation.

Scope: an effective new data protection framework must be overarching, clear in scope and easy to understand and apply

- The new framework should consist of high-level principles with the detail in implementing measures, codes of practice and other mechanisms.
- It should be a single, overarching framework applying to all the processing of personal data carried out in the EU, complemented with a set of more specific rules dealing with particular areas, for example, electronic communications or law enforcement.
- The scope should be clear, particularly in the context of new forms of individual identification, the online world and the transparency agenda.
- Rather than a list-based prescriptive approach, the definitions (such as sensitive data and risky processing) and the obligations on organisations should focus on risk, context and purpose.
- The framework should place clear responsibility on and require accountability by those processing personal data, throughout the information life cycle, including applying obligations directly to data processors.
- It should contain more clearly defined exemptions for domestic purposes and journalism that are fit for Web 2.0 and beyond, specifically taking account of societal and technological changes (such as social networking and citizen journalism and blogs).

Rights: individuals should have clear, effective rights and simple, low-cost means of exercising them

- The framework should strengthen individual rights to object to and block processing, and to have their data deleted, and reverse the burden of proof so the organisation has to provide compelling legitimate grounds for continuing processing.
- It should not introduce a stand-alone 'right to be forgotten' which could mislead individuals and falsely raise their expectations, and be impossible to implement and enforce in practice. There are implications for freedom of expression and questions as to how far individuals should be able to rewrite their own or others' history.
- It should be easier for individuals to exercise their rights: through using technology to provide subject access; being able to move their data around and have it in a reusable format; being able to use alternative dispute resolution; and being able to take complaints to whichever relevant regulator can serve them best.

- The framework should clarify the relationship between transparency and consent and be realistic about the levels of individual control, both in terms of what is possible and what is desirable.

Obligations: organisations should be responsible and accountable

- The framework should be less prescriptive in terms of the processes we expect organisations to adopt, but clearer in terms of the standards we expect them to reach. For example, obligations on organisations to have good information management and to demonstrate compliance and accountability, without prescriptive lists of measures to take or how to demonstrate compliance and accountability.
- Any general obligation associated with PIAs should only be to consider whether one is required. Organisations should carry out a PIA where processing has or could have a significant or adverse impact on the individual; uses intrusive technology; or the purpose of the processing creates a particular risk.
- Privacy by design should be encouraged as an approach, and encompasses tools such as PIAs. It could also be reflected in requirements to regularly review technology, systems and processes. However, any explicit provisions to compel privacy by design would be difficult to implement and enforce in practice.
- Any provisions for breach notification should follow those of the e-privacy Directive and its implementing measures. Criteria and thresholds for reporting should relate to the level of risk to the individual.
- Information provided to regulators by organisations should be meaningful and a way to demonstrate compliance and accountability (for example, as part of any notification obligation).
- As with all other aspects of a organisation's processing, assessing adequacy for international transfers should be the responsibility of the organisation in the first instance, not the data protection authority.

Data protection authorities: independence, clarity of role, effective powers and flexibility are key

- DPAs should have a role to supervise, enforce, and advise; not to give prior approval or authorisation to organisations' activities.
- DPAs should have powers to take action against any organisation, regardless of their role in the stewardship of the personal data. These powers should include the ability to audit all organisations without consent, not just the public sector.
- DPAs should co-operate and share information with each other, but remain independent with the flexibility to carry out their role according to their own strategy and as appropriate to the national situation. For example, as regards deciding priorities; what complaints to take forward; what sanctions to impose.
- The UK should continue to be able to use a fee-based funding model for the regulator, based on the 'polluter pays' principle, even if it is not linked to notification.

More information

The European Commission communication of 4 November 2010 set out the following objectives for the revision of the data protection Directive 95/46/EC.

- **Strengthening individuals' rights** so that the collection and use of personal data is limited to the minimum necessary. Individuals should also be clearly informed in a transparent way on how, why, by whom, and for how long their data is collected and used. People should be able to give their informed consent to the processing of their personal data, for example when surfing online, and should have the "right to be forgotten" when their data is no longer needed or they want their data to be deleted.
- **Enhancing the Single Market dimension** by reducing the administrative burden on companies and ensuring a true level-playing field. Current differences in implementing EU data protection rules and a lack of clarity about which country's rules apply harm the free flow of personal data within the EU and raise costs.
- **Revising data protection rules in the area of police and criminal justice** so that individuals' personal data is also protected in these areas. Under the Lisbon Treaty, the EU now has the possibility to lay down comprehensive and coherent rules on data protection for all sectors, including police and criminal justice. Naturally, the specificities and needs of these sectors will be taken into account. Under the review, data retained for law enforcement purposes should also be covered by the new legislative framework. The Commission is also reviewing the 2006 Data Retention Directive, under which companies are required to store communication traffic data for a period of between six months and two years.
- **Ensuring high levels of protection for data transferred outside the EU** by improving and streamlining procedures for international data transfers. The EU should strive for the same levels of protection in cooperation with third countries and promote high standards for data protection at a global level.
- **More effective enforcement of the rules**, by strengthening and further harmonising the role and powers of Data Protection Authorities. Improved cooperation and coordination is also strongly needed to ensure a more consistent application of data protection rules across the Single Market.

Glossary

- **Article 29 Working Party**: EU member states all have an independent data protection authority (DPA) for data protection that meet regularly under article 29 of Directive 95/46/EC on data protection.
- **Data controller**: someone (usually a business) who controls the use of personal data.
- **Data processor**: processes personal data for the data controller (not an employee of the data controller).
- **Data protection authority (DPA)**: the national regulator for data protection
- **Directive 95/46/EC on data protection**: The 1995 directive which forms the basis of all member states' data protection law, including the UK Data Protection Act.

- **Information Commissioner's Office (ICO):** UK's independent regulator for data protection and freedom of information legislation.
- **Prior checking:** some DPAs must give prior approval to organisations before processing can start. This is not the practice in the UK.
- **Privacy by design (PbD):** thinking about privacy at the start of processing, and building it into projects, systems and designs.
- **Privacy impact assessments (PIAs):** a tool for organisations to assess the privacy and data protection impact of their processing and identify measures to mitigate risks.

Links

European Commission communication – 4 November 2010

http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

ICO response to the European Commission consultation 2009

http://ec.europa.eu/justice/news/consulting_public/0003/contributions/public_authorities/ico_uk_en.pdf

ICO response to the European Commission consultation 2010

http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/ico_infocommoffice_en.pdf

ICO response to the Ministry of Justice's call for evidence on the current data protection legislative framework 2010

http://www.ico.gov.uk/about_us/consultations/~media/documents/library/Data_Protection/Notices/response_to_moj_dpframework.ashx

ICO privacy impact assessment handbook

http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/0-advice.html

ICO guidance on security breach management

http://www.ico.gov.uk/for_organisations/data_protection/~media/documents/library/Data_Protection/Practical_application/GUIDANCE_ON_DATA_SECURITY_BREACH_MANAGEMENT.ashx

ICO guidance on reporting breaches

http://www.ico.gov.uk/for_organisations/data_protection/the_guide/~media/documents/library/Data_Protection/Practical_application/BREACH_REPORTING.ashx