MEMO/10/542

Brussels, 4 November 2010

Data protection reform – frequently asked questions

Why does the EU need to revise its approach to data protection?

The 1995 Data Protection Directive (95/46/EC) set a milestone in the European Union's history of protecting personal data. It aims to protect people's fundamental rights and freedoms – in particular the right to data protection – as well as ensuring the free flow of data within the Single Market.

While the Directive's core principles remain valid, modern technology and globalisation pose new challenges to data protection. These changes have led to questions on whether the existing EU data protection legislation can still fully and effectively be relied on or whether a reform is needed. To address these issues, the Commission consulted the public in 2009 and stakeholders throughout 2010.

The Commission concluded that the EU needs a more comprehensive and coherent approach to its policy on the fundamental right to personal data protection. For example, the Data Protection Directive does not cover police and criminal justice cooperation. Following changes brought by the Lisbon Treaty, the EU can now adopt comprehensive rules on data protection covering all EU policies, including police and judicial cooperation in criminal matters. Under the review, data retained for law enforcement purposes should also be covered by the new legislative framework.

What are the challenges of modern technology to data protection?

High-speed internet, web-connected mobile devices, and user-generated content have made the exchange of information easier, faster and global. These changes have pushed individuals to the forefront when it comes to the "management" of their personal data, requiring policy makers to shift their focus. Social networking sites – based on personal data processing – have become extremely popular on a global scale, particularly among young people. A single social network service now counts half a billion users globally – as many as the entire EU population. The benefits of this technology to individuals, businesses and public authorities must go hand in hand with the necessary respect for personal data. Individuals' personal data must be effectively protected, whatever the technology used.

What is the added value of EU action in this field?

Data does not stop at national borders. As a result, citizens and businesses need common, harmonised rules to protect their personal data and ensure that it flows freely throughout the EU. A unified approach at EU level will make Europe stronger in promoting high data protection standards globally.

How will the new approach help individuals?

The new approach will strengthen individuals' rights by giving them a high level of protection and control over their own data.

This is particularly important in the online environment, where data protection policies are often unclear, non-transparent and not always fully compliant with existing rules. Individuals need to be informed in a clear and transparent way by data controllers – either internet services providers, search engines or others – about how and by whom their data is collected and processed. They need to know what their rights are if they want to access, rectify or delete their data. People should be able to exercise these rights for free and without constraints.

For example, there should be a "right to be forgotten," which means that individuals should have the right to have their data fully removed when it is no longer needed for the purposes for which it was collected. People who want to delete profiles on social networking sites should be able to rely on the service provider to remove personal data, such as photos, completely.

Similarly, users should know and understand about how their internet use is being monitored for the purposes of behavioural advertising. For example, people should be aware when online retailers use previously viewed web sites as a basis to make product suggestions.

It is also important that individuals are informed when their data has been unlawfully accessed, altered or destroyed by unauthorised persons. The Commission is therefore considering extending the obligation to notify personal data breaches beyond the currently covered telecommunications sector to other areas, such as the financial industry.

How will individuals and companies benefit from the consistent implementation of data protection rules?

The current divergent implementation of data protection rules across the EU raises costs and administrative burdens for data processing companies. Data Protection Authorities in the different Member States do not always have the same approach when applying the Data Protection Directive. The result is that a multinational company operating in several countries can be subject to different requirements in several Member States which leads to legal uncertainty.

Further harmonisation of data protection rules is needed at EU level to ensure a true level playing field for all data controllers. To lessen the administrative burden, notifications to Data Protection Authorities could be reduced, simplified and harmonised.

At the same time, data controllers should implement effective policies to ensure compliance with the EU data protection rules, such as appointing Data Protection Officers, carrying out Privacy Impact Assessments and applying a “Privacy by Design” approach, which means that privacy issues are taken into account when products and services are under development.

What are the implications for national authorities?

In principle, the same data protection rules apply to both the public and private sectors. This means that national authorities have to comply with the obligations in relation to transparency and controllers' responsibility, taking into account the specificities of the various sectors, such as the area of police and criminal justice.

What are the implications for national Data Protection Authorities?

Independent national Data Protection Authorities are essential for the effective enforcement of data protection rules. The Commission believes that their role should be considerably strengthened, and that they should be provided with the necessary powers and resources to properly exercise their tasks both at national level and when co-operating with each other.

At the same time, the Commission considers that Data Protection Authorities should reinforce their cooperation and better coordinate their activities, especially when confronted with issues which, by their nature, have a cross-border or an international dimension.

What is the role of the Article 29 Working Party?

The "Article 29 Working Party" is an advisory body established in 1996 by Article 29 of the Data Protection Directive. It is made up of national Data Protection Authorities from the Member States, plus the European Data Protection Supervisor and a Commission representative. The Commission also provides the Working Party's secretariat.

The tasks of the Working Party include, amongst others, examining any question in relation to the implementation of the Data Protection Directive, giving the Commission an opinion on the level of protection in the EU and in third countries, and advising the Commission on measures concerning the protection of personal data.

The Working Party should become a more transparent body and help achieve a more consistency application of EU data protection rules under the authority of the Commission.

Will there be new legislation?

The Commission will propose in 2011 a new general legal framework for the protection of personal data in the EU covering data processing operations in all sectors and policies of the EU. This comprehensive new legal framework will ensure an integrated approach as well as seamless, consistent and effective protection. The European Parliament and the Council of Ministers will then negotiate and adopt the Commission's proposal.

Does this mean the existing rules are no longer relevant?

The principles enshrined in the Data Protection Directive are still sound. However, the rules need to be revised and modernised in order to respond to new challenges and situations.

In any case, until new rules are adopted and enter into force, the current rules remain entirely valid and still have to be correctly implemented by Member States and applied by all those concerned.

What are the other main actions planned?

The Commission will also consider and pursue non-legislative measures, such as promoting awareness-raising campaigns on data protection, encouraging self-regulation and the possibility of EU certification schemes in the field of privacy and data protection.

In addition, the Commission will continue to promote high standards of data protection in third countries and at international level. Consequently, it will step up its cooperation with third countries and international organisations, such as the Organisation for Economic Co-operation and Development (OECD), the Council of Europe and the United Nations.

Is the Commission also reviewing the Data Retention Directive?

The Commission is reviewing the 2006 Data Retention Directive (2006/24/EC), which was adopted to harmonise Member States' different laws on data retention. Under the Directive, companies are required to store communication traffic data for a period between six months and two years. The Commission's current review focuses on whether the type and amount of data is necessary for security reasons and whether the length of time that authorities can hold data is appropriate.

What about data protection in criminal matters? Do authorities need access to this data?

The collection and processing of personal information can be very valuable to secure important and legitimate public interests, such as the prevention, investigation, detection or prosecution of criminal offences. However, this needs to be done in a way that fully respects the requirements of legality, necessity and proportionality, including the possibility to challenge these actions in courts.

The EU needs to ensure that the fundamental right to data protection is consistently applied in all areas, including law enforcement and crime fighting. The establishment of a comprehensive protection scheme does not, however, exclude the need for specific rules for data protection for the police and criminal justice sector.

How can the EU prevent data being misused abroad?

To ensure that personal data is adequately protected when transferred and processed outside the EU, the Commission intends to improve, strengthen and streamline the current procedures for international data transfers, including the so-called "adequacy procedure." Under this procedure, the Commission verifies that a third country ensures an "adequate" level of protection of personal data and allows personal data to be transferred from the EU to that third country.

When data is exported outside the EU, the Commission will ensure that EU citizens enjoy the same rights – including judicial redress – as third country nationals have in the EU.

What is the timetable now?

The public can respond to the Communication until 15 January. The Commission will then translate the objectives and issues raised in the Communication into legislative proposals in 2011. In particular, it will propose legislation to revise and strengthen data protection rules regarding all EU policies, including law enforcement and crime prevention. At the same time, the Commission will pursue non-legislative measures, such as encouraging self-regulation and exploring the feasibility of privacy seals.

As a second step, it will assess whether other legal instruments need to be adapted to the new general legal framework.