Ladies and gentlemen,

I very much welcome this opportunity to speak to you about the review of the EU data protection framework, and more specifically about the proposal for a General Data Protection Regulation, as it was presented by the European Commission on 25 January 2012.

Let me, first of all, explain why the review of the current EU data protection framework is taking place, and secondly, discuss some of the main elements of what is now on the table, to provide the backdrop for today’s discussion.

However, let me say very clearly that I consider the proposal for a General Data Protection Regulation as “a huge step forward” towards a more effective and consistent protection of personal data across the EU, but that there is also a need for clarification and improvement on a number of important details.

For further information on both, I would like to refer to the substantial Opinion of the EDPS on the data reform package, submitted on 7 March 2012, and available on our website, with other relevant documentation. This also includes an Opinion of the Article 29 Working Party adopted on 23 March 2012.
Drivers of EU Review

So, why is this review taking place? This is basically for three reasons. The first reason is that there is a need to update the current framework, and more specifically Directive 95/46 which is the key element of the framework. And "updating" means in this case, most of all, ensuring its continued effectiveness in practice.

When the Directive was adopted, the Internet barely existed, and we now live in a world where all this is becoming increasingly relevant, so we also need stronger safeguards that deliver good results in practice. The challenges of new technologies and globalisation really require some imaginative innovation to ensure a more effective protection.

The second reason is that the current framework has given rise to increasing diversity and complexity, if only for the reason that a Directive is transposed into national law – that is its nature – and we now have ended up with 27 versions of the same basic principles. That is simply too much, and translates into costs, but also a loss of effectiveness.

In other words, there is a need to scale up harmonisation, and make the system not only stronger and more effective in practice, but also more consistent. This will lead to a reduction of unhelpful diversity and complexity.

The third reason has to do with the new institutional framework of the EU. The Lisbon Treaty entered into force a few years ago, with a strong emphasis on fundamental rights. Among them a special provision on the protection of personal data in Article 8 of the Charter of fundamental rights, and a new horizontal legal basis in Article 16 TFEU providing for comprehensive protection in all EU policy areas, regardless of whether it relates to the internal market, law enforcement, or almost any other part of the public sector.

So, the review of the framework is all about stronger, more effective, more consistent, and more comprehensive protection of personal data.

If we now look at what is on the table, there is a package of at least two main proposals: a Directive for – briefly put – the law enforcement area, and a directly binding Regulation for what used to be Directive 95/46, applying to the commercial areas and the public sector, other than law enforcement.
This architecture in itself signals that there is a problem with the comprehensiveness of the package. And indeed, if you look more closely, this is where I would see the main weaknesses of the package. The level of protection in the proposed Directive is substantially lower than in the proposed Regulation.

This can be analysed on its own merits, but exchange of data between public and private entities, e.g. law enforcement and banks, telephone, travelling etc is increasing, and a lack of balance will have some practical consequences in a wider field.

**Continuity and change**

But if I now focus on the Regulation, there are some main messages which you need to keep in mind.

The first one is that – in spite of all innovation – there is a lot of continuity. All basic concepts and principles that we have now will continue to exist, subject to some clarification and some innovation. An example of innovation is that there is now a stronger emphasis on data minimisation: i.e. not more data than strictly necessary. Another example is the recognition of “Privacy by Design” as general principle. There is also a clarification of consent: when you need it, it needs to be real and robust consent.

Where the innovation comes in, it is mainly about “making data protection more effective in practice”. This implies, as we will see, a strong emphasis on implementation of principles, and on enforcement of rights and obligations, to ensure that protection is delivered in practice.

At the same time, the Regulation provides for simplification and reduction of costs. A clear example is that prior notification of processing operations has been eliminated. This is only required in situations of specific risks. The Regulation also provides for a one-stop-shop for companies with establishments in different member states. This involves the introduction of a lead DPA.

A directly binding Regulation will of course also bring much greater harmonisation – in principle: one single applicable law in all Member States – and greater consistency. In itself, this will also bring an important simplification and reduction of costs for companies operating in different member states.
**General scope**

Let me also emphasize that the proposed Regulation has a general scope: it will apply both in the private and in the public sector. This is completely consistent with the situation under the present Directive 95/46. The possibility of a systematic distinction in this Directive between the public and the private sector was explicitly considered and rejected.

This comprehensive approach of the present Directive has been feasible, because of the fact that some of its provisions – referring to public tasks – are more relevant for public bodies and other provisions – referring to contracts or legitimate interests – are more relevant for private actors.

The ECJ has clearly explained in its judgment in the Rechnungshof case (May 2003) that the present Directive also applies in the public sector of a member state. However, it also emphasized that national law can only serve as a legitimate ground for processing if it complies with fundamental rights.

This position is only reinforced by the fact that Article 8 of the EU Charter now also provides for an explicit recognition of the right to the protection of personal data, and that Article 16 TFEU provides an explicit horizontal legal basis for the adoption of rules on the protection of personal data, both at EU level and in the member states, when they are acting within the scope of EU law.

At the same time, I have called for a much closer analysis of the relationship between EU law and national law on the basis of the proposed Regulation. The impression that the Regulation will simply replace all relevant national law is not correct. There are at least four different ways in which national law and EU law will co-exist and interact. Among them also the fact that the Regulation will build on national law in much the same way as happened in the Rechnungshof case.

In this context, we should also consider very carefully whether - and if so where and how - the Regulation should allow more space for specification of its provisions in national law. We are currently looking into this question, and we will of course share our conclusions with the Commission, and with the European Parliament and the Council.
Therefore, I would not find it useful to consider a change of the Regulation into two different legal instruments - one for the public sector and another for the private or commercial sector. In any case, let me say very clearly that I see no reason at all to do so.

If we now come to the substance of the Regulation, it is strengthening the roles of the key players: i.e. the data subject, the responsible organisation, and the regulatory authorities.

**User control**
The first perspective could also be seen as enhancing user control. The current rights of the data subject have all been confirmed, but strengthened and extended.

The requirement of consent has been clarified. There is a stronger right to object. There are also stronger means to ensure that the rights of the data subject are respected in practice. There is more emphasis on transparency. There is a provision introducing a collective action, not a class action in US style, but still organisations acting on behalf of their members or constituencies.

There is also much talk about the “right to be forgotten”, but if you analyse this, it is basically an emphasis on deleting data when there is not a good enough reason to keep them. The right to data portability is basically also a specification of the present right to require a copy of any personal data.

**Responsibility**
The biggest emphasis is on real responsibility of responsible organisations. Responsibility is not a concept that only comes at the end, when something has gone wrong. Instead, it comes as an obligation to develop good data management in practice. This appears in language such as *taking all appropriate measures to ensure compliance*, and *verifying and demonstrating that these measures continue to be effective*.

This is one of the major shifts. It also implies that the burden of proof is in many cases on the responsible organisation, i.e. to demonstrate that there is an adequate legal basis, that consent is real consent, and that measures continue to be effective.

The Regulation also provides for a number of specific requirements, such as the need for a privacy impact assessment, the keeping of documentation, and the appointment of a data
protection officer. Some of those provisions, especially on documentation, are in my view overly detailed and would require some modification to make them more appropriate. Some exceptions in the same provisions may not be fully justified. A better balance in this part of the proposal may in fact solve both problems.

A general provision on security breach notification is also included. EU law now provides for such a notification only in the case of telecommunication providers.

**Supervision and enforcement**

A third main emphasis in the Regulation is on the need for more effective supervision and enforcement. The safeguards for complete independence of data protection authorities have been strengthened fully in line with the ECJ judgment in the case *Commission vs Germany*.

The Regulation also provides for regulators with strong enforcement powers in all Member States. Administrative fines of millions of euros - competition size fines – catch a lot of attention, but the message is: if this is important, it should be dealt with accordingly. This will therefore drive "data protection" higher on the agenda of corporate boardrooms, which is welcome.

If we look more closely, we see a practice of more vigorous enforcement, with various means: remedial sanctions, administrative fines, and also some increased liabilities.

International cooperation among data protection authorities is also strongly encouraged and facilitated. The introduction of a lead authority for companies with multiple establishments is welcome, but this lead authority will not be acting on its own, but in fact be part of a network of close cooperation with other competent authorities.

Very important is the introduction of a consistency mechanism in the context of a European Data Protection Board, which is to be built on the basis of the present Article 29 Working Party. This mechanism will ensure consistent outcomes of supervision and enforcement in all member states.

**Global Privacy**

A final element is the wider international dimension of the Regulation, in two ways. The scope of the Regulation has been clarified and extended. These provisions now apply not only
to all processing in the context of an establishment in the EU, but also when from a third
country, goods or services are delivered on the European market, or when the behaviour of
Europeans is being monitored.

As you can understand, this is a reality on the Internet nowadays. At the same time, it is a
realistic approach in my view that builds on an increasing synergy of thinking on data
protection around the world.

Speaking on international aspects, also provisions on trans-border data flows have been
extended and in some ways streamlined and simplified. There is a specific provision now on
Binding Corporate Rules, with also a number of simplifications.

Let me also mention here that international cooperation is developing among data protection
authorities in a wider context – e.g. between the Federal Trade Commission in the US and
DPAs in the EU – in a global network (GPEN). This will make it better possible to deal with
global actors on the Internet. This is also based on a growing convergence of data protection
principles and practices around the world.

*Final remarks*
So, my view is that this is a very welcome proposal, but subject to certain improvements of
some important elements.

Apart from the current lack of balance between the Regulation and the Directive for law
enforcement, I have already mentioned the possible need for more space for interaction
between EU law and national law, and the need to reconsider some of the present exceptions,
including those for small and medium enterprise. In my view, it is *essential* that general
provisions are inherently *scalable*. Inappropriate specifications may only call for unnecessary
exceptions.

Finally, a word on procedure: discussions are now taking place in Council and Parliament.
This will not take a few months. My guess is that we will see some conclusions in the course
of next year, probably under the Irish presidency.
So, in any case by 2014, I would think, this has a good chance of being adopted. I would expect that the Regulation will make it to the end, with some necessary improvements obviously.

Thank you very much.