High Level Conference: "Ethical Dimensions of Data Protection and Privacy"
Centre for Ethics, University of Tartu / Data Protection Inspectorate
Tallinn, Estonia, 9 January 2013

EU Data Protection Law - Current State and Future Perspectives

Peter Hustinx
European Data Protection Supervisor

Privacy and data protection - more precisely: the right to *respect* for private life and the right to the *protection* of one's personal data - are both fairly recent expressions of a universal idea with strong ethical dimensions: the dignity, autonomy and *unique value* of every human being, which also implies the right of every individual to develop his or her own personality and to have a fair influence on matters that may have a direct impact on them.

Privacy and data protection as a specific field of law have been elaborated over the last four decades, notably in the context of the Council of Europe and the European Union, in view of the growing impact of information and communication technology (ICT). That impact is now all around us, every minute of every day, both in our personal and professional lives, and this is likely to increase even further in the near future.

In my remarks today, I would like to discuss the history and current state of the law in this area, as well as the direction in which the law on privacy and data protection might be going to provide a more effective protection, in line with its ethical roots and calling.

In this overview, we will see two main lines: the first having to do with the development of *stronger* privacy and data protection rights as such, and the second with the need to ensure a *more consistent* application of these rights across the EU. Both with a view to promoting

more effective protection in practice and less *unhelpful diversity* in the way such protection is delivered in the different Member States.

Privacy and private life

It was only after the Second World War that the concept of a 'right to privacy' emerged in international law. This happened first in a rather weak version in Article 12 of the Universal Declaration of Human Rights (UN General Assembly, Paris 1948), according to which no one shall be subjected to *arbitrary* interference with his privacy, family, home or correspondence.

A more substantive protection followed in Article 8 of the European Convention on Human Rights (Council of Europe, Rome, 1950), according to which everyone has the right to respect for his private and family life, his home and his correspondence, and no interference by a public authority with the exercise of this right is allowed except in *accordance* with the law and where *necessary* in a democratic society for certain important and legitimate interests.

The mentioning of home and correspondence could build on constitutional traditions in many countries around the world, as a common heritage of a long development, sometimes during many centuries, but the focus on privacy and private life was new, and an obvious reaction to what happened in the Second World War.

The scope and consequences of this protection have been explained by the European Court of Human Rights in Strasbourg in a series of judgments. In all relevant cases, the Court considers whether there was an *interference* with the right to respect for private life, and if so whether it had an *adequate* legal basis - i.e. clear, accessible and foreseeable - and whether it was *necessary* and proportionate for the legitimate interest at stake.

The concept of 'private life' in the case law of the Court is not limited to 'intimate' situations, but also covers certain aspects of professional life and behaviour in public, either or not in the past, where the persons concerned have a reasonable expectation of privacy, but this often applies to special situations, involving sensitive information or inquiries by police or secret services.

Data protection

In about 1970, the Council of Europe concluded that Article 8 ECHR had a number of shortcomings in the light of new developments, notably in the field of ICT: the uncertain

scope of 'private life', the emphasis on interference by public authorities, and the lack of a more proactive approach against the possible misuse of personal information by companies or other organisations in the private sector.

After a thorough preparation, this resulted in the adoption of the Data Protection Convention, also known as Convention 108 (Strasbourg 1981), which has now been ratified by 44 Member States of the Council of Europe, including all EU Member States.

The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection'). The concept of 'personal data' is defined as "any information relating to an identified or identifiable individual ('data subject')".

This means that 'data protection' is *broader* than 'privacy protection' because it also concerns other fundamental rights and freedoms, and all kinds of data *regardless of* their relationship with privacy, and at the same time *more limited* because it merely concerns the processing of personal information, with other aspects of privacy protection being disregarded.

All sorts of activities in the public or private sector are nowadays connected, in one way or another, with the collection and processing of personal information. Protecting individuals (citizens, consumers, workers, etc.) against unjustified collection, recording and exchange of their personal details therefore also concerns their participation in social relations, either or not in public spaces, and this may also entail protecting freedom of expression, preventing unfair discrimination and promoting 'fair play' in decision-making processes.

Structural safeguards

The Convention contains a number of basic principles for data protection to which each Party must give effect in its domestic law before its entry into force. These principles still form the core of any national legislation in this area. According to the Convention, personal data are to be "obtained and processed fairly and lawfully" and "stored for specified and legitimate purposes and not used in a way incompatible with those purposes". Personal data should also be "adequate, relevant and not excessive in relation to the purposes for which they are stored" and "accurate and, where necessary, kept up to date".

Other basic principles in the Convention call for "appropriate security measures" and "additional safeguards for the data subject" such as the right to have access to his or her own personal data, the right to obtain, as the case may be, rectification or erasure of such data, and the right to a remedy if such rights are not respected. The concept of 'independent supervision' was initially not incorporated in the Convention, but nevertheless followed widely in practice and at a later stage added to the Convention via a Protocol.

To be sure: the Convention's approach is *not* that processing of personal data should always be considered as a *breach* of privacy, but in the interests of privacy and other fundamental rights and freedoms, any processing must *always* observe certain legal conditions. Such as the principle that personal data may only be processed for specified legitimate purposes, where necessary for those purposes, and not used in a way incompatible with those purposes.

Under this approach, the core elements of Article 8 ECHR, such as interference with the right to privacy only on an adequate legal basis, and where necessary for a legitimate purpose, have been transferred into a *broader* context. In addition, under the Convention, no exceptions to these principles are allowed, except under similar conditions as for the right to privacy itself.

Variable contexts

It should be clear that this only works well in practice, if the system of checks and balances - consisting of substantive conditions, individual rights, procedural provisions and independent supervision - is sufficiently flexible to take account of variable contexts, and is applied with vision and with an open eye for the interests of data subjects and other relevant stakeholders. In this approach, the right to respect for private life as set out in Article 8 ECHR continues to play an important role at the back, for certain specific more intrusive measures.

The provisions of the Convention were not intended to be directly applicable or incorporated in judicial supervision. Since 1997, however, the European Court of Human Rights has ruled in a number of cases that the protection of personal data is of "fundamental importance" for the right to respect of private life under Article 8 ECHR, and also derived yardsticks from the Convention for determining the extent to which that right had been infringed. This suggests that the Court is increasingly inclined to assess compliance with the Convention – at any rate for 'sensitive data' – within the context of Article 8 ECHR.

The Convention has played a major role in most Member States of the Council of Europe in determining legislative policy. In this context, the issue of 'data protection' has been viewed from the outset as a matter of great structural importance for a modern society, in which the processing of personal data is assuming an increasingly important role. The Convention is currently under revision and we will return to this theme in a wider context.

Harmonisation

Although the Council of Europe was very successful in putting 'data protection' on the agenda and setting out the main elements of a legal framework, it was less successful in terms of ensuring greater consistency across the EU. Some Member States were late in implementing the Convention, and those who did so arrived at different outcomes, in some cases even imposing restrictions on data flows with other Member States.

The European Commission was therefore quite concerned that this lack of consistency could hamper the development of the internal market in a range of areas - involving a circulation of people and services - where the processing of personal data was to play an increasingly important role. At the end of 1990, it submitted a proposal for a Directive to harmonise the national laws on data protection in the private and most of the public sector.

After four years of negotiations, this led to the adoption of the present Directive 95/46/EC which has a double objective. Firstly, it requires all Member States to protect the fundamental rights and freedoms of natural persons, and in particular the right to privacy with respect to the processing of personal data, in accordance with the Directive. Secondly, it requires them neither to restrict nor prohibit the free flow of personal data between Member States for reasons connected with such protection. Both obligations are closely connected. They aimed to bring about an equivalent high level of protection in all Member States with a view to achieving a balanced development of the internal market.

In that context, the Directive started from the basic principles of data protection, as set out in Convention 108 of the Council of Europe. At the same time, it specified those principles and supplemented them with further requirements and conditions. However, since the Directive adopted generally formulated concepts and open standards, it still allowed Member States fairly broad discretion on its transposition. The result is that the Directive has led to a much greater consistency between Member States, but certainly not to identical or fully consistent solutions.

Further substance

The current Directive includes criteria for the legitimacy of data processing. Personal data may be processed only if the data subject has *unambiguously* given his consent, if processing is *necessary* for the performance of a contract to which the data subject is party, or for compliance with a legal obligation, for the performance of a government task, in order to protect the vital interests of the data subject, or to protect the legitimate interests pursued by the controller, except where such interests are overridden by the interests of the data subject. This requires a subtle examination of the different phases of data processing and makes it necessary for data controllers to take this analysis into account at the right time.

Another feature of the Directive is the obligation for the controller always to provide the data subject with information, except where he already has it, on his identity, the purposes of the processing and other relevant matters, in so far as such further information is "necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing" in respect of the data subject. Failing to provide such information may lead to the data being obtained unlawfully, with all the relevant consequences.

The Directive also provides for the establishment of supervisory authorities for monitoring compliance with national legislation within their territory, with a number of specific functions and powers, which they should exercise "with complete independence". These authorities cooperate ever more closely in the exercise of their functions, also in the 'Article 29 Working Party' with independent advisory status at EU level.

International scope

The Directive applies to the processing of personal data carried out "in the context of the activities of an establishment" of the controller on the territory of an EU Member State. The place where the processing takes place is in that connection not relevant. This criterion is also crucial for the scope of national law within the EU. Where the controller is not established in the EU, the applicable law is that of the Member State in which the equipment used for the processing is located.

The Directive also applies the principle that personal data may only be transferred to third countries that ensure an adequate level of protection. In the absence of such protection, transfer is permitted only in certain situations.

These provisions apply to a complex reality in which, both within the EU and in relation to third countries, the question arises increasingly frequently as to what law applies and who is responsible for its compliance.

This also raises new questions concerning the Internet – about the position of websites, search engines, social networks and modern advertising technology – and relating to data traffic within multinational companies, outsourcing of services and cloud computing. In practice, adequate protection is increasingly frequently delivered in 'binding corporate rules', codes of conduct endorsed by enterprises that meet specific requirements and which the competent supervisory bodies accept as sufficiently effective.

Relevant case law

All Member States have transposed the Directive into national law, including the new Member States for which transposition was a condition of accession. The Commission has by now launched several legal actions for improper implementation of the Directive. The first action concerned one of the Member States with the longest experience in this area: Germany. In March 2009, the Court of Justice in Luxembourg ruled that the requirement of 'complete independence' for a supervisory authority means that it should be free from *any* external influence. This has recently been confirmed and elaborated in a case against Austria.

The Court of Justice has also issued a few other important judgments on the existing legal framework for the protection of personal data. In its first judgments on Directive 95/46/EC, for example, the Court ruled that it has a broad scope which is not dependent on a direct link with the internal market. This meant that the Directive also applies to a dispute in the public sector of a single Member State, or to a website of a church or charitable foundation. In the latter case, it became clear that the Directive applies in principle to the Internet, although the mere fact that personal data are available on a website does not mean that the provisions governing data traffic with third countries apply.

Where the Directive applies to an area within the scope of Article 8 ECHR, it must be interpreted in accordance with that provision. In that context, the Court distinguished between processing operations that may - or may not - breach Article 8 ECHR. The first applied to a legal provision compelling employers to supply certain salary data to a government body. Processing of the same data by the employer himself did not raise any issue of principle, as

long as data protection rules were respected. This fits in with the distinction between 'privacy' and 'protection of personal data' in the development of the law, as mentioned before.

Need for reform

Directive 95/46/EC is still the main element of the EU legal framework for data protection, but it has now become the subject of a wide ranging reform. On 25 January 2012, almost a year ago, the European Commission presented a package of proposals with a view to update and modernise the present EU legal framework. In the meantime, discussions on the elements of the package have been going on in the European Parliament and in the Council.

Why is this review taking place? This is basically for three reasons. The first reason is that there is indeed a clear need to update the current framework, and more specifically Directive 95/46/EC as its key element. 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 data processing 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 different 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, in December 2009, with a strong emphasis on fundamental rights. A separate right to the protection of personal data was laid down in Article 8 of the Charter of fundamental rights, and a new horizontal legal basis in Article 16 TFEU for rules on data protection, providing for comprehensive protection in *all* 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 about stronger, more effective, more consistent, and more *comprehensive* protection of personal data.

A huge step forward

We now have a package of at least two main proposals: a Directive for – briefly put – the law enforcement area, and a directly binding Regulation for what is now still Directive 95/46, applying to the commercial areas and the public sector, other than law enforcement.

I have welcomed the proposal for a Data Protection Regulation as "a huge step forward" towards a more effective and consistent protection of personal data across the EU, but also asked for clarification and improvement on a number of important details. Those interested can find the substantial Opinion of the EDPS of 7 March 2012 on our website, together with all relevant documentation.

However, the architecture of the package in itself - a Directive and a Regulation - signals that there is a problem with its comprehensiveness. And indeed, this is where we 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 at this interface will have practical consequences in a much wider field.

Continuity and change

But if we now focus on the Regulation, there are some main messages which you all 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 much stronger emphasis on 'data minimisation' - briefly put: "not more data than strictly necessary". Another example is the recognition of 'Privacy by Design' - "taking privacy into account from the start" - as a general

principle. There is also a clarification of 'consent': *when* you need it, it must 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, acting in close cooperation with other competent authorities.

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 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 fully 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 that fully complies with fundamental rights.

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. In any case, I would not find it useful to consider a change of the Regulation into two different instruments - one for the public sector and another for the private or commercial sector. Quite to the contrary, such a change would have a *disastrous* impact, both on the effectiveness and on the consistency of the new framework, particularly for services at or across the borderline.

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 sufficient 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, e.g. 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 against Germany.

The Regulation also provides for supervisory authorities 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' much higher on the agenda of corporate boardrooms, which is very welcome.

In reality, we already see a quickly growing practice of more vigorous enforcement, with various means: remedial sanctions, administrative fines, and also some increased liabilities. This trend will no doubt continue in the near future.

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 again, this lead authority will not be acting on its own, but be part of a network of close cooperation with other competent authorities.

A very important additional element 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. 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 the behaviour of data subjects in the EU is being monitored.

As you will understand, this is a growing reality on the Internet nowadays. At the same time, it is a realistic approach that builds on an increasing synergy as to data protection in many relevant countries 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 now a specific provision on Binding Corporate Rules, with a number of simplifications.

Let me finally mention that international cooperation among data protection authorities is developing also 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 mentioned the 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.

But in a wider perspective, let me also say that this is a time of great opportunity. Although it is necessary to once again consider the ethical dimensions of data protection and privacy, it is also necessary to link the need for more effective and more consistent protection of privacy and personal data with other important subjects, such as economic recovery, where the Digital Agenda for Europe and the EU 2020 Strategy will likely have great impact.

In any case, I strongly believe that a "smart, sustainable and inclusive Europe", as aimed for in these policy programs, is not achievable without proper safeguards for fundamental rights, including data protection and privacy. This is why this high level conference is so welcome and why its location is so well chosen.

As already briefly touched on, the EU does not stand alone in its efforts for a data protection reform. The Council of Europe and the OECD (not yet mentioned) are also looking at their respective frameworks. So far, there has been remarkable synergy among these efforts. This is important to ensure a good amount of consistency and interoperability around the world.

Finally, where are we in Brussels? Discussions are proceeding in Parliament: a draft report is now on the table in the LIBE Committee. The Council is expected to arrive at conclusions under the new Irish presidency by the middle of this year. Both Commission and Parliament are no doubt eager to come to final results by the end of their current mandates in 2014.

Although the future is always uncertain, I would expect that the proposed Regulation will make it to the end, with some necessary improvements obviously, and I will do my utmost to help make that possible.

Thank you very much.