Le Point Conference "Connected and Intelligent Home"

Paris, 28 March 2013

Peter Hustinx

European Data Protection Supervisor

"Sharing personal information and respecting privacy at home"

I am delighted to be able to contribute to this conference on an issue of great practical and symbolic importance: how to preserve our privacy at home in an ever more connected world?

The privacy of our homes has always been at the core of constitutional protections and is now a key element of the fundamental right to the protection of private life. Entering a home without permission or intercepting private communications is for good reasons subject to special safeguards.

In an Information Society that is driven by the pervasive use of information and communication technologies - both at home and elsewhere - we have to invest in stronger safeguards for the protection of personal data in general. That explains the current review of the legal framework for data protection in the European Union.

However, the introduction of 'intelligent homes', if not subject to extensive safeguards, could seriously undermine existing protections. While smart metering systems may bring significant benefits, they also enable massive collection of personal data which can track what members of a household do within the privacy of their home.

These data can be useful for analysis of our energy consumption, but together with data from other sources, the potential for extensive data mining is very significant.

This is even more so, if the 'Internet of Things' becomes a reality and all objects we currently use at home would be connected online, and would start to communicate, with each other and with outside providers, about our habits and needs.

Who will be in charge of that information: is it really going to be us? Or are we bound to live in 'transparent homes' where protection of privacy at home has lost its meaning. How do we make sure this will *not* be the case?

Let me first explain what is now being done to provide stronger safeguards for the protection of personal data. Our current legal framework, which is the basis of all national laws in the EU, was adopted in 1995, at a time when the Internet barely existed. There is thus a clear need for innovation, mostly to ensure better protection against current challenges.

There is also a problem of undue diversity and complexity, because the legal framework has been transposed in 27 different national laws. More harmonisation and more consistency in the EU would help to make the protection more effective. Finally, the Lisbon Treaty has introduced a basis for more effective and comprehensive protection in all policy areas.

For these reasons, the European Commission has proposed a thorough reform of the current legal framework in January 2012, which is now under debate in the European Parliament and the Council. Although the whole package still raises quite a few questions, there is also great consensus about its main lines.

First, the scope of EU law will be extended: it will also apply whenever goods or services are offered at the European market, or when residents of the EU are being monitored. This means a 'level playing' field where Internet service providers and other key actors will be covered, regardless of whether they operate from the EU or from a third country.

Secondly, the position of data subjects will be reinforced so as to ensure an adequate control over the collection and use of their personal data. This will come from more transparency of data processing, stricter rules on consent, and more effective rights of access, correction and erasure of data, including rights to be forgotten and to data portability.

Thirdly, the controller's responsibility will be emphasized by duties to ensure and demonstrate compliance with data protection requirements, to conduct timely data protection impact

assessments, and to ensure that all relevant privacy aspects are included in new developments from the start ("Privacy by Design").

Fourthly, the position of independent authorities will be reinforced, with stronger and uniform powers for more effective supervision and enforcement, including the possibility of heavy fines and other effective sanctions.

Finally, it is likely that a General Data Protection Regulation will apply directly in all member states, to ensure more harmonisation and consistency across the EU. Supervisory authorities will also be cooperating more closely on issues with a European or international dimension.

Now, what does all this mean for 'intelligent homes', and more specifically for smart metering systems? It simply means that privacy will play a much bigger role in the development and introduction of any such systems than has been the case so far.

About one year ago, the European Commission adopted a Recommendation on preparations for the roll-out of smart metering systems. This roll-out is now foreseen latest by 2020 subject to an economic assessment of costs and benefits.

However, this roll-out should not only be subject to *economic* considerations. Due to the high potential for intrusive tracking of private behaviour, any smart metering should also be subject to a data protection impact assessment.

The Article 29 Working Party has recently been consulted on the proposed template for such a data protection assessment, as defined by the industry. The initial reaction of the Working Party was quite critical. It felt that the proposed template was too general, did not include sufficient guidance to make it a genuine risk assessment and did not provide any best practice recommendations that would be applicable to the smart grid context specifically.

The EDPS Opinion adopted in June 2012 has highlighted the need for additional safeguards, including possible legislative action at EU level. These safeguards should at least contain a mandatory requirement for controllers to conduct a data protection impact assessment and an obligation to notify personal data breaches.

We have also recommended more guidance on the legal basis for the processing of data and the choices available to data subjects, including on frequency of meter readings, and more guidance on retention periods.

We also feel that this is an excellent case for the mandatory application of privacy-enhancing technologies (PET) and other best available techniques for data minimisation. In other words: Privacy by Design should be the standard. Consumers should also have direct access to their energy data, their individual profiles and the logic used for data mining, and any information on remote on/off functionality.

There is an obvious link with the use of cloud computing. Here it is essential to keep in mind that storing data "in a cloud" does not mean outside the scope of EU data protection law. In fact, both current and future data protection rules also apply in the cloud.

Therefore, it will be essential to clarify who will be responsible for compliance with data protection rules in this environment. It is not only a question of who is controller or processor. Increasingly, we see that customers and providers of cloud services are both responsible. This requires a clear description of the responsibilities of each party in order to avoid a serious lack of protection in practice.

The Article 29 Working Party has adopted an opinion in July 2012 on cloud computing which clearly demonstrated that effective controls are possible to ensure adequate data protection. It only takes responsible parties to agree on those controls in practice.

In my view, the current imbalance of power between cloud customers and cloud providers could be addressed in standard terms and conditions that respect data protection requirements, and by standards and certification schemes that fully incorporate data protection criteria. Most issues in international data transfer could be addressed in binding corporate rules (BCR). In November 2012, we have advised the European Commission along these lines.

So, all this shows that privacy is now indeed a hot issue. Both privacy and security concerns should be addressed by including them in all relevant projects from the start. That is the best way to develop effective protection in practice and to provide Trust in the Information Society in the years ahead.