Introductory words by Jacob Kohnstamm

Safe Harbour Conference, Washington 2009

Ladies and gentlemen,

Let me please first take the opportunity to thank our host, Mrs O'Neill, who, by organizing this conference provides us with the opportunity to - as the conference agenda mentions - **advance mutual cooperation** and **understanding** and **to improve data protection oversight.**

As you may know, apart from being vice chairman of the European Union's Working Party 29, I am the chairman of the **Dutch** Data Protection Authority.

As a Dutchman, I am specifically honored to be in the United States this year, as the year **2009** officially marks the **400th (four hundredth) anniversary** of the Dutch **founding** of what is now called the Hudson River. An anniversary that has triggered many festivities, both in the Netherlands and –as I have understood- in the United States.

400 years ago, the Dutch domination of the seas fueled a hunger for new markets and raw materials and for shorter and safer routes to reach them.

To find a shorter route to the Orient, the powerful Dutch East India Company (the VOC) hired an ambitious English explorer, Henry Hudson, who sailed the Atlantic three times. Henry Hudson did not find a passage, but on his third voyage in 1609 he found a place we now call the Hudson River and Albany.

Hudson returned to Europe without the silk and spices he had expected to find. Instead he found a "Safe Harbour" and many beaver furs...![1]

The "Safe Harbour" that the United States provided in 1609 has evolved immensely. In data protection terms, the Safe Harbour agreement that was concluded between the United States and the European Union in 2000, has provided for a specific set of rules enabling US organizations to qualify as offering adequate data protection, as is required by European legislation for all international data transfers.

As you may know, in the European Union, the protection of personal data is a **fundamental right**. Article 8 of the European Charter of Fundamental Rights explicitly recognizes this. The EU's Data Protection Directive has established a legal framework for the protection of personal data and has a twofold objective: not only does it ensure the protection of individuals' right to privacy; it also guarantees the free movement of personal data throughout the European Union, which might otherwise be hampered in the absence of such protection.

In order to ensure that European citizens' fundamental right to data protection is also ensured in a global economy, the EU legal framework naturally also addresses the issue of **transfers of personal data beyond the European territory.**

As you know, transfers of data outside Europe are possible when the third country's legal framework on personal data offers, as I mentioned earlier, an **"adequate level of protection"**.

The framework agreed between the United States and the European Union in 2000 was concluded **precisely for that reason.** It was set up to provide for a set of rules enabling US organizations to qualify as offering the required adequate protection. And its principles are meant to ensure that the protection of personal data is a guarantee to the **free flow of information across the Atlantic.**

Let me be frank with you, the system we have in place today may **not** be **perfect**. However, in the meantime, the Safe Harbour agreement is the instrument on our table. Its success now primarily depends on the **implementation of its principles in practice**. The proof of the pudding is, as always, in the eating.

But questions will continue to be raised with regard to the Safe Harbour system's effectiveness and its strength in protecting personal data. **Especially in today's globalised world.**

In a global economy **regional** or specific rules for data exchange, such as the Safe Harbour agreement, do not suffice. Many -and I am certainly one of them- are convinced that **in the long term international regulation** is needed. I am sure you are all aware of the significant efforts that have been made by my Spanish colleague, Artemi Rallo, in order to make the first steps in achieving this goal.

In striving to reach international regulation, we have found many **commonalities**. But we have also found fundamental **differences of approach.**

The most essential differences between our continents are the following: in Europe there is **one comprehensive legal data protection framework** which includes **independent oversight.**

In the United States a **sectoral regulatory approach** is taken. And, in the absence of sectoral regulation in the US, **self-regulation** mechanisms are in place.

In **striving to bridge these differences** in approach, European data protection authorities have recently been discussing the concept of **"accountability"**.

What does -from a European perspective- "accountability" mean?

In essence, accountability means that **data controllers take proper care of the personal data they handle.**

Data controllers should be able to demonstrate their capacity and responsibility to achieve privacy objectives and to determine appropriate and effective measures to reach those goals.
Data controllers can and should make use of all kinds of instruments, such as privacy impact assessments, audits and privacy enhancing technologies in order to accomplish this.

Being accountable also means being **transparent**.

In the complexity of today's world, it is increasingly difficult for individuals to make decisions to control the use and sharing of information. Data controllers therefore need to be **transparent** about the fact **that** they process data and **why** they do so.

Individuals should be able to acknowledge and understand the purpose of data processing. They should be assured that safeguards are taken in order to prevent the illegal use of their data. And they should be informed how they can exercise their rights.

Data controllers can achieve this by establishing **clear and accessible privacy policies** and by enacting **easily accessible complaints procedures**. Furthermore, **recourse mechanisms** should be set in place, which are **affordable** and **independent**.

Data controllers are the ones that should be **accountable** and responsible for compliance. However, in our view, in the end accountability needs **strong and independent oversight as well**.

Data processing around the world is becoming more and more complicated. Due to new technological applications transparency alone (notice and choice) is no longer sufficient to guarantee that individuals can oversee the consequences of data processing activities. Therefore independent oversight is necessary. It is necessary to ensure a **level playing field**. To ensure that all are abiding to the same rules.

In order to be able to take appropriate action against controllers that fail to live up to their responsibilities, oversight mechanisms need to have **appropriate enforcement tools**. Only the prospect of substantial fines can act as a strong deterrent and can help ensure that data protection obligations are taken seriously. In order to be most effective, these enforcement tools should be **targeted to material infringements,** not to merely procedural issues.

In addition, according to Europeans, it is essential that data protection oversight is **comprehensive** and covers **all data protection matters, not merely a specific sector.**

Henry Kissinger famously asked *"Who do I call if I want to call Europe?"* Also in data protection matters it needs to be clear whom to call, not only in Europe but also in the United States!

Ladies and gentlemen,

I believe **this concept of "accountability"** may in the future be able to bridge our differences in approach. It might bring our continents closer to each other than they are now in terms of data protection.

Let us **explore** this concept further and let us strive to find ways in order to achieve a **well-functioning system of data protection that works globally.**

Many interesting items will be discussed in the next two days. Several instruments to achieve compliance and accountability are on the agenda such as privacy by design and information security

measures. But we will also be discussing challenges to data protection by phenomena such as online social networks and behavioral targeting.

My **hopes for this conference** are twofold:

1) that all present here will be confirmed of the **mutual need and importance** for sound data protection policies and oversight mechanisms
2) that these policies are **properly implemented** in order to achieve real protection.

But I hope I have also been able to make my **hopes for the future** clear to you!

Ladies and gentlemen, let me end by quoting your current president, Mr Barack Obama: "if you're walking down the right path and you're willing to keep walking, eventually you'll make progress"

I look forward to discussing with you and wish you a very successful conference!