Fundamental Rights Forum in Vienna

Guiding Questions chosen by MEP Marju Lauristin during the workshop

1. How should ethical principles and cultural norms, which pursue respect for dignity and privacy be best upheld in the digital age?
2. What is the impact of ICT and social media on people's expectations of dignity and privacy?
3. How does the recently adopted data protection legal framework address the risks related to digital technologies and enable to make use of its benefits?
4. How will risk assessment and compliance work in practice under the EU's new General Data Protection Regulation?

We do not protect data, we protect people.

- Why data protection is fundamental part of the digital society? Parallelism between off-line an on-line interactions is not working, when we deal with the personal data. In real life we can hide our traces, we can experience things "incognito" but in digital life we leave traces online everywhere. The online world has become much more than simply a way for us to perform specific tasks. Our personal photos, address books and medical information are usually in the cloud. Many of our intimate conversations take place and are often stored online. And in our online activities we leave so many digital traces behind that companies can draw a surprisingly intimate portrait of us. It is therefore clear that in the online environment the protection of our personal data is even more pressing than in the offline world.

- Privacy and security: Constant tension between two fundamental values. Privacy to have our own life in our hands vs the unstable and insecure environment that one needs to be protected from. It is connected with democracy (freedom of speech, movement), rule of law and equality. We have to put clear limits, not to be overwhelmed with fear and shut down everything but not to be overwhelmed by an absolute privacy either.

- The current trends towards using Big Data are presenting both possibilities and threats. New wave of digital development will create new

opportunities for competitiveness and effective management but at the same time also enables bulk surveillance, gathering of personal data from the indirect sources and violations of the privacy of data subjects or the secrecy of business transactions. The European Union is implementing new GDPR to protect its citizens and is also investigating protection mechanisms for business data.

- Having in mind the rising speed and scope of data processing in our everyday life we have to focus more on the standards of ICT development and the need to introduce new in- built technological solutions. In my view privacy by design and by default is the centrepiece of this text and if we emphasize this side we can become champions worldwide.

- The most important aspect of GDPR lies in its capacity to shape the way how citizens and businesses face the new digital reality. The most effective mechanisms in privacy protection are embedded in **the new digital culture**. Law cannot protect the personal data of someone who does not want to be protected. But as legislators we are obliged to protect those that wish to be protected The challenge and aim of the new legislation is not to put restrictions on innovative developments but to increase confidence in technology throughout Europe and make all European citizens able to handle their privacy, reflecting their personal choices and **own way of life.**

- Digital society should bring fundamental changes in education. Since the early childhood the digital culture, including the norms of privacy protection should be part of the curricula. Life-long learning should include training in digital skills for all citizens, including the elder generation that sometimes feels neglected as technology achievements move too fast. Our deep concerns are about low awareness of data controllers: some companies or individuals do not even know they are processing personal data! Data protection must be included in the ABC of business education.

Some major changes under the new GDPR

- **A single set of rules and identical system of institutions dealing with data protection, will apply to all EU member states.** Each member state will establish an independent Supervisory Authority (SA) to hear and investigate complaints, sanction administrative offences, etc. Where a business has multiple establishments in the EU, it will have a single SA as its “lead authority”, based on the location of its "main establishment" (i.e., the place where the main processing activities take place). The lead authority will act as a “one-stop shop” to supervise all the processing activities of that business throughout the EU

- **Consent:** Valid consent must be explicit for data collected and purposes data used (Article 7; defined in Article 4). Data controllers must be able to prove "consent" (opt-in) and consent may be withdrawn. For children under certain age, defined by national legislation, consent must be given by child’s parent or custodian, and be verifiable (Article 8).

- **Right to object to Profiling**: The proposal maintains the *(unlimited)* right to object profiling with no condition, when data are processed in the interest of the controller (eg. direct marketing). The data subject can exercise his/her right by automated means -"do not track" feature that will from now on have a legally binding force. The right to object to profiling could be limited on the grounds of public interest or legitimate interest of the controller when linked to the particular situation of the data subject.

- **Data Protection Officer**: A mandatory DPO will exist in limited cases: a) public authorities, b) controllers whose core activities consist of processing operations which require regular and systematic monitoring of the data subjects in large scale, and c) controllers whose core activities consist of processing sensitive data on a large scale.

- **Sanctions**: The following sanctions can be imposed: a warning in writing in cases of first and non-intentional non-compliance, regular periodic data protection audits or a fine up to 1,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.