Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Eingangsstatement

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Prof. Ulrich Kelber

“How to foster Sustainable Digitalisation in Europe and Africa”

African Leadership Academy

Deutsches Institut für Entwicklungspolitik (DIE)
German Development Institute

4. Mai 2021
online

Es gilt das gesprochene Wort – the spoken word shall prevail

Anrede,

1. Europe has become beacon of hope for privacy rights

- Dynamic digitalization increases new risks for privacy and self-determination of people

- Concerns regarding internet platforms prominent, but actually all business and government data processing affected

- The EU GDPR Privacy and data protection legislation has become a global standard and benchmark for legal regulation in this field. Countries like Japan, Thailand or even the US-state of California now have data protection laws following this standard.

2. Basic intention, scope and oversight infrastructure

- The key idea of data protection roots in human rights: there is an individual right to know and to decide on whether the personal data regarding one´s own person may be processed or not. Data protection laws deliver a rather broad concept of different elements supporting this right. They obligate companies and public administration to follow strict rules on how to process personal data.

- Data protection laws regulate the processing of all personal data, meaning all information and data referring to individual persons

(with the exception of data processed in the course of family use or purely private activities). These laws offer real rights for citizens and full access for judicial redress in the courts.

- Processing encompasses all form like the collection, storage, transmission of data (like for instance from one country to another)

- A core element of data protection legislation is supervision. The success of European DPA legislation largely relies on effective and independent oversight bodies and their mutual coordination within the EDPB. Rather high sanctions with up to 4 % of the annual financial turnover of a private company have really forced business world into compliance.

- It is important that irrespective of the location of a company, data subjects can contact their local supervisory authority which can handle requests and complaints in a citizen-friendly manner.

- The so-called marketplace principle obliges all companies outside Europe to comply with the European data protection law when they offer their services on the European market or monitor the behaviour of data subjects in the EU, for instance via the internet. This will ensure that equal competitive conditions apply to all companies operating in the European single market.

3. The seven golden rules of data protection law

- Data protection laws are considered complicated. With the following basic principles you should have a pretty good basic understanding. As this is supposed to be a quick and very comprehensive seminar I´d like to draw your attention to the following seven basic points:

  1st Rule is lawfulness and fairness:

  Any processing of personal data requires a legitimation in the form of the data subject's voluntary decision or other explicit legal basis. These legal bases aim for a fair balancing of interests between the citizens affected and the interest of the company or other institution. It really is about balancing of typically very asymmetrical powers. Data protection in this respect is a kind of a consumer regulation and aims at supporting and protecting the weak.

  2nd Rule is purpose limitation:

  Data may basically only be used for the purpose for which they were collected in the first place. This purpose has to be communicated to consumers/ citizens and documented in advance. A contract may allow for processing of customer data in order to finalize the contract. These data may not automatically be used for advertisements for other products. That would typically require an additional legal basis such as consent by the customer.

3rd Rule is the necessity principle (and data minimization):

As a rule of thumb, all processing of personal data should be limited to what is necessary for achieving the purpose of the business process. Once a purpose is fulfilled, a storage limitation kicks in and data have to be deleted. Excessively collected data without need to execute the given purpose also have to be deleted. The new GDPR rules include principles of privacy by design ("data protection by technology design") and privacy by default ("privacy-friendly pre-settings"), so that technology itself is designed to process few or no personal data at all.

4th Rule is transparency:

Empowering citizens is all about offering them real choices. Good choices are based on transparent environments. IT and data processing for most is the opposite of understandable and transparent. So data protection laws oblige companies and administrations to inform in advance on the details of handling the data (purpose, storage duration, possible data sharing with others, rights of users, offering accessible contact). All laws offer a right of access to one´s own personal data and detailed information about the processing itself.

5th Rule is data security:

The integrity and confidentiality of processing personal data has become more important than ever. There is a rat race going on between attackers and defenders of IT systems. Data protection laws set standards for the quality of the defensive systems and very often poor standards are cause for legal action and fines by DPAs.

6th Rule is accountability:

Data protection impact assessments, the provision of information to data subjects and supervisors about data protection breaches or a regulation limiting automated decision-making, including profiling. In general, data controllers always have to be able to demonstrate compliance with data protection law

7th Rule is accuracy:

All personal data being processed need to be kept accurate. This corresponds with an individual right to rectification of incorrect/ inaccurate data being stored by companies/ authorities.

4. Some thought on the situation of African states

With regard to the African states and with increasing dynamics of digitalization in parts of Africa some additional key points:

- Privacy legislation is all about securing human rights of citizens in the face of increasing data power of institutions like Facebook, Google etc., but also government institutions

- Europe itself to some extent has witnessed being overpowered by Silicon Valley companies (and some have called this “digital colonization” but Europe really voluntarily gave in to it and also profited from it). Today China is another key player in this global competition for market place domination.

- I urge you as young leaders to look out for and engage in protecting elements of digital sovereignty for your countries. This may sound over-idealistic considering some offers being rolled out and with regard to the lack of own IT resources and funding. But keeping control over one´s own data on an infrastructural level has become key to not being susceptible to blackmailing and avoiding extreme dependency, even foreign control. Tools for protection are multiple, like for instance keeping data within own state borders where possible, insisting on open source data, securing data protection compliance in public procurement rules, seeking cooperation with organizations like the Council of Europe (which Senegal and Tunisia apparently are a member), the Global Privacy Assembly (GPA) and cooperating with the UN and its UN High

Commissioner on Human Rights (OHCHR) and its special rapporteur on the right to privacy

- Numerous NGOs in the field of privacy protection have pointed out that in some cases Africa may have become prey to the roll-out of European IT products for concepts of government surveillance and handling of population data which would not stand the test of data protection with DPAs in Europe. I am thinking about biometric data bases of all citizens for a variety of purposes with poor data security and almost no boundaries for access by government authorities. This really needs a wake, healthy civil society and solid resistance to deal with. As we have learned from the Cambridge Analytica/ Facebook case, numerous countries like Kenya were targeted with the meddling in political elections and voter fraud action. Keeping this in mind, digitalization of elections is a very risky approach open to misuse and manipulation. No wonder that on a state level most European countries don´t use these systems.

- When talking to business leaders you may hear about data protection being a mere hindrance and obstacle to trade. This does not hold true. Data protection rules do force businesses to carry out business in a particular order. But this order serves both the companies and the customers. The companies have to re-structure their internal organization which allows for a better focus on their key assets and how to protect them (their customers). With regard to customers, respecting their privacy rights and legal compliance to data protection standards opens up for a real

relationship of trust. Thus data protection may become a key competitive factor for companies because it allows them to stand out for respecting their customers and for protecting their human rights at the same time.

Thank you for your attention.