G20 Consumer Summit, 15.03.2017 in Berlin

Panel 2: Consumer data – Giving consumers clarity and control over the use of their online data

Input Statement from Marit Hansen, Data Protection Commissioner Schleswig-Holstein

Ladies and Gentlemen, As a Data Protection Commissioner, I am very glad that I was invited to the G20 Consumer Summit on the important topic of a trustworthy digital world. I want to talk about putting consumers in control and not at risk.	 Putting consumers in control … … and not at risk Marit Hansen Data Protection Commissioner Schleswig-Holstein, Germany Berlin, 15 March 2017 G20 GERMANY 2017 ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Today's world is characterised by increasing processing of personal data. Current developments towards Big Data, algorithms with more or less Artificial Intelligence and the sensors in all "smart" solutions (Smart Car, Smart Home, Smart City) show that data processing is planned – or already done – in almost all areas of our lives. Data processing becomes ubiquitous. A great variety of small- or medium-sized companies is involved in this data processing, but a huge part of data processing is done by only a few companies. Their customer base consists of millions or even billions of people world-wide – these giants are bigger than many states. And their influence in setting the rules and governing the digital world must not be underestimated. The data processing itself has become very complex. This is not only the case with ambitious endeavours like autonomous cars safely driving and finding their way on their own. Even surfing a website often does not mean that there is only one connection between the user's browser and the server with the content. Instead many websites automatically contact other servers for specific content, but also for user tracking and analytics as well as different approaches for ad delivery, marketing and behavioural targeting of users. A few clicks from the user on one server may result in access operations on hundreds of other servers – and the user's data are being disclosed and harvested. In the digital world more and more data are analysed, and on their basis, decisions are being generated. Decisions that can influence people's lives, e.g. on the creditworthiness of consumers, on the prices they are asked to pay, whether they are entitled to get some subsidies or not, and – according to their psychological profile – how they may be nudged into buying a product. The police are testing "predictive policing", companies and governmental authorities look at arbitrary big data results that support their goals. The question now is: "How to establish fair rules?" What are fair rules, which stakeholders can support or enforce them? What are the incentives, what are the obstacles? And we must not forget our basic values for society, the human rights.	 ULD www.datenschutzzentrum.de Status quo: self-reinforcing trends • Data processing everywhere … • … with a few dominating giants • Complex systems … • … generating decisions on people How to establish fair rules? What about the human rights? Putting consumers in control …

These rights encompass the right to privacy and to data protection.

Consumer protection and data protection face similar challenges:

The power of the individual, the human being, the consumer is tiny compared with the overwhelming power of organisations that are processing the data for their purposes.

This imbalance in power is the reason for the demand for “data protection” and the implementation of a system of Data Protection Commissioners in many countries:

- They are designed to be independent supervisory authorities and handle complaints from individuals.
- They usually can inspect the processing of personal data in their jurisdiction both at companies and at governmental organisations.
- They give advice how to be compliant with the data protection law.
- And they put the perspective of the individual in focus.

You’ll notice that “data protection” is not a good term for the work of the Data Protection Commissioners. In fact, their task concentrates on protection of fundamental rights with respect to information, to protect the individuals and not any arbitrary data chunk.

ULD www.datenschutzzentrum.de

Imbalance in power
⇒
data protection necessary

Important:
Perspective of the individual

Source: [illegible]

Putting consumers in control ...

If I evaluate data protection in the digital world, I have to admit that the current state of play is not sufficient at all.

Certainly Data Protection Commissioners have limited resources and cannot comment on all kinds of potential or actual data processing.

In the past, the leverage for improving the setting of usual data processing and enforcing data protection law was not very strong. But the situation is changing:

One year ago the European General Data Protection Regulation was adopted by the European Parliament and the Council. Beginning from May 2018 all data processing organisations in Europe will have to be compliant with the General Data Protection Regulation (GDPR). In my point of view this regulation can be a real game changer.

The “market location principle” means that not only companies in the EU, but also those offering goods or services to people in the EU or monitoring their behaviour are being addressed by the regulation.

I would like to stress a few of the new instruments laid down in the GDPR that are related to the design of data processing systems:

- Data protection by design (Art. 25(1) GDPR)
- Data protection by default (Art. 25(2) GDPR)
- Data protection impact assessment (Art. 35 GDPR – to mitigate risks to the “rights and freedoms of natural persons”)
- Certification (Art. 42+43 GDPR) as a result after a thorough examination

I think these instruments have a great potential, and all organisations as well as producers should have already given thought on how to implement data protection requirements into the systems.

ULD www.datenschutzzentrum.de

Regulation (EU) 2016/679

EU General Data Protection Regulation – A game changer

- Market location principle (Art. 3 GDPR)
- Data protection by design (Art. 25(1) GDPR)
- Data protection by default (Art. 25(2) GDPR)
- Data protection impact assessment (Art. 35 GDPR – “rights and freedoms of natural persons”)
- Certification (Art. 42+43 GDPR)
- Fines & sanctions (Art. 83+84 GDPR)
- Courts

Powerful toolbox, but only as good as its implementation

Source: [illegible]

Putting consumers in control ...

It seems that the most valuable and most convincing incentive is not really an incentive, but the possibility of tangible punishment. The fines for being not compliant with the GDPR can be quite high:

“Infringements […] shall […] be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year”

This seems to function as a wake-up call for several companies that were ignoring demands by Data Protection Commissioners so far.

However, the GDPR is designed to last not only for a few years, but perhaps 30 to 40 years. This has resulted in a very high level of abstraction in the provisions and, consequently, results in a lack of certainty how to implement the regulation. In the end, there will be much work for courts that have to provide clarity, especially the European Court of Justice.

To summarise, I regard the GDPR as a powerful toolbox, but we have to put it into practice.

On two principles I want to give some more information: transparency and intervenability.

ULD www.datenschutzzentrum.de

Enhancing transparency

- Clear and simple language
- "Layered Policies"
- Standardised icons
- Machine readable

PRIVACY NOTICE

Self-protection tools not sufficient: putting the burden on the consumer

Putting consumers in control ...

The GDPR demands better transparency for individuals whose data are processed. This means for example:

- Clear and simple language that can be understood
- “Layered Policies“: not “one size fits all”, but at first the most important information, and further details for those who want to get more information
- Article 12(7) GDPR even demands:
  “The information […] may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.”

The standardisation of icons is not an easy task, and I have seen many not so convincing examples. But several researchers and also my office have already done some work in this area, and we believe that it is possible to kick off good solutions, even if a full standardisation may be a long shot. For instance, icons can already be used in addition to the normal privacy policies for illustration purposes.

On the right side you’ll see an approach for improving privacy policies.

On the left side is a transparency tool developed in a European research project as a self-protection tool. It is called “Data Track” and visualises for the user where and to whom she disclosed personal data or left data trails. This enables her to exercise her data subject rights to access or erasure.

But beware: Self-protection tools must not be the centrepiece of a solution because this would mean to put the burden on the consumer instead of on those mighty players who are processing the personal data.

Sometimes data protection is reduced to the notion of “notice & choice”. This sounds good, but it is by far not sufficient. Especially very often the choices are too limited, and the consumers are required to take action to be on the safe side instead of being able to rely on a safe environment in the digital world.

The GDPR takes a different stance by introducing the principle of “data protection by default”. In my interpretation this means that personal tracking could not happen without an active intervention by the user. And obviously there wouldn’t be an unnoticed uploading or synchronising of the address books of the users containing information of all their contacts – what is currently happening on a regular basis.

But intervenability – the possibility to intervene – means much more than clicking and consenting to additional data processing. It encompasses even the possibility to stop a process. Think, for instance, of sensors monitoring your home. You have to be able to deactivate them. Or think of software generating decisions on consumers. It has to be possible to intervene and not to take the correctness and fairness of those decisions for granted.

My conclusion as a Data Protection Commissioner with the background in computer science and decades of experiences in collaborating with lawyers and people from other disciplines is:

System design is key. And by this I don’t think only of technology design, but also of processes, organisations, standards and the law.

Consumer protection and data protection share a lot of values – even if they are not twins, they are siblings and should work hand-in-hand for improving our digital world.

Enhancing intervenability

- Giving consumers meaningful choices ...
- ... on the basis of "data protection by default"
  - No "tracking by default"
  - No upload of contacts/address books
- Sometimes necessary to intervene by stopping a process

Source: Playing Futures: Applied Nomadology

Source: Mark Hillary

Conclusion

1. System design is key: technology & organisation & law
2. Consumer protection ↔ data protection

Putting consumers in control ...