

# SECURITY, CONFIDENTIALITY, PRIVACY BY DESIGN

## FUTURE OF EPRIVACY DIRECTIVE

### Threats

- The connected world is facing an increasing amount of cyber attacks
- Massive surveillance activities shake consumers trust in digital business models
- All kind of data are subject to cyber attacks and abuse

**The level of security and confidentiality at least must be stable in all areas.**

**f.e. “Ten-point program for increased cyber security” by DT from 2015**

<https://www.telekom.com/media/company/264248>



# SECURITY, CONFIDENTIALITY, PRIVACY BY DESIGN

## FUTURE OF EPRIVACY DIRECTIVE

### Does the “traditional” focus of the information to be protected still fit?

- What kind of data breaches are likely to result in a high risk for data subjects
- Processing of what kind of data might have the most severe impact on data subjects
- Consider impact of lawful linkage of any data and indicators (e.g. banking, insurance or health data, ...)

Rethink the evaluation – what is covered by the GDPR and is there still a need for specific solutions?

### Do the “traditional” addressees of the legislation still fit?

- Who is processing what kind of data
- What are the consumers expectations
- Which legal framework provides the required safeguards and security measures

Rethink the evaluation – are Telecommunication Providers still the only ones that process confidential information?

