50th Anniversary of Data Protection: What's Next?

Technology, Privacy, and eCommerce

As data protection recently celebrated its 50th anniversary, we look back on a true success story.

The Hessian Data Protection Act in Germany (October 1970) was the first of its kind worldwide, but it was based on an old understanding of terms. Data protection had essentially been defined as the literal protection of the data itself through data backups.

However, before the Hessian Act was passed, Ulrich Seidel, co-author of this article, laid the foundation for how we currently understand data protection. Seidel defined it as the protection of privacy for personal data in general, doing away with the distinction between data in the social sphere and that in the private sphere.

Fifty years later, the EU General Data Protection Regulation (GDPR) is now considered the gold standard for data protection by many around the world. However, some see it as a bureaucratic brake on innovation without proportional added value for the individual. In other words, data protection has structurally reached its limits, because technology, society, and people's self-image have changed radically. Data protection must be rethought to address this development, not just to follow these changes, but to become part of social reality and function as a catalyst for innovation so individuals can become sovereign actors alongside data-processing bodies.

Below are some areas of development that may become focal points over the next few years.

Data minimization

The principle of data minimization, where data collection is limited to only what is necessary, has increasingly been leveraged as data-intensive areas have experienced exponential growth, such as the Internet of Things (IoT) and artificial intelligence (AI). The principle has

been documented in OECD guidelines since 1980, when one gigabyte of storage space cost up to US$1 million and neither the personal computer nor the internet itself existed in its present form. According to the German Federal Network Agency, in 2019, the monthly data volume of the average German user (excluding use of mobile internet) was 124 gigabytes.

Data has long since become the oxygen that keeps the digital everyday life around social networks, e-Commerce, entertainment, smart home, connected car, mobile work etc. alive. Society's demand for data to be processed as economically as possible has given way to the rush of digital participation. There is a need for more modern principles that recognize the enormous volume of data, focus more on the usage and control level, and address data hygiene with clear deletion concepts.

Consent

Consent is considered the core of the processing bases. However, in today's pace of media use and frequency of data processing requiring consent, it has degenerates into an unpopular compulsory exercise and in any case only confronts the individual with an "all-or-nothing" decision. This criticism is not new. Nevertheless, the legislative process for the GDPR recently missed the historic opportunity to fundamentally reform consent. The (stalled) eprivacy regulation would probably cement this outdated understanding for years.

Data sovereignty

A modern data protection law without the possibility of the explicitly expressed will of the individual seems unthinkable indeed. Hence, consent should not be weakened or even abolished, but rather strengthened and lead to real data sovereignty. The discourse term “data sovereignty” needs a generally accepted definition. With a new conceptual orientation of data sovereignty, one could essentially overcome the deficit of voluntariness via a "sovereign consent process" (cf. U. Seidel, LR 2020, 229). This new conceptual orientation assumes a shared data power between the processing body and the data subject (or data provider).

This overcomes the controversies about data reprocessing, non-transparent Big Data processing, and the exaggerated notions of (failed) data ownership ("my data belongs to me"). In this shared data power, processing bodies offer preset data usage options, while individual case usage is done by data providers. Data sovereignty thus establishes a legal claim to a self-designable and thus self-optimizable data use, which has not previously existed in the legal system and which expands the right to informational self-determination.

As part of the digitization of public administration, citizens could use a personal account to track which public authorities process which data about them and for what purposes. In accordance with the “Once-Only Principle,” citizens enter standard information only once in their account and allow public authorities to access it efficiently and transparently on a case-by-case basis. This path to administrative data sovereignty (as opposed to the economic data sovereignty as described above) is already laid out in the German eGovernment Act and should be pursued further by the German government, using Estonia as an example. Data protection problems could be overcome by data trustees and acceptance of such a model among the population could thus be strengthened.

Smart linkage of documentation and documented processes

Data protection is still "paper compliance," with the accountable body's documentation detached from the documented processing operations, data categories, and TOMs. The complexity and dynamic nature of processing operations requires new approaches to combine documentation and documented processes in a smart way. A self-updating processing register, which receives information directly from the processing body's systems and in turn transfers required input to relevant privacy statements, will hopefully become the standard at some point in the future. Real-time linkage to data processing operations reduces the documentation burden while at the same time it increases transparency as well as control options, not only by the individual, but also by contractual partners and authorities.

New possibilities for a European way

The ECJ's Schrems II decision leading to a stricter scrutiny on third-country data transfers has put its finger in the wound of the special problem of data protection in the field of tension with intelligence services. The checks on the level of data protection in the recipient country, which are hardly feasible in practice for data exporters, testify to a certain helplessness in legitimizing international data transfers in times of whistleblowers. Against this background, the European cloud initiative GAIA-X is a welcome approach to strengthening technical data sovereignty in the EU. Although no sealed-off parallel ecosystem will emerge here, especially next to the United States, third-country transfers could be increasingly limited to the result of certain processing operations (just as the case with edge computing). GAIA-X should also be developed as a technical basis for European substantive data sovereignty, e.g., through cloud-based trust center concepts, which could make this digital ecosystem a global pioneer.

Ethics by design/default

Technology will increasingly move into areas where it competes with human behavior. The self-driving car that makes a split-second decision in a dilemma or the voice assistant reserving a restaurant table by phone are no longer visions of the future. "Ethics by design/default" will have to become a central building block in the further conquest of this field. Due to the globalized tech industry, one will not only have to deal with different product designs, but also with different ideas of ethics to win the favor of users. After the Americanization in the 20th Century, intercultural transfer in the 21st Century could also take place through technological market leadership. The EU must strike a balance between data ethics debates and innovation-friendly funding if it does not want to lose out here.

Open Data

We are experiencing a time when the concentration of huge data silos on a few tech giants can no longer be tolerated. The fact that data can be copied at will without loss of quality is increasingly being linked to societal demands for data openness, which should lead to a new dimension of transparency and collaboration. This will result in new regulatory models, such as open data and the use of data trustees.

Government Surveillance

Parallel to the demand for data openness, there will again be a growing "hunger for data" on government level. The debate about data retention in stock might seem harmless when western hunger is also driven by omnipresent surveillance models from other parts of the globe that have an

extensive network of surveillance cameras, facial and gesture recognition, and AI and social scoring. The German Federal Council approved a draft act in March 2021 that went almost unnoticed by the public. Under the act the individual tax ID will lead to a "cross-register identity management" and make individuals identifiable across all public administration registers. In the 1970s, the so-called federal uniform personal identification number was abandoned due to data protection concerns. A corresponding discussion on the possible dangers of the current legislative initiative for the democratic constitutional state would have been desirable, especially due to its ability to be linked with private sector databases.

Data protection is at a crossroads. In data-driven everyday life, with continuously exponentially growing data, data protection must be expanded beyond the classic defensive right and designed to become a sovereign right of participation. Individuals should no longer be protected merely as "data subjects" in a rather passive role but additionally empowered in a new model to become self-designing data sovereigns.

This article was originally published in the *German Journal of Privacy* (*Zeitschrift für Datenschutz*) in German in December 2020.

Hendrik Seidel

Assistant General Counsel

Capgemini

Hendrik Seidel is an in-house lawyer for data protection and data security at Capgemini in Munich.

Ulrich Seidel

Dr. Ulrich Seidel is a lawyer and holder of the German Federal Cross of Merit for the scientific justification of data protection.