

WHITE PAPER

**EU GENERAL
DATA PROTECTION
REGULATION –
SITUATION IN 2019**

.CPC



avocado
rechtsanwälte

EU General Data Protection Regulation – Situation in 2019

Since the EU General Data Protection Regulation (GDPR) took effect, many organizations have been busy implementing the sweeping new data protection standard. A well-established data protection management system is more important than ever. Companies should consider the initial experiences others have made with the GDPR.

Since it took effect on May 25, 2018, the GDPR has led to many, in some cases absurd, misunderstandings. There were stories about kindergarten class photos with faces blacked out, landlords who took down doorbell nameplates, and children's drawing competitions where the winner could not be identified because the organizer, for privacy reasons, recorded only the first names of the participating children. Beyond the media hype, many companies continue to work on implementing the comprehensive GDPR requirements.



From an organizational perspective, the purpose of a GDPR implementation project is to establish a solid position vis-à-vis regulatory authorities and courts in charge of data protection. It is virtually impossible to implement all of the requirements over the medium term.

The GDPR introduced sweeping new obligations. Companies must not only comply with them, but they must also prove their compliance if requested. Many organizations are still in the midst of their GDPR implementation project. At this stage, it is critical to keep an eye on the experiences of other organizations and on the evolution of the risks in order to realign the project to new or changing risks if needed.

BENCHMARK – WHERE DO OTHERS STAND?

Current status of many implementation projects

Although many German companies took little advantage of the two-year lead time before the GDPR took effect, most have completed or at least begun a project to put GDPR regulations in place. Very few companies, however, have been able to fully implement every requirement. In fact, most companies have chosen a risk-based approach **and implemented the “visible” measures first**, such as appointing a data protection officer, creating privacy notices (especially on the web site), and finalizing data processing agreements.

Next milestones

After implementing the “visible” measures, organizations now need to turn their attention to other “necessary” measures. These are GDPR-mandated measures whose absence during an audit by data protection authorities would most likely lead to sanctions. This is why many companies are now focusing on these measures:

- Complete a records of processing activities and implement supporting processes (e.g., for new or modified processing tasks)
- Implement technical and organizational data protection measures
- Implement a process for data protection impact assessment
- Design a deletion concept and implement requirements in all the affected IT systems
- Implement a process for efficient and automated processing of requests from data subjects
- Define a response to personal data breaches and publicize commensurate processes in the company



WHAT ARE THE REAL RISKS?

What have the data protection authorities been doing?

After major panic about the GDPR implementation and predicted fines in the millions or even billions, the data protection authorities were astonishingly quiet in the first few months after the GDPR took effect. At the beginning of 2019, a fine **of 50 million euros** was levied against Google in France. The highest GDPR-related fine in Germany totaled a comparatively low 80,000 euros. According to the media, the German data protection authorities are busy with a number of ongoing investigations. But investigations take a great deal of time, and many data protection authorities are currently (still) extremely understaffed.

The investigations that have garnered attention to date are most focused on:

- Data privacy violations (e.g., due to inadequate encryption)
- **Compliance with transparency obligations** of the GDPR, and
- Use of illegal e-mail advertising.

Moreover, some data protection authorities are conducting large-scale surveys on the implementation of the GDPR, on the data protection organization, or specifically on the correct design of Facebook pages.



According to an Allianz study published in 2018, total damages from cyber incidents amount to 500 billion euros worldwide, making them one of the greatest risks to organizations.

Other risks?

Except for a few cases, little has been seen of the highly publicized wave of formal warnings. Thus far the courts have issued different rulings regarding the legitimacy of formal GDPR warnings. Even if a rise in formal warnings remains possible in the future, they appear to be a relatively low risk over the medium term. The situation is different for privacy-related damage claims. The new class action declaratory proceedings and the European-wide class action discussed at the EU level could make such claims a serious challenge for companies. The risks of possible reputational damage resulting from data protection breaches do remain high.

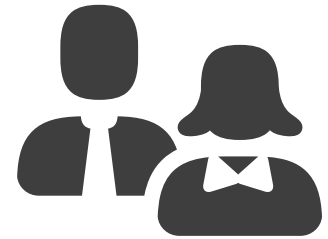
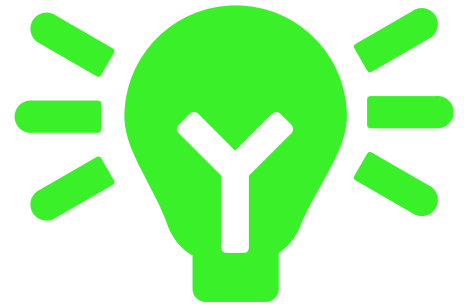
FINDINGS FROM GDPR PROJECTS

In light of the risks that remain very high and the current state of implementation in many organizations, a successful and comprehensive implementation of GDPR requirements continues to be on the agenda of many companies. Based on our experience, the following conclusions can be drawn from GDPR projects that have already been completed:

- A GDPR implementation project can only be effective if it is fully supported at the board and C-level.
- Implementation takes time and patience – but companies can quickly achieve results and continuously drive the implementation forward.
- Data security is not only achievable from a strictly technical standpoint but requires changes in the process and organizational structure.
- Permanent solutions require changes in awareness and behavior on the part of all parties involved.
- This requires early and active engagement of employees who deal with and process personal data every day.

As for data protection regulatory authorities, please keep the following in mind:

- The authorities reward cooperation – possibly even with lower fines.
- Currently, the data protection authorities are overloaded, but planned staff increases can quickly change that.



EXAMPLE OF A SUCCESSFUL IMPLEMENTATION

avocado rechtsanwälte and CPC Unternehmensmanagement AG offer a holistic and proven approach to implementing GDPR requirements. Let us look at one customer in the financial sector.

A B2B financial services provider consisting of multiple corporate entities had set itself the goal of implementing the most important requirements (especially those with external impact) and initiating longer-term measures by the time the GDPR took effect. avocado rechtsanwälte and CPC Unternehmensmanagement AG guided this project from the beginning all the way to its successful completion.

Analysis

To understand which impact the GDPR would have on the company, the stakeholders first conducted a data protection audit which looked at the GDPR requirements against the current situation in the company. The existing organizational and process structure, governance structures (including guidelines and contracts), as well as IT were included in the analysis. Corporate culture and employee-specific factors were also taken into account. (How do employees view the “data protection” issue? What is their current level of knowledge on the topic?)

The result gave the customer a fuller picture of all the challenges as well as the required action items and recommendations for a prioritized implementation timeline. Priorities were set based on what was externally visible, what was necessary, and what made sense for the company.

Design and setup of the implementation project

The chosen measures were split into six content-related workstreams for which designated customer employees assumed responsibility. Overall management of the project was shared by a customer project manager and a consultant. The top management levels were represented by the steering committee.



Implementation was planned in weekly sprints. This approach meant changes were immediately tangible and visible. Moreover, short-term requirements could be included, prioritized, and implemented quickly.

Permanent implementation by including parties affected

Modified procedures and behaviors must be effective. To ensure this is the case, people in the organization must have the right awareness with regard to handling data, accept the new practices, and be trained in the new processes and procedures. In this context, the following strategies have proven valuable:

1 Data protection does not have to be complicated.

Necessary process changes were made on the basis of existing processes and familiar workflows. These changes were developed in workshops together with those involved. The results were lean, customer- and employee-oriented modifications that flowed into compliant processes and were largely accepted by those affected.

2 Data protection is easy to incorporate into day-to-day work.

Together with the employees affected, guidelines and memory aids were created and strategies defined on how to easily integrate data protection requirements into daily workflows. As a result, employee confidence went up and the likelihood of data protection breaches went down.

3 Data protection is a team effort.

These activities were augmented by higher-level and cross-departmental empowerment initiatives in which top management participated. One example was extensive communication on how the information requirements and rights of those concerned would be implemented across the entire customer life cycle and individual departments.

By the time the GDPR took effect, the major data protection requirements had been implemented on schedule and the affected employees could immediately put them into practice.

Broad-based acceptance of the measures on the part of employees and business partners ensures sustainable implementation.



ABOUT AVOCADO RECHTSANWÄLTE

avocado rechtsanwälte has more than 50 lawyers and 75 employees in Berlin, Frankfurt am Main, Hamburg, Cologne, Munich and Brussels. Our activity covers the entire range of commercial law advice with a focus on labour law, banking law, corporate law, real estate law, information technology law including data protection law, public law and litigation. In the fields of information technology and data protection, we advise and represent a large number of companies from all sectors, from SMEs to international group companies.

The numerous mandates we handle include, in particular:

- classic IT projects (introduction of new IT systems or products, SAP projects, ERP systems, e-commerce projects, SaaS, hosting / data centers, support agreements, cooperation agreements, license agreements etc.),
- IT outsourcing and business process outsourcing projects (framework agreements, service level agreements, etc.), cloud computing,
- Data protection and data security issues (implementation of the General Data Protection Regulation “GDPR” in companies, order processing, international data transfers, data protection audits, product-related data protection consulting e.g. in the areas of payment services, mobile devices, social media, smart metering / smart grid, etc.),
- extrajudicial and judicial conflict resolution as well as
- support in dealing with data protection supervisory authorities.
For example, requests for information, controls or fine proceedings.



avocado
rechtsanwälte


avocado rechtsanwälte

Nextower
Thurn-und-Taxis-Platz 6
60313 Frankfurt am Main
T +49 69 9133010
F +49 69 91330119
www.avocado.de



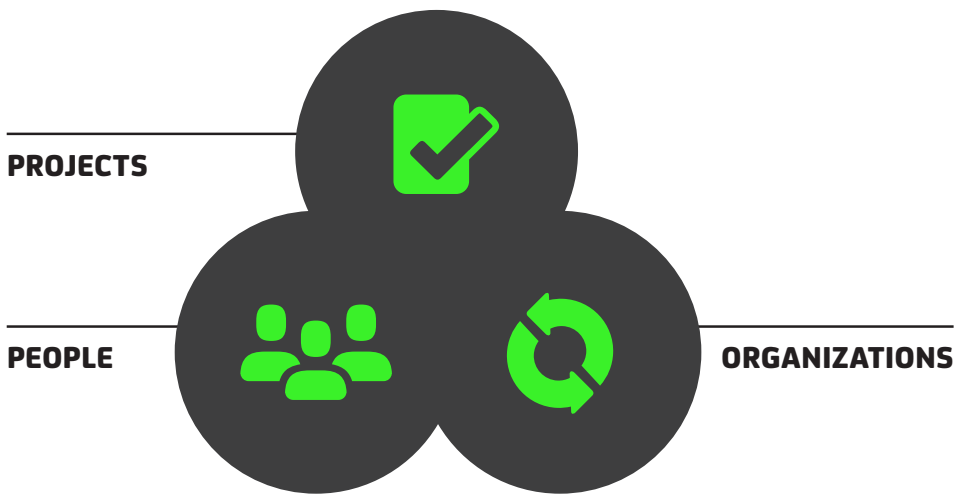
 **JAN PETER VOSS**
PARTNER
T +49 69 913 30 11 32
j.voss@avocado.de



 **PROF. DR. THOMAS WILMER**
COUNSEL
T +49 69 913 30 11 32
t.wilmer@avocado.de

ABOUT CPC

CPC is a leading German based change management consultancy. We are a reliable partner helping corporations and medium-sized companies create lasting change. To effect such change, we follow a holistic, customer-focused approach built around the three core competencies: **People, Projects, and Organizations.**



Over 25 years ago, CPC began its consulting business with a focus on reorganizing medium-sized companies. Today, we are a leading change partner for large corporations. The experience of our 100 consultants proves that stock solutions are not enough because every change initiative is unique. In more than 1500 national and international projects, we have developed a method and format toolkit and have learned to skillfully apply it towards organizational change and to create precise, customized solutions.

As of January 2018, we officially are „**Hidden Champion for Change Management and Implementation**“.

CPC Unternehmensmanagement AG
The Squire 11
Am Flughafen
60549 Frankfurt am Main / Germany
T +49-69-56 03 03 03
F +49-69-56 03 03 05
contact@cpc-ag.de
www.cpc-ag.de

.CPC



CLEMENS HEISINGER
PARTNER
M +49-171-442 35 04
clemens.heisinger@cpc-ag.de



DIRK THATER
ADVISOR
M +49-160-97 43 61 86
dirk.thater@cpc-ag.de