CORE®

OPT-IN

PRIORITY REGULATION GDPR PUTS PRESSURE ON INDUSTRIES WITH A HIGH PROPORTION OF P&L WITHIN THIRD-PARTY MARKETING OF USER DATA

Marc-André Dymala
Christian Everts
Dr. Mirko Schiefelbein

May 2018
COREtechmonitor | Blogpost

Key Facts

- Entry into force of the European General Data Protection Regulation GDPR on May 25th, 2018, Federal and State Data Protection Conference of April 26th, 2018 defines priority of GDPR over Telemedia Act in Germany despite delay of ePrivacy regulation to probably 2019
- GDPR compliant obtaining of user consent to process personal data necessary, however only partially ensured in single sectors – with partly drastic effects on data management and business model
- High pressure to harmonize regulatory requirements and those of the market, especially for media enterprises and marketers

Report

The effectiveness of the sentence: „In relation to national law, the GDPR applies as a matter of priority to all automated processing of personal data as of May 25th, 2018 [...]“ is understood by experts. The Düsseldorfer Kreis – the conference of the independent federal and state data protection authorities on April 26th, 2018 – thereby confirms a regulatory framework – and once again surprises an entire industry. Just as, for example, the financial industry has underestimated the determination of the regulation for a long time, the media industry seems to underestimate the inherent connections between technological opportunities, changing regulatory conditions and the associated changes in decision-relevant parameters until now. This generally assumed that the previous regulations of the Telemedia Act would remain in force until the new ePrivacy regulation came into force, or at least could be based on the so-called legitimate interest according to Art. 6 para. 1lit.f) GDPR, i.e. the processing of personal data was covered by the „legitimate interest“ of the advertiser or website operator. At the same time, the in-house lawyers brought the assessment to the management boards that the interpretation – if to be applied at all – should be mitigated and avoided, for example by referring to the preservation of jobs through supplementary lobbying measures.

Now, however, with a few exceptions, media companies must promptly and comprehensively switch their consent management as well as data usage to an „opt-in“. In addition to contract data processors, media companies and marketers are particularly affected: their business model is largely based on using personal data for the placement of personalized offers across domain and session boundaries.

The precedence of the GDPR is therefore connected with changes compared to the previous structure:

- **Restriction Telemedia Act**
  §§ 12, 13, 15 of the Telemedia Act will no longer apply to assess the legality of the usage of tracking mechanisms as of May 25th, 2018.
- **Establishment of GDPR as a new legal basis**
  Art. 6 para. 1 represents the new legal basis for the processing of personal data by service providers of telemedia.

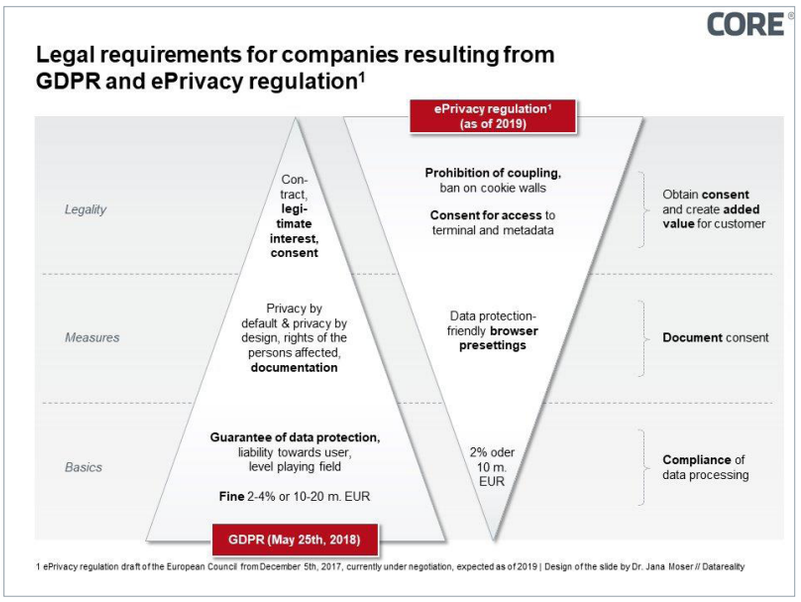


Illustration 1: Requirements of GDPR and ePrivacy regulation

- **Formulation of further principles**
  This encompasses in particular the transparent and for a specific purpose processing of personal data according to Art. 5 Para. 1 GDPR as well as compliance with the guideline of data protection-friendly presettings according to Art. 25 Para. 2 ibid. („privacy by default“).

The result is nothing less than a drastic break within the area of data protection and informational self-determination. In particular, as of May 25th positive opt-in votes by users with regards to the use of their data will be required. The use of tracking mechanisms, for example for the creation of user profiles, requires likewise an informed consent in the form of a clear confirmation by the user, as does data processing.

If the user‘s consent in accordance with the requirements and principles of the GDPR is not available, reduced options for action and stricter sanctions will result cascadingly. Although the consents obtained continue to apply, e.g. for sending newsletters, it can be assumed that in most cases no active consent for the processing of personal data has been obtained in advance. As a consequence, the corresponding collected data may no longer be retained, as in the case of con-sents that do not comply with the GDPR. The consequence of this affects the companies’ vital lifelines: The missing data will make it impossible to personalize offers. Estimates of the extent of this loss amount to an annual drop in sales of up to 30% in the media and marketing industry. It could take months to rebuild the relevant data and analyses – it would take years to rebuild lost trust after published violations.

Another factor, although an indirect one, is exacerbating the situation: Google, for instance, requires from its partners to obtain the consent of users according to GDPR, in order to use Google services. If consent is not given, companies may no longer be allowed to use Google tools and platforms. That would be another harsh blow to the companies‘ ability to act. They would either have to focus on the technology base of their main competitor in media

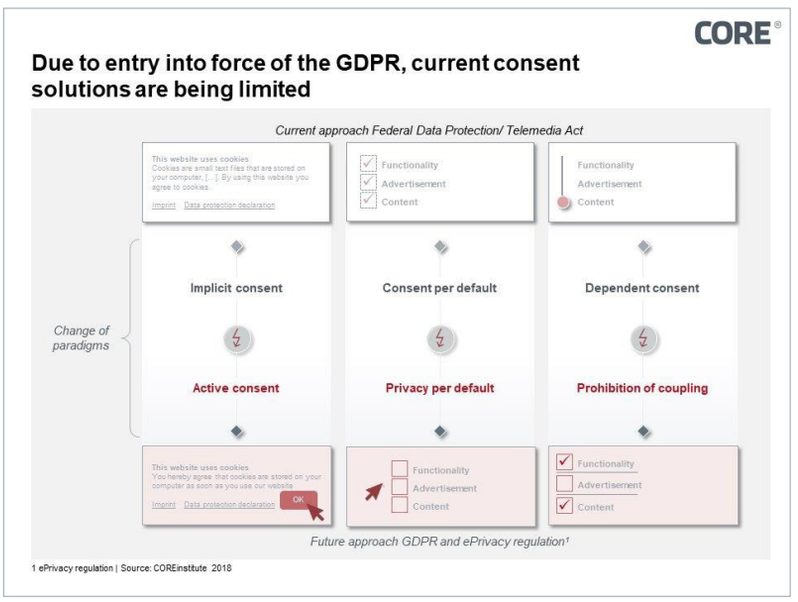


Illustration 2: Paradigmatic change in data protection by GDPR

marketing or enter into high-risk technology investments, whose success depends on the formation of critical masses and the development of network effects. Especially as Google and co. anticipated this development a year and a half ago and are well prepared in the current situation.

In view of the impending loss of the core competence of personalized placement of offers, the task and its urgency are understood: A marketable solution must be formulated as soon as possible for the media and marketing industry in order to obtain users‘ consent for the collection, transmission and processing of personal data, which is earmarked for this industry.

Currently, companies in the media and marketing industry are pursuing different approaches. (1) Individual solutions separately integrate an opt-in layer for individual websites in order to obtain the consent of the users. In contrast, (2) group-specific solutions organize the consent of individual users for several domains. Finally, (3) generic solutions are applied directly to the management of the user‘s accesses. Each of the approaches formulates a particular solution for obtaining consent. However, none of the solutions harmonizes regulatory requirements, functional requirements and technical implementation options in a marketable manner: The range of the individual solutions is too small because no web networks are integrated; group solutions focus solely on the interests of the group companies; the generic solutions pursue a cross-industry approach, which is why they do not fully cover the specifics of individual industries or rather do not produce the necessary transparency with sufficient accuracy.

For the urgent task of creating a GDPR compliant solution for obtaining user consent, three workstreams must be initiated from our perspective with immediate effect:

Scope of the solution: Individual vs. industry-wide

Every company is obliged to implement a GDPR compliant solution. In contrast to the „natural“ path of individual solutions, it may be advisable to join forces industry-wide and establish a standard against

globally operating structures in this non-differentiating area.

How far this standard goes, i.e. whether the solution would cover many needs directly or would be configurable in many areas or by individual companies and associations, has to be discussed. It would be an approach, which on the one hand would have to meet the highest demands for convenience and simplicity, technical security and adaptability, and on the other hand, it would have to stand up to actual standardization by tech companies.

In this context, initiatives with an industry-specific approach should also be con-sidered, e.g. the IAB Framework of the Interactive Advertising Bureau Europe. This framework focuses on the establishment of a standard according to the transparency requirements of the GDPR.

Solution concept: Regulatory, functional, technical

The task is to make the collection of personal data, its transmission as well as its use transparent in the sense of earmarking, to give users the opportunity in detail to decide for or against certain proposals of use, as well as finally to provide a tool for control and, if necessary, subsequent change of decision - certainly as an instrument for the technological emancipation of users.

The solution concept should be guided by harmonizing regulatory requirements, functional-market requirements as well as technical options. This could be synchronized with the transparency requirements of the IAB framework.

Moreover, any lengthy finding phase is unacceptable in the view of urgency. After a short phase of embossing the vision, an iterative approach enables the close linkage of the functional design to the technical implementation. It would be essential to commission interdisciplinary teams in an agile arrangement with extensive decoupling of hierarchical cultures with the implementation and to trust that innovation absolutely requires leaving established patterns. A subse-quent operationalization should take place in established structures of corpo-rates.

Further development: adaptation and integration

There will be many adjustments: the regulatory requirements will be specified by the ePrivacy regulation, and new technical practices will also reveal further potential. It is therefore critical for success to design the process of further development right from the start and parallel to the solution concept and to consider necessary elements of further development in the technical solution design. The main goal should be, to efficiently encounter the expected dynamics of development.

Necessary changes are to be syndicated proactively with the various stakeholders, so the regulator should be understood as an active interlocutor and integrated into the planning. The process for the technical implementation must be designed close to the market, i.e. changes must be integrated as quickly as possible. Governance must be geared to the modularity of the solution.

Résumé

With entry into force of the GDPR on May 25th, 2018, one of the most drastic breaks for data protection and informational self-determination becomes a reality. In concrete terms: the paradigm of an extensive free availability of usage data in Europe is being replaced by the one of active availability and control of users over their data, at least in the target state. This development is to be welcomed from the civil society's perspective, concomitant adjustment processes must be actively accompanied.

Unlike other industries, media companies are particularly affected by the GDPR: The collection, transmission and analysis of data forms the basis for the placement of personalized offers across domain and session boundaries, which again forms the core of their business model.

In view of the fact that media companies and marketers will have developed only partly solutions in time, they are faced with the following choice: to continue previous patterns of action of hierarchical culture with high legal competence and little technical expertise – or to pursue a trust- and competence-based approach, taking into account network policy arguments and network strategic horizons in order to be able to actively participate in new paradigms also economically.

Sources

Düsseldorfer Kreis

[German only:] Position of the Conference of Independent Data Protection Author-ities of the Federal and State Governments, Düsseldorf, 26 April 2018: https://datenschutz.saarland.de/fileadmin/datenschutz/dsk_entschliessungen/95/Positionsbestimmung-TMG.pdf

Federal Court of Justice

[German only:] Press release, No. 78/2018: Federal Court of Justice: Offer of the AdBlock Plus advertising blocker not unfair: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=2018&nr=82856&linked=pm&Blank=1

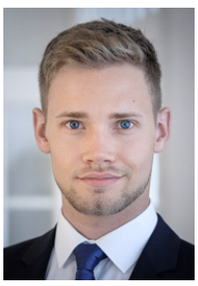
Google

[German only:] „Wie Google deutsche Vermarkter mit vorauseilenden Opt-in-Forderungen quält", in: http://www.horizont.net/medien/nachrichten/Datenschutz-Wie-Google-deutsche-Vermarkter-mit-vorauseilenden-Opt-in-Forderungen-quaelt-166612

IAB

IAB Europe 2018, https://www.iabeurope.eu

Authors



Marc-André Dymala is Transformation Associate at CORE and supports clients in optimizing complex IT processes. With a double Master's degree in economics and international study experience, he supports IT transformation processes from strategic alignment to implementation.

Mail: marc-andre.dymala@core.se

Marc-André Dymala

Christian Everts is Transformation Manager at CORE and in particular adds his regulatory experience to support our clients. Prior to joining CORE, Christian served as Compliance Manager. The focus is on implementing regulatory requirements in international companies.

Mail: christian.everts@core.se

Christian Everts

Dr. Mirko Schiefelbein, as Transformation Director, is responsible for the research activities of the COREinstitute. His focus is on researching technology-induced changes in organizations. Under his leadership, a large number of publications has been published and repeatedly taken up in the context of technology transformations.

Mail: mirko.schiefelbein@core.se

Dr. Mirko Schiefelbein

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
https://institute.core.se
Phone: +49 30 26344 020
office@coreinstitute.org

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zurich | Helvetia
https://www.core.se
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
https://www.core.se
Phone: +44 203 319 0356
office@coretransform.co.uk

COREtransform MEA LLC
DIFC – 105, Currency House, Tower 1
Dubai P.O. Box 506656 I UAE
https://www.core.se
Phone: +971 4 3230633
office@coretransform.ae