ePrivacy

Position paper

Shaping ePrivacy in an up-to-date and practical way – adjust on TTDSG-implementation

Data is a valuable resource. They are just as indispensable for science and innovation as they are for communication and competitiveness. Europe must evolve into a knowledge-based data economy. Simultaneously, privacy and confidential use of Internet-enabled terminal equipment, i.e., all devices/applications that can be connected to the Internet, represent a high-level protected property. It is a government task to provide a reliable legal framework with clear, competitive, internationally coordinated political conditions. In this framework data processing is made possible, but at the same time the legitimate interests of protecting citizens and companies are safeguarded. At the EU level, the ePrivacy-Regulation (ePR) is currently being drafted in trilogue. Its introduction is not expected until 2024 at the earliest. Until then, the Telecommunications-Telemedia-Data-Protection-Act (TTDSG) will apply in Germany. This has implemented Art. 5 sect. 3 of the ePrivacy-Regulation since December 1st, 2021.

The TTDSG affects all internet-enabled applications such as websites, web applications, apps, Internet of Things (IoT), reach-measurement and reach-analysis. The current implementation entails considerable financial and personnel expenses for the companies. It significantly restricts digital designs compared to foreign countries through a very narrow interpretation by Data Protection Authorities. The lack of clarification in the explanatory memorandum to the Act leads to uncertainties in implementation. In order not to jeopardize Germany's competitiveness, the interpretation of the TTDSG must be corrected. The aim is to avoid overregulation and ongoing adjustments, to strive for uniform legal views and practice-oriented handling throughout the EU, and to strengthen digital innovations. At the same time, these regulations should be technology-neutral as well as coherent and consistent with existing regulations (e.g., GDPR). New legal developments (payment with data) and existing established business models must not be restricted.

The Position „Shaping ePrivacy in an up-to-date and practical way – adjust on TTDSG-implementation" was adopted by the plenary assembly of the Chamber of Commerce and Industry of Munich and Upper Bavaria on March 16, 2022 with 53 votes in favor, 0 against and 1 abstention.

IHK München und Oberbayern

enterprise europe network
Wir stehen Unternehmen zur Seite

Wirtschaft für Zukunft

The following requirements must apply to TTDSG / ePrivacy

1. Modernizing the law – using IT as an opportunity

A digital world needs a reliable, practicable and technology-neutral legal framework. Simultaneously, the protection of privacy and the confidential use of Internet-enabled terminal equipment must be safeguarded. Here, ePrivacy legislation must be examined to see if it needs to be adapted and, if necessary, modernized. ePrivacy regulations should be consistent and coherent with other sets of regulation, such as the GDPR and its legal obligations (including the obligation to ensure state-of-the-art security) or payment with data, which has been permissible since January 2022.
Legitimate needs of the Internet world must be legally secured. For example, advertising should be able to reach users geolocated, e.g., using generic geo-IP information. The Conference of Data Protection Authorities (DSK) has not commented on „services with additional functions" or „payment with data" in its „Guidance on Telemedia". Practical solutions are needed here, so that the media industry, for example, can offer legally secure contractual models for modern information and consumption needs.

2. Clear and understandable legal framework

The legal framework to be created must be clear and understandable.
If necessary, the legislator must provide implementation information on the grounds for consideration and thus ensure clarity itself. Under no circumstances should interpretation be the sole responsibility of the Conference of Data Protection Authorities. ePrivacy rules must be formulated in accordance with the data protection law requirement of transparency, i.e., in clear language that SMEs can understand. Legal requirements must be checked in advance in practice checks before they enter into force.

3. No over-regulation

The ePR will open up more scope for data processing. With this in mind, over-regulation and adjustments to changing legal requirements and their interpretation should be avoided during the transition period. Established technologies and business processes must not be jeopardized as a matter of principle. It must be possible to retain the Transparency and Consent Framework (TCF) as a standard consensus procedure. Further bloating of data protection rules must be avoided. The ePR should not further tighten the high requirements of the EU's existing ePrivacy regulation.

4. Strengthen competitiveness

ePrivacy is a marketing tool if it is regulated in a future-oriented and technology-neutral way. Gold-platinum standards jeopardize competitiveness and must be avoided both in the transition period with regard to Germany and with regard to ePrivacy in an international context. Research and development should continue to be carried out in Europe and not be affected by migration abroad. For example, companies need legally secure procedures for customer models in order to be able to offer product optimization on a regular basis. In a digital society, data is processed in ever new contexts. For these changes in purpose, a knowledge-driven modern economy needs robust legal foundations. As such, ePrivacy provides only for consent for data processing. Particularly in the case of IoT, a legitimate interest of the economy should also legitimize data processing as a legal basis - as in the GDPR. In the case of „services with an additional function" and „payment with data", contractual regulations should also be permissible.

5. Do not create unnecessary bureaucracy

State intervention must be subject to the requirement of effectiveness. Information and documentation requirements must be proportionate. Appropriate solutions for information obligations must be rethought for certain constellations of cases (e.g., moving vehicles).
New legal frameworks must be appropriate. Adaptations of websites, apps or IoT cause high personnel and financial costs. These also entail an adaptation of data protection documentation. The state must not overburden companies with costs, obligations, and ongoing new adaptations. Mandatory technical protection measures must be implemented without the need for consent. An assessment of necessity purely from the user's point of view, as strictly interpreted by the DSK in its Guidance on Telemedia, falls short of the mark. The legitimate concerns of the business community must be considered appropriately.

6. Enable data transfer legally secure

A knowledge-based data economy knows no borders. Therefore, in a digital world, access to and reading of end devices must be protected, regardless of whether this information is located in or outside Europe. Uniform global standards for this and legal certainty for transatlantic data transfers are therefore indispensable. Transnational regulations are needed that enable more comprehensive data transfers than previous legal instruments, such as Standard Contractual Clauses (SCC), can do. Bridges must be built between different legal regimes. After all, business demands uniform international standards, not many. Reorganizing corporate structures simply to avoid violating the legal requirements of other countries is not a solution.

7. Uniform standards in the EU

It is to be welcomed that the ePR will standardize and harmonize the ePrivacy rules in the EU. The ePR should contain specifics in the recitals and thus directly ensure legal clarity. Differing opinions of Data Protection Authorities, e.g., on questions of range measurement, should be harmonized by then at the latest. Prompt standardization of legal interpretations would already be desirable. The ePR will give companies more legal scope. In this respect, it should enter into force contemporary.

8. Needs of SMEs

In a digital world, SMEs increasingly have to offer goods and services online. Designing a legally compliant website has become an insurmountable challenge for many companies. It is time-consuming and requires specialist expertise to create a legally compliant data privacy statement in compliance with the law. SMEs in particular cannot afford the high financial outlay involved. A two-stage check according to TTDGS/ePrivacy and the GDPR requires explanatory and advisory measures to make the regulations feasible for SMEs as well. Data processing based exclusively on consent under ePrivacy hits SMEs particularly hard. This is because large platform operators obtain consent much more easily than SMEs. In this respect, the ePR should take greater account of the needs and practical reality of SMEs and provide for facilitations or exceptions for SMEs in order to avoid distortions of competition. For the implementation of legal requirements, the business community must have appropriate adaptation periods and alternatives that are in line with practice.

Contact:
Rita Bottler @ rita.bottler@muenchen.ihk.de

Design: ideenmuehle.com, photo credit: AdobeStock © RoBird