LEGAL UPDATE
Data Protection
Cologne, 20 December 2017

GÖRG
YOUR BUSINESS LAWYERS

Protection of Data Concerning Health under the General Data Protection Regulation (GDPR)

Dr. Katharina Landes
Dr. Katja Kuck

The General Data Protection Regulation (EU) 2016/679 (GDPR), which was adopted in 2016, will take effect on 25 May 2018. At the same time, the new Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) will replace the version currently in effect.

The new legislation will also result in changes as regards the protection of data concerning health and will therefore be relevant for companies and other organizations whose business activities involve dealing with such data (physicians, hospitals, healthcare centers, vendors of medical products, healthcare service providers, laboratories, etc.).

Due not only to the many imprecisely defined legal terms in the GDPR, but also to the lack of clarity as regards the relationship between the GDPR and existing provisions governing specific areas such as, for example, the healthcare and social welfare sectors (e.g., social codes, legislation of the various states governing hospitals, etc.), many questions remain to be addressed in respect of the implementation of the GDPR at the practice level. In addition, the various escape clauses available to national legislatures mean that the GDPR also falls short of achieving uniformity in the area of European data protection legislation.

Definition of Data Concerning Health under the GDPR

Under the GDPR, data concerning health are "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*".

Such data include primarily personal data that make it possible to draw direct conclusions as regards the health status of an individual (e.g., information on medical findings, diagnoses, laboratory results, etc.), and to be sure independently of the origin of the data, i.e., regardless of whether they are obtained by a physician, pharmacist or any other healthcare professional, a health insurance provider or through the use of a health app.

Additionally, such data may under certain circumstances also include data that are considered health-related insofar as they may make it possible to draw conclusions as to the health status of an individual only indirectly or in combination with other data (e.g., information on weight, dietary habits, stays in healthcare or related facilities, use of medicines, etc.).

Prerequisites for the Processing of Data Concerning Health

As is also the case under the current version of the Federal Data Protection Act, the GDPR will permit the processing of personal data that fall into certain categories, including data concerning health, only with the valid consent of the respective data subject or on the basis of any of the prerequisites enumerated in Art. 9 of the GDPR (in the form of exceptions to a general rule). Such particularly sensitive data may therefore be processed only subject to stringent limitations (see more on this below).

Requirements for Consent under Data Protection Legislation

The valid consent of the data subjects will thus regularly be an important consideration when dealing with data concerning health. However, the provisions contained in the GDPR set high standards for valid consent; in particular, consent must be freely given and informed.

Compulsory Consent

Art. 7(4) of the GDPR contains a new legal hurdle. According to this provision, the voluntary nature of consent will regularly be open to question whenever execution of a contract is contingent upon consent to process such personal data which is not necessary for the performance of that contract.

The provision contained in recital 43 of the GDPR further stipulates that a consent can be assumed to not have been freely given if the data subject is not offered the possibility of consenting to different processing operations separately although this would be appropriate in the given case. The GDPR does not, however, reveal precisely what is meant by different processing operations (e.g., different types of processing or processing for different purposes) or when separate consent would be *appropriate*.

It is thoroughly possible to construe the provision to mean that the controller is now required to provide separate opt-in boxes for each of the various processing operations involved to obtain valid consent. Whether opt-in boxes are to be provided and, if so, to what extent must be decided in the individual case.

Duties to Provide Information

According to Art. 13 and 14 of the GDPR, the controller must fulfill significantly more exhaustive duties in terms of providing data subjects with information than even under the Federal Data Protection Act (old version) before processing personal data. For example, one new requirement is that the controller must specify the legal grounds for processing personal data and the term of its storage. The GDPR does not clearly specify whether the omission of such mandatory information renders consent invalid. According to recital 42, the data subject must be informed "at least" of the identity of the controller and the intended purposes of processing. The fact that omission of other information may cause consent to become invalid under certain circumstances should, however, also be obvious.

Formal Requirements

A written-form requirement for consent as previously required by the third sentence of § 4a(1) of the Federal Data Protection Act (old version) no longer exists under the GDPR. In fact, other forms of consent will also regularly be considered sufficient as long they constitute a clear and affirmative act (no opt-out). In the case of special categories of personal data – which means also in the case of data concerning health – "explicit" consent is required, which means the possibility of relying on implied consent is excluded.

However, since the controller will have to be able to prove that consent has been given, it will not be possible to avoid written documentation of consent in practice for reasons of legal certainty.

The Key Clause: § 22(1) no. 1 b) of the Federal Data Protection Act (new version) in Conjunction with Art. 9(2) h) of the GDPR

With § 22(1) no. 1 b) of the Federal Data Protection Act (new version), which regulates the processing of special categories of personal data, the German legislature adopted the escape clause contained in Art. 9(2) h) of the GDPR virtually verbatim and as a result for the most part retained the key clause permitting the processing of data concerning health previously found in § 28(7) of the Federal Data Protection Act (old version).

According to § 22(1) no. 1 b) of the Federal Data Protection Act (new version), special categories of personal data may be processed for the following purposes

- preventive healthcare,
- assessment of the occupational health of employees,
- medical diagnosis,
- care or treatment in the areas of healthcare or social services,
- administration of systems and services in the areas of healthcare and social services,
- or on the basis of an agreement between the data subject and a healthcare professional.

if necessary and the respective data are processed by or under the responsibility of physicians or other persons who are bound to an equivalent professional secrecy.

The permissive rule thus implies that processing must be carried out by a member of the professions bound by a professional secrecy pursuant to § 203 of the German Criminal Code (*Strafgesetzbuch* – StGB). Incidentally, § 203 of the Criminal Code was also recently amended in order to allow members of professions who are subject to professional secrecy requirements to outsource data processing, which is already allowed under data protection legislation.

Special Provisions

In Germany, there are many special laws that cover specific areas when it comes to the protection of data concerning healthcare and social services (examples include provisions contained in the social codes, legislation governing the hospitals in the various states or the provisions related to religious facilities).

It is not yet possible to state conclusively what the status of these laws relating to special areas will be under the GDPR and in particular whether it will be possible to have all of these laws subsumed under one of the escape clauses contained in Art. 9 of the GDPR, or whether this will require remedial action by the German legislature. In any case, a corrective draft for Social Codes I through III, VII, IX, X and XII already exists with Social Code V to follow.

Conclusions

In view of the very hefty administrative fines now in effect for violations of data protection law (up to € 20 million or 4% of total (!) worldwide annual group turnover), we recommend that companies take implementation of the requirements of the GDPR seriously and determine whether their organizations treat data concerning health in compliance with (new) requirements. This will apply in particular in view of the current uncertainties in the area of the protection of data concerning health and the patchwork of special laws for individual areas found in Germany.

Note

Our Offices

GÖRG Partnerschaft von Rechtsanwälten mbB

BERLIN
Kantstraße 164, 10623 Berlin
Phone +49 30 884503-0, Fax +49 30 882715-0

COLOGNE
Kennedyplatz 2, 50679 Köln
Phone +49 221 33660-0, Fax +49 221 33660-80

FRANKFURT AM MAIN
Neue Mainzer Straße 69 – 75, 60311 Frankfurt am Main
Phone +49 69 170000-17, Fax +49 69 170000-27

HAMBURG
Dammtorstraße 12, 20354 Hamburg
Phone +49 40 500360-0, Fax +49 40 500360-99

MUNICH
Prinzregentenstraße 22, 80538 München
Phone +49 89 3090667-0, Fax +49 89 3090667-90