Whitepaper

SKW Schwarz

October 2023

Data protection in the use of medical devices

Content

A. Introduction

Whether X-ray or ultrasound devices, pacemakers or health apps: Medical devices have long been an integral part of patient treatment and are playing an increasingly important role in the provision of healthcare services. Digitalization in particular is playing an increasingly important role in the further development of these products, as they are increasingly being equipped with digital functions. However, this digital progress is also associated with new challenges in terms of data protection and data security: The use of such products results in the processing of a large amount of personal data. In order to adequately protect this data, the parties involved, above all manufacturers and users, must comply with data protection regulations. Because as important as medical treatment is, the protection of personal data must not be ignored.

So what do manufacturers need to consider with regard to data protection when developing medical devices and what do users need to look out for when using these medical devices in order to adequately protect the data of data subjects? These and other questions are the subject of the following whitepaper and will be examined in more detail.

B. Medical Devices

I. Definition

In order to understand the data protection issues, it is first necessary to clarify what is actually meant by a medical device. The term medical device is defined in the Medical Device Regulation (hereinafter "**MDR**") under Article 2 para. 1 MDR and refers to all products that are intended by the manufacturer to diagnose, monitor, alleviate and treat diseases and injuries of patients.

Article 2 para. 1 MDR states the following:

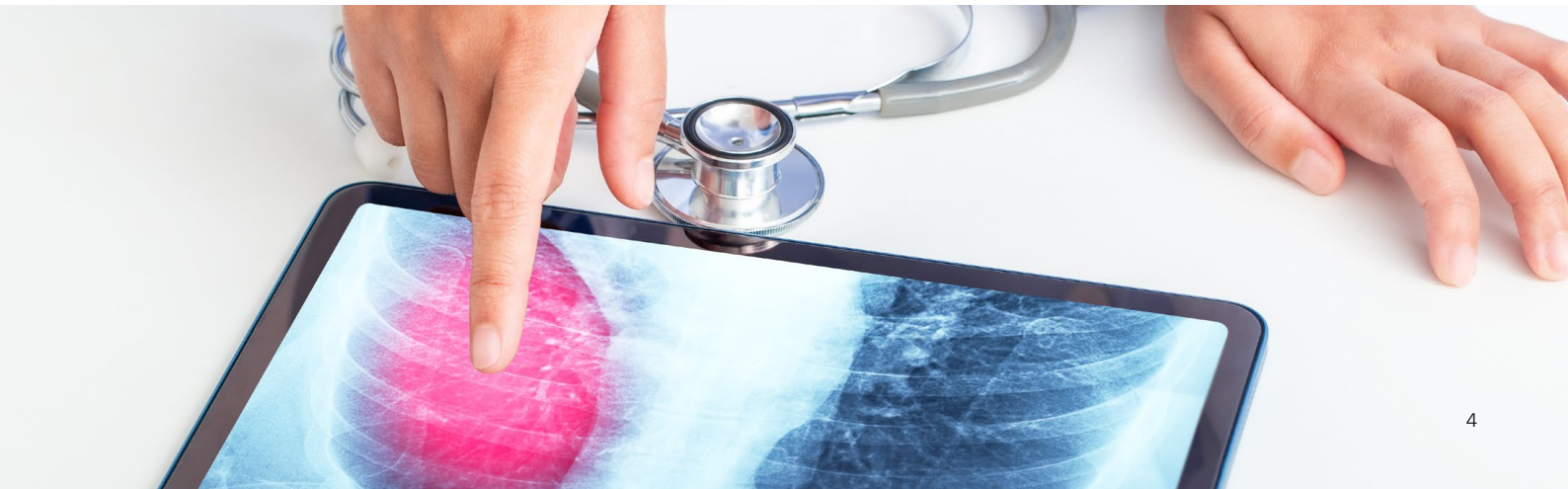
"A medical device means an instrument, apparatus, appliance, software, implant, reagent, material or other article which, according to the manufacturer, is intended for human beings and which, alone or in combination, is intended to fulfill one or more of the following specific medical purposes:

- diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of or compensation for injuries or disabilities,
- examination, replacement or modification of the anatomy or of a physiological or pathological process or condition,
- obtaining information by the in vitro examination of specimens derived from the human body - including from organ, blood and tissue donations samples

and whose principal intended action in or on the human body is not achieved by pharmacological or immunological means or metabolically, but whose mode of action can be supported by such means."

The wording of the MDR therefore makes it clear that qualification as a medical device is fundamentally dependent on depends on the intended purpose.

Medical devices are divided into the four risk classes I, IIa, IIb and III according to the MDR.



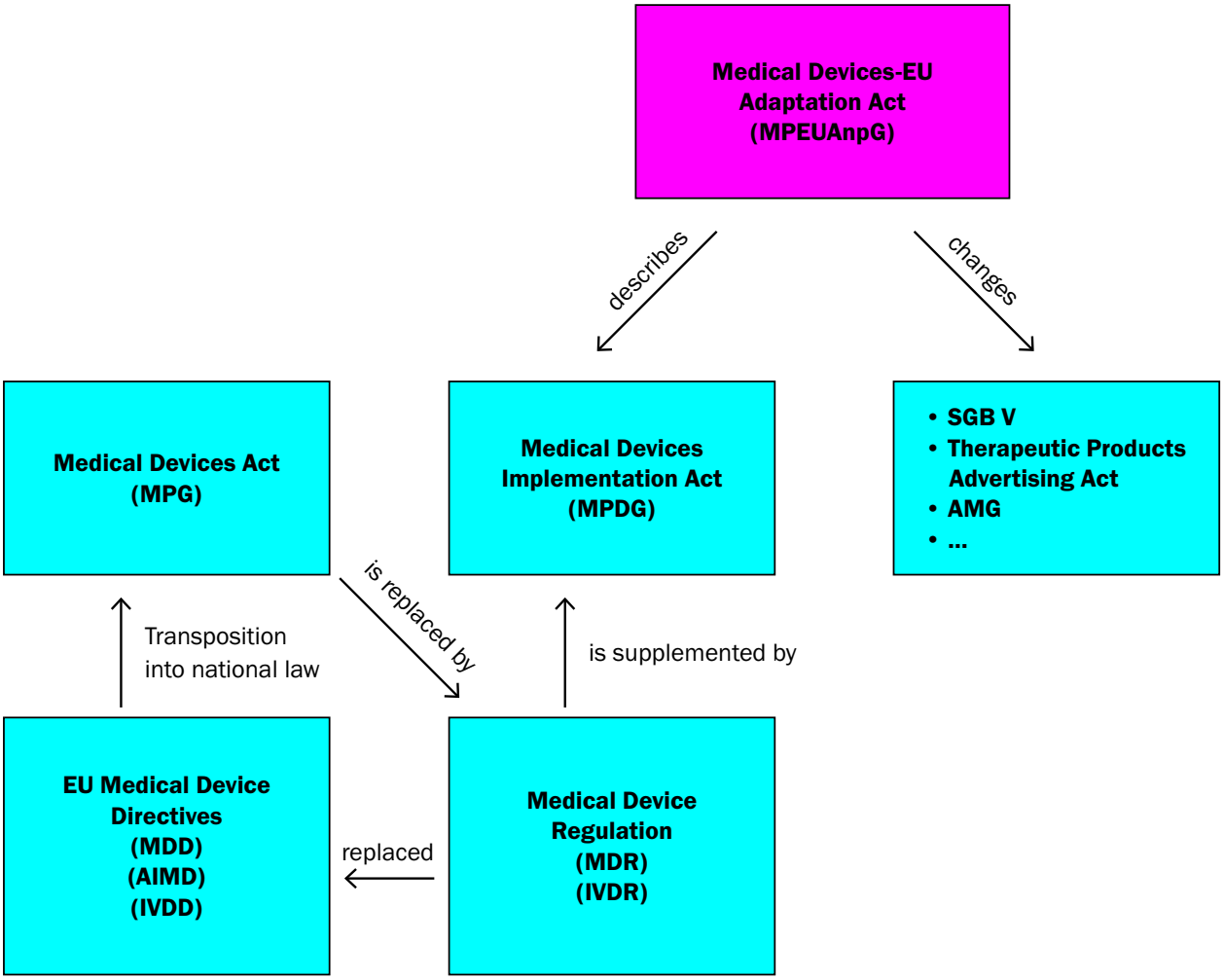
II. Examples

Medical products (+)	Medical devices (-)
• **Class I: Low risk** e.g: Reading glasses, wheelchairs, clinical thermometers • **Class IIa: Medium risk** e.g: Hearing aids, ultrasound devices, X-ray films • **Class IIb: High risk** e.g: X-ray machines, infusion pumps • **Class III: Very high risk** e.g: Hip and knee joint implants, cardiac catheters, breast implants	• Pharmaceuticals • Hospital information systems, provided they only support patient management (such as appointment scheduling or insurance and billing purposes) Cardiac catheters, breast implants

III. Laws and Regulations

The Medical Devices Implementation Act (hereinafter "**MPDG**") has been binding for manufacturers, operators and other stakeholders of medical devices since May 26, 2021. The MPDG supplements the MDR and the EU Regulation for in-vitro diagnostics (EU) 2017/746 (In-vitro Diagnostics Regulation, hereinafter "**IVDR**") with national requirements. The MPDG replaced the previously applicable Medical Devices Act (hereinafter "**MPG**"), whereby the latter served to implement the EU Medical Device Directives (MDD, AIMD, IVDD). The MPDG was introduced as part of the Medical Devices EU Adaptation Act (hereinafter "**MPEUAnpG**"), whereby the MPEUAnpG also provides for amendments to other laws (e.g. SGB V, Therapeutic Products Advertising Act and Medicinal Products Act). The MPDG and the EU Medical Devices Regulations have the joint aim of regulating the handling of medical devices with regard to placing them on the market and putting them into service, thereby ensuring the safety, suitability and performance of the products and guaranteeing adequate protection for patients, users and third parties.

The following diagram is intended to illustrate the most important regulations:



IV. Manufacturers of medical devices

When talking about medical devices and data protection, the first question that arises is which actors in the chain are actually obliged to protect the data of data subjects when using medical devices within the meaning of the GDPR and other accompanying laws.

At first glance, the answer seems obvious: Users of medical devices, such as clinics or medical practices, are primarily responsible for compliance with data protection. After all, they are the ones who collect patient data for the purposes of treatment or monitoring, and subsequently store it.

However, it is often not as simple as it seems at first glance. If you take a closer look at the requirements of the General Data Protection Regulation (hereinafter referred to as "**GDPR**"), another player in the chain emerges: The manufacturer of medical devices (hereinafter referred to as "**manufacturer**"). It is true that manufacturers are only controllers within the meaning of the GDPR in certain constellations and therefore do not have comprehensive data protection obligations in the "classic" use cases of medical devices - especially when it comes to the "mere" provision of the medical device - like a controller, such as carrying out a data protection impact assessment. However, they regularly act as processors in this respect and must also comply with some obligations under the GDPR in this context, such as maintaining a processing directory in accordance with Article 30 para. 2 GDPR (see section IV. 5).

In addition, manufacturers have a great interest in offering their products to the widest possible audience once they are on the market. In order for them to achieve this, they should urgently ensure that they make it easier for users of medical devices (hereinafter referred to as "**users**") to implement data protection when using these products later on. In accordance with Article 25 GDPR, this can already be taken into account during the product development phase. While para. 1 concerns data protection-friendly technology design (so-called **privacy by design**), para. 2 regulates the data protection-friendly default settings of the medical device (so-called **privacy by default**). Privacy by design means that the product must be designed to be data protection-friendly. This means that risk-based, effective and appropriate technical and organizational measures must be taken for the specific product in order to protect the rights of data subjects as far as possible. Privacy by default, on the other hand, concerns the default settings of the medical device. With regard to the principle of data minimization, these must be designed in such a way that only data that is necessary for the respective processing purposes is used. Article 25 GDPR does not specify which specific measures should ultimately be taken during development. The regulation is deliberately kept abstract and provides plenty of scope to remain technology-neutral and adapt to technical developments. In this respect, manufacturers should view their own products through the customer's data protection lens. A win-win situation for both sides: While manufacturers can offer potential customers data protection-compliant and attractive products and thus boost their sales opportunities on the market, users will find it much easier to meet their data protection requirements. In this respect, data protection and data security should be a high priority for manufacturers during product development. Other data protection use cases from the manufacturer's perspective include conducting clinical trials (before and after the product is placed on the market) as well as research and quality assurance for their own purposes (outside of regulatory requirements). However, the latter cases are very specific - also in terms of data protection law - which is why they are not the focus of this whitepaper. In contrast, the following is intended to answer "classic" data protection issues that typically arise when providing a corresponding application. Further legal requirements are of course also possible if the classic 3-person relationship (patient, user and manufacturer) addressed here is not involved.

Regardless of whether they are manufacturers or users of medical devices, all of the data protection principles set out in Article 5 para. 1 GDPR must be observed. These include the lawfulness of data processing, purpose limitation, data minimization, transparency, data accuracy, storage limitation, the principle of data security and accountability.

How this can look in concrete terms and what manufacturers should pay particular attention to is shown in detail below.

1. Technical Implementation

During the development phase, manufacturers should implement certain technical functionalities in their medical devices in order to support users in complying with data protection regulations. The following points should therefore be considered right from the start of the development phase:

a) Encryption

→ Manufacturers should ensure that communication and data transfer via interfaces between the medical device in question and other technical systems, as well as subsequent data storage (particularly in the case of cloud-based tools), is encrypted. In order for the product in question to be "attractive" for the user, the data should be secured throughout the entire life cycle - in accordance with the state of the art.

b) Authorization concept

→ As part of product development, manufacturers should also ensure that a detailed authorization concept is in place to guarantee data protection-compliant use. In this way, the personal data to be processed is given a high level of protection, as only those employees who have been actively authorized are granted access to the medical device. In the event that an employee should subsequently require more rights, the necessary adjustments should be made deliberately and to the extent required.

c) Clustering of the storage system

→ Furthermore, manufacturers are also well advised to ensure that the storage system is clustered with regard to the storage of the respective data for medical devices, thereby distributing the data across different systems. Here is an example: A hospital uses a cluster-based X-ray machine. The medical images captured by this X-ray machine are not stored locally on the machine, but are replicated on several storage nodes in the network. If one server fails due to a hardware failure or a natural disaster, the images are still available on the other servers. This ensures that the medical data is not lost and that patient care is continuously guaranteed. In this respect, the clustering of medical devices offers increased failure and data security to ensure the integrity of the stored data.

d) Archive format

→ With regard to the archiving of data, the archive format as a whole should be designed in such a way that the readability of the data is also ensured in the future. To this end, manufacturers should in particular use open standards that are supported by a wide audience. For example, DICOM (Digital Imaging and Communications in Medicine) is a widely used open standard for the transmission and storage of medical images and the associated information. DICOM is used by medicalimaging devices such as X-ray machines, CT scanners and ultrasound devices to store and exchange images in a standardized format and exchange images in a standardized format and to ensure access to this medical data. In addition, manufacturers should also provide comprehensive documentation on how, for example, the archive format is structured and how it can be accessed.

e) Remote maintenance

→ In the event that external service providers take over the remote maintenance of medical devices, special attention should be paid during the development of the medical device to ensure that no personal data is disclosed to these service providers (principle of data minimization). Where possible, access should be limited to the disclosure of technical data only. To this end, personal data and technical data should be stored in separate tables in advance as part of product development. As manufacturers generally take over remote maintenance, they should therefore transparently explain to users which specific data they have access to and how the individual data streams are structured. If it is not possible to restrict access, the stored data should alternatively be pseudonymized, for example, so that no personal reference can be established in this way. Furthermore, it should be ensured that the respective user always grants the service provider (digital) access authorization before the remote maintenance work begins. As long as such authorization has not been granted, it is not possible for the service provider to access the medical device and thus the data.

f) Deletion

→ In line with the principle of storage limitation, manufacturers should also ensure that individual data can be deleted automatically at different times. In this context, the implementation of an automated deletion concept is a good idea. If this is not possible for technical reasons, an anonymization of the data could alternatively be integrated into the system in order to prevent the creation of a personal reference. However, it must of course be noted that anonymization is subject to strict data protection requirements. The procedure must therefore be suitable for ensuring that no one (i.e. neither the user nor the manufacturer) is able to (re-)establish a personal reference with reasonable effort.

g) Updates and security patches

→ Manufacturers should also provide regular updates and security patches to close vulnerabilities and security gaps. In case of doubt, they know their products best and therefore have the necessary know-how to develop and use the appropriate products. In this way, users can ensure that their products are up to date in order to counter any data protection incidents from the outset.

h) Support with data protection audits

→ Manufacturers can also provide important support by helping their customers to carry out data protection audits. data protection audits. The following can provide significant assistance provide the information and documentation required for such audits. required for such audits.

2. Provision of data protection information

As already explained at the beginning, in the constellation illustrated here, users as responsible persons are regularly obliged to comply with the formal requirements laid down in the GDPR. In order to be able to meet these requirements properly, users need some important information. For example, when conducting a data protection impact assessment, users need to understand the data flows related to the medical device in order to assess whether there are high risks to the rights of the data subjects. In these cases, manufacturers can provide assistance and increase transparency, especially as they ultimately have the necessary know-how. As a rule, medical devices already specify or imply a certain amount of data due to the functionality provided. Manufacturers should therefore provide additional documents in addition to the medical device, such as FAQs or a whitepaper with data protection information for their customers, including e.g. indicates how personal data is collected, processed, stored and protected by the medical device. In addition, a detailed description of the respective data flows should be provided. In this respect, it is advisable to draw up such model documents on a regular basis and to make them available to the customer. This is the only way to ensure that users are able to comply properly with their obligations under the GDPR.

Important:

If the manufacturer of a medical device should (have to) process the respective data also for its own purposes, this information should also already be incorporated into a corresponding model document. In particular, in such cases, very careful consideration should be given to the data protection legal basis on which such processing for own purposes may be based. This will depend on the nature and background of the data processing, which is why no overall classification can be made in this respect. However, it will need to be clarified regularly whether the patient's consent is appropriate or even necessary, or whether, as a legal basis may be used, it is not necessary.

3. Provision of sample documents

Against this background, manufacturers are also well advised to keep some data protection standard documents, such as a contract for order processing, data protection impact assessments, data protection notices or a written deletion concept, which are tailored to the specific product and can be made available to potential customers or users prior to the use of the medical device.

4. Training

Manufacturers should also provide training to users in the handling of the medical device. As the manufacturer of the respective medical device, they bring with them the necessary knowledge on how to use the product in accordance with its intended purpose and how to be operated by users. In this respect, the provision of training should be another part of their offer. In this way, data protection risks due to improper operation can be reduced. This can be e.g. also include the provision of additional training materials such as user manuals and guides to help users understand and implement best data protection practices.

5. Demarcation issues

As already shown, a multitude of constellations are conceivable in which manufacturers of medical devices (must) process personal data for their own purposes. This can be e.g. in order to comply with regulatory requirements or, for example, to increase its own efficiency (i.e. for research and/or quality assurance). Manufacturers are therefore regularly faced with the major question of whether they (still) act as processors with regard to the data processing in connection with the medical device or rather are responsible for the data processing – possibly also jointly with the user.

Processor within the meaning of Article 4 No. 8 GDPR is any natural or legal person, public authority, institution or other body that processes personal data on behalf of the controller. A classic feature of this is the purely instruction-bound processing for originally "foreign" purposes. On the other hand, joint responsibility is to be assumed if at least two controllers jointly determine the purposes and means of processing. The legal classification of this issue is undoubtedly extremely difficult and depends on various factors. Thus, if manufacturers e.g. undertake various processing operations during the use of a medical device, they should always check whether they are actually (only) acting as a processor before the start of data processing. Constellations are also conceivable in which different data processing operations have to be evaluated in a differentiated manner. For example, it is conceivable that the provision of IT support services is subject to order processing, while the subsequent use of the data for own purposes falls under a (possibly joint) responsibility. Depending on which of these two alternatives is considered, the respective contract between the user and the manufacturer must be prepared and signed. In the case of order processing, one might think of the conclusion of a contract for order processing.[1] A joint responsibility, on the other hand, entails the conclusion of a socalled joint controller contract.[2] The latter requires a detailed and clearly understandable agreement between the controllers, e.g. with regard to the question of who must specifically comply with which data protection requirements.

Producers are therefore strongly advised to clarify these demarcation issues before the start of data processing and to check whether they are acting as processors or joint controllers, in order to draw up and sign the corresponding contract with the user.

6. Obligations for manufacturers to act

In order to be on the safe side of data protection, manufacturers should keep the following three aspects in mind when developing and making available their medical devices:

- Compliance with regulatory requirements (in particular MDR, MPDG)
- Compliance with contractual provisions
- Compliance with data protection requirements (including Section 203 StGB)

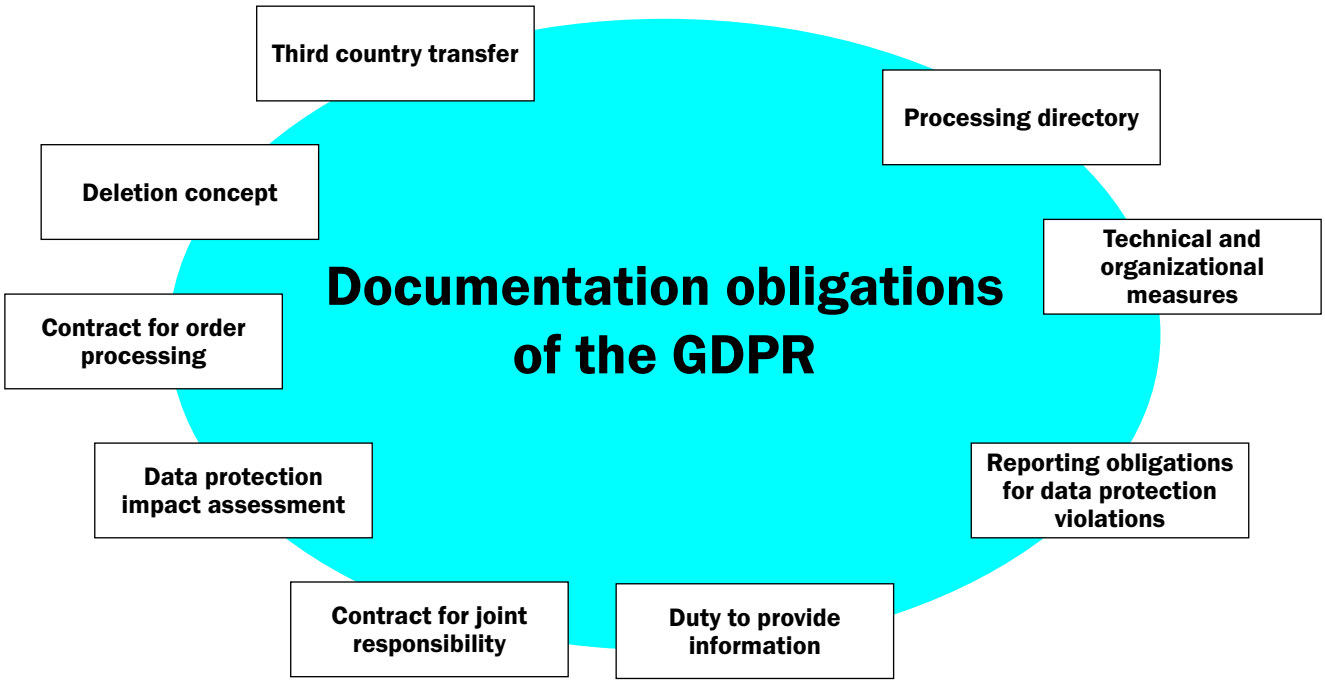
[1] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf.

[2] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf.

V. Users of medical devices

While manufacturers should consider the aspects listed above as part of their product development, users are obliged to comply with data protection when using the medical device (see above).
In order to ensure that medical devices are used in compliance with data protection regulations, users must meet certain requirements.

The following diagram is intended to illustrate this:



As can be seen from the diagram, users must fulfill certain formal requirements for verification purposes in order to comply with their documentation obligations.

These include in particular:

Legal basis for data processing

→ Firstly, before using a medical device, users as the responsible body must always thoroughly check which legal basis is relevant for the specific data processing in connection with the medical device. Depending on the specific application, several regulations may apply.

→ On the one hand, it is possible to base data processing in certain cases on Article 9 para. 2 lit. h) GDPR. However, the first alternative requires that, in addition to a treatment contract "with a healthcare professional" - meaning doctors and staff employed by doctors or in hospitals - the data processing is also necessary for the purposes specified in the provision, namely "in the interest of individual natural persons and society as a whole". It is not possible to conclusively define which purposes are in the interests of

individual natural persons.[3] Whether this provision can actually be applied in a specific case, for example because it is a "classic" case of patient treatment, depends on the individual case and must be examined in advance. In addition, in the second alternative of Article 9 para. 2 lit. h) GDPR, the corresponding provisions in the state hospital laws may also have to be observed - in addition or as an alternative.

→ However, it is also possible to base data processing on the data subject's consent under data protection law in accordance with Article 9 para. 2 lit. a) GDPR. This can be assumed in particular for "atypical" constellations in which more processing steps are carried out than would be necessary for the original treatment (e.g. in the case of highly technical medical devices with a large number of actors involved). In this case, users should have a corresponding model declaration of consent ready, which can be presented to the data subjects for signature before the medical device is used.[4] However, with this alternative, users should be aware that in the event of withdrawal, the data must be deleted in accordance with data protection regulations.

→ Article 9 para. 2 lit. c) GDPR can also be considered as an alternative legal basis. According to this, data processing is permitted if it is necessary to protect the vital interests of the data subject or another natural person and the data subject is physically or legally incapable of giving consent. This refers to emergency situations in which presumed consent replaces a declaration that cannot be made due to a lack of capacity to consent.[5] Whether this provision is actually relevant in a specific case must be thoroughly checked in advance, and users must always weigh up vital interests against data protection. In these cases, precise documentation of the relevant circumstances that led to the incapacity to consent and that support the presumed consent is always strongly recommended as a safeguard.

Processing directory

→ Users should also ensure that the corresponding medical device is listed in the processing directory and that the relevant information of Article 30 GDPR is entered in it.[6] To this end, they should ask the manufacturer to provide the relevant data protection information, if this has not already been done (see also section IV. 2.). If users use several medical devices in their facilities and these are predominantly similar - for example, they pursue the same purposes or access similar data - users can also list these medical devices as a joint process in the processing directory.

Technical and organizational measures [7]

→ With regard to the implementation of technical and organizational measures, users can take measures such as the encryption and pseudonymization of data, access controls, regular security updates or the implementation of firewalls in order to sufficiently guarantee the security of the data. If processors are used (e.g. in the case of remote maintenance), attention should also be paid to the inclusion of corresponding regulations with regard to technical and organizational measures.

[3] Ehmann/Selmayr/Schiff, 2nd edition 2018, DS-GVO, Art. 9 Rn. 60.

[4] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf.

[5] Kühling/Buchner/Weichert, 3rd edition 2020, DS-GVO Art. 9 Rn. 64.

[6] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf.

[7] https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf.

Reporting obligations in the event of data protection breaches

→ Users should always bear in mind that data protection incidents can occur when using medical devices despite careful data protection compliance.[8] If such a case occurs, users should refer to their data protection management system and implement the procedural steps described therein.

Duty to inform

→ Users are also obliged to inform the data subjects - usually patients - about data processing. This must be implemented in the form of data protection notices.[9] Since health data is regularly processed, this must be indicated in the data protection notices. Furthermore, care must be taken to name the respective (external) data recipients, for example when transmitting MRI images to external doctors. It is sufficient to name categories of recipients, e.g. treating physicians, as part of the information obligations.

Data protection impact assessment

→ As health data is also processed when medical devices are used, data processing is generally associated with a high risk to the rights and freedoms of the data subjects. For this reason, users should generally carry out a data protection impact assessment before using the medical device.[10]

Deletion concept

→ In order to comply with the principle of storage limitation, the institution must implement a deletion concept to ensure that the respective data is deleted after a certain period of time.[11] In this context, it is advisable to instruct certain groups of people, such as the IT department, to delete the data and to record this accordingly in the deletion concept.

[8] https://www.datenschutz-bayern.de/datenschutzreform2018/OH_Meldepflichten.pdf.

[9] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_10.pdf.

[10] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf.

[11] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_11.pdf.

Contract for order processing

→ In certain cases, it may be necessary for users to use service providers in the context of the use of medical devices (see also Section IV. 5.). If the manufacturer or user comes to the conclusion that the specific service requires an order processing contract, the second step should be to consider concluding such a contract. However, the service provider's duty of confidentiality can be problematic in this context. Compliance with medical confidentiality on the one hand and the disclosure of health data to processors on the other can lead to legal problems in case of doubt. It is true that doctors, for example, are increasingly reliant on the assistance of external service providers in their professional or official activities. However, they are liable to prosecution under Section 203 para. 4 cl. 1 no. 1 StGB if the service provider discloses a third party secret without authorization and the doctor has not ensured that the service provider has been obliged to maintain confidentiality. In essence, therefore, users or doctors, as holders of professional secrets, must additionally oblige the service providers they commission to maintain confidentiality in writing. Against this background, users are therefore well advised to thoroughly review the contract for order processing with regard to the service provider's confidentiality obligation.

Third country transfer

→ When processing data in the context of the use of medical devices, data may sometimes be transferred to third countries (= countries outside the EU/EEA). In these cases, the third country to which the data is transferred and the legal basis for the data transfer for this third country must be examined.[12] In this respect, it is possible to base the data transfer on an adequacy decision in accordance with Article 45 GDPR. In this context, it must always be checked in advance whether any decision on an adequate level of protection exists for the third country in question. Alternatively, suitable guarantees in accordance with Article 45 GDPR can also be used as a legal basis, such as the conclusion of binding corporate rules or standard contractual clauses. In these cases, however, care must be taken to carry out a risk assessment in advance in the form of a transfer impact assessment (hereinafter referred to as "**TIA**"). Furthermore, in individual cases, data subjects also have the option of expressly consenting to the transfer of their data to a third country in accordance with Article 49 para. 1 cl. 1 lit. a) GDPR. Whether this legal basis can actually be used should be checked in advance.

→ Current developments in the USA:
With regard to data transfers to the USA, users have always had to carry out a TIA to date, as the data transfer was based on the standard contractual clauses. Since July 10, 2023, however, data transfers to the USA can generally be based on an adequacy decision adopted by the EU Commission. The respective companies based in the USA still have to undergo a certification procedure in some cases in order to be able to invoke the adequacy decision. This means the following for users: If such certification has already taken place for the respective US company, users can now rely on the adequacy decision with regard to the legal basis for the data transfer, which is why it is no longer necessary to carry out a TIA. In this context, however, it is essential to ensure that no subcontractors are used in other third countries, as the adequacy decision alone is not sufficient in these cases.

[12] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf.

Practical tip:

The Bavarian State Office for Data Protection Supervision, in cooperation with the Bavarian State Commissioner for Data Protection, has produced a guide to cyber security for medical facilities, which provides an overview of some helpful practical measures in the form of a checklist.[13] The measures listed therein represent a best-practice approach that can support effective protection against current cyber security threats and can also be used by users as an aid for the use of medical devices.

[13] https://www.lda.bayern.de/media/checkliste/baylda_checkliste_medizin.pdf.

VI. Artificial Intelligence and Medical Devices

The integration of artificial intelligence in medical devices has made great progress in recent years. It can be assumed with high probability that development in this area will increase rapidly in the coming years. The specific legal issues that arise in this context and what manufacturers and users should pay attention to - particularly with regard to the forthcoming Artificial Intelligence Act ("AI Act") - are analyzed in more detail in a separate whitepaper.

C. Special case: Digital Health Applications

Since the Digital Healthcare Act (hereinafter referred to as "DVG") came into force on December 19, 2019, so called "health apps" have been offered on the market in addition to traditional physical medical devices, marking a turning point for the healthcare industry. Since then, doctors and therapists have also been able to prescribe digital health applications (also known as “DiGA”) to their patients. In contrast to the previous common healthcare services, DiGA is therefore a software or application that runs on digital platforms such as smartphones or tablets and that doctors or therapists can prescribe to their patients - just like with medication. All in all, it can therefore be seen as a type of prescription-only digital medical product ("app on prescription").

I. Definition

According to Section 33a SGB V, DiGA is a medical device that has the following characteristics:

- **Medical device** of **risk class I** or **IIa** (according to MDR or, within the framework of the transitional provisions of the MDR, according to MDD).
- The **main function** of the DiGA is based on **digital technologies**.
- The DiGA is not a digital application that merely serves to read or control a device; the medical purpose must be substantially achieved by the **main digital function**.
- The DiGA supports the **detection**, **monitoring**, **treatment** or **alleviation of diseases** or the detection, treatment, alleviation **or compensation** of **injuries** or **disabilities**.
- DiGA is **not** intended for **primary prevention**.
- The DiGA is used jointly **by the patient or by the healthcare provider and the patient**, i.e. applications that are only used by the doctor to treat the patient ("practice equipment") are not DiGA.

II. Examples

DiGA (+)	DiGA (-)
• Apps for depressive patients that provide information about the illness, document patients' moods and give instructions on relaxation exercises. • Apps to remind patients to take their medication, which may also provide dosage suggestions. • Apps for patients with chronic inflammatory bowel disease, which provide information about the disease and diet, document symptoms, give instructions for creating diet plans and provide a digital shopping companion with a scan function for groceries.	• The app is only used to coordinate and conduct video / telephone / chat conversations between therapist and patient. Other therapeutic services are not included. • Apps for patients with chronic inflammatory bowel disease, which put patients in contact with nutritionists via a chat function or telephone calls if required.

1. Inclusion in the DiGA directory

Anyone wishing to launch a DiGA on the market must deal with numerous legal requirements in advance and take a number of steps into account during implementation: First, for example, manufacturers must submit an application for inclusion in the "DiGA directory".[14] The Federal Institute for Drugs and Medical Devices ("**BfArM**") then checks whether the manufacturer has also complied with all requirements when developing the product, particularly with regard to functional suitability, data protection and data security. In addition, manufacturers must also prove that the product has a medical benefit (e.g. improvement of the state of health) or a patient-relevant structural and procedural improvement in care (e.g. detection or alleviation of diseases).

[14] https://antrag.bfarm.de/de.

2. Data protection

With regard to data protection, users and manufacturers of DiGA must also ensure compliance with data protection requirements. In this respect, the principles set out above under B.IV.1. and the general requirements for data protection and data security set out in the DPA also apply to DiGA. For manufacturers, there are additional special features that they must take into account. In particular, inclusion in the DiGA directory and the associated approval of the DiGA is linked to high data protection requirements, which manufacturers should always keep in mind when developing their product. In addition to the GDPR and the regulations already outlined in section B.III., the Digital Health Applications Ordinance (hereinafter "**DiGAV**") and the BfArM[15] test criteria are therefore of particular relevance:

These include in particular:

a) DiGAV

→ The regulations contained in the DiGAV are highly relevant for manufacturers. In order for their product to be approved at all, manufacturers must complete the questionnaire listed in Annex 1 of the DiGAV, which is presented in the form of checklists.[16] The checklists are divided into the two subject areas of data protection and data security and list all relevant aspects, from data protection principles to topics such as access controls and authentication. As part of these checklists, manufacturers must declare compliance with the requirements in accordance with Section 4 DiGAV. Against this background, Section 4 DiGAV expressly clarifies that informed consent must be obtained from the data subject from the digital application and at the start of the use of the DiGA, unless another regulation permits data processing.

b) Test criteria

→ The BfArM has also published test criteria for the data protection requirements for DiGA. In future, these criteria will form the basis for new certificates that manufacturers of healthcare applications can use to prove that their applications comply with data protection requirements. These include both the requirements of the GDPR and the extended requirements for DiGA. However, proof of compliance with data protection requirements by the manufacturer is only to be provided from August 1, 2024 by submitting a certificate issued on the basis of these test criteria. Until this date, the data protection requirements specified in Section 4 para. 6 DiGAV will apply.

→ The test criteria are divided into a total of 12 subject areas, whereby they are aligned with the key points of the GDPR that are relevant to the DiGA. For users, the statements made under Part 3 of the BfArM test criteria catalog are particularly relevant. The main points of content therein essentially correspond to the data protection principles and formal requirements listed above.

[15] https://www.bfarm.de/SharedDocs/Downloads/DE/Medizinprodukte/diga-dipa-datenschutzkriterien.pdf?__blob=publicationFile.

[16] https://www.gesetze-im-internet.de/digav/BJNR076800020.html.

D. Checklist

I. For users

- ☐ Is the process documented in the processing directory?
- ☐ If no other legal basis is relevant: Is informed consent obtained from the data subject prior to the start of data processing?
- ☐ Have appropriate technical and organizational measures been taken and implemented?
- ☐ Is there an emergency plan for dealing with data breaches?
- ☐ Are the data subjects sufficiently informed about the processing of their data by means of data protection notices?
- ☐ Was a data protection impact assessment carried out before the product was introduced?
- ☐ Is there a deletion concept in place with regard to the storage of data?
- ☐ If service providers are used (e.g. for remote maintenance): Has a contract for order processing been concluded?
- ☐ If several controllers determine the purposes and means of data processing: Has a joint controller agreement been concluded?

In the case of data transfer to a third country:

- ☐ Is there a legal basis for the data transfer under data protection law?

II. For manufacturers

- ☐ Is it ensured that the data is encrypted during data transmission?
- ☐ Is an authorization concept implemented in the product to regulate access rights?
- ☐ Has clustering of the storage system been ensured?
- ☐ Does the archive format ensure that the data can still be read in the future?
- ☐ Is it ensured that no personal data is disclosed to the service provider in the event of remote maintenance?
- ☐ Can the data be automatically deleted after a certain period of time?
- ☐ Are there regular updates and security patches for the medical device?
- ☐ Is there a document (FAQ document or a whitepaper) with data protection information for customers with regard to information on the medical device?
- ☐ Are there sample documents (e.g. data protection impact assessment) that are tailored to the respective medical device and made available to customers?
- ☐ Is there a user-friendly contract for order processing (Article 28 GDPR) in compliance with the relevant legal requirements (including Section 203 StGB) that can be made available to customers?
- ☐ In the case of DiGA: Have the requirements from the questionnaire in Annex 1 of the DiGAV been implemented accordingly?

Our experts
for data protection when using medical devices

Fabian Bauer, LL.M.
Senior Associate

+49 69 630001-82
f.bauer@skwschwarz.de

Marius Drabiniok
Associate

+49 69 630001-65
m.drabiniok@skwschwarz.de

Dr. Oliver Hornung
Partner

+49 69 630001-65
o.hornung@skwschwarz.de

Marwah Kamal
Associate

+49 69 630001- 65
m.kamal@skwschwarz.de

Franziska Ladiges, LL.B.
Partnerin

+49 69 630001-29
f.ladiges@skwschwarz.de

10719 Berlin
Kranzler Eck
Kurfürstendamm 21
T +49 30 8892650-0
F +49 30 8892650-10

60598 Frankfurt/Main
Mörfelder Landstraße 117
T +49 69 630001-0
F +49 69 6355-22

20459 Hamburg
Ludwig-Erhard-Straße 1
T +49 40 33401-0
F +49 40 33401-530

80333 Munich
Wittelsbacherplatz 1
T +49 89 28640-0
F +49 89 28094-32

skwschwarz.de