Whitepaper

SKW Schwarz

# Digital Health

## The Interaction of Regulatory Affairs, AI and Data Protection in Medical Technology – 20 Questions and Answers

September 2024

# Digital Health

## The Interaction of Regulatory Affairs, AI and Data Protection in Medical Technology – 20 Questions and Answers

1. **Why is the interaction between regulatory affairs, AI and data protection crucial for modern medical technology?**
2. **What would be conceivable use cases in practice?**
3. **When is a medical device or an in vitro diagnostic device an "AI system" within the meaning of the AI Act or rather when does it contain an "AI system"?**
4. **Which types of AI in the meaning of the AI Act are particularly relevant for medical technology?**
5. **How are medical devices and IVD containing AI systems classified in the risk classification system of the AI Act?**
6. **What regulatory requirements apply to medical devices/IVD with AI systems within the meaning of the AI Act?**
7. **What do the regulatory principles of the AI Act and of the MDR/IVDR have in common?**
8. **What is the relationship and interaction between the AI Act and the MDR/IVDR?**
9. **What problems currently exist in the CE certification of medical devices and in-vitro diagnostics with AI in relation to the MDR/IVDR? Can the AI Act solve these problems?**
10. **Does data protection stand in the way of the use of medical devices with artificial intelligence?**
11. **Who must implement the data protection requirements of the GDPR?**
12. **How can medical devices with AI be used in compliance with data protection regulations?**
13. **How can an AI be trained with health data in compliance with data protection regulations?**
14. **Which data sets may be used to train an AI?**
15. **When is health data anonymized and when is it pseudonymized?**
16. **May medical device data records be passed on to third parties?**
17. **Do manufacturers and users of medical devices that contain AI have to carry out a data protection impact assessment?**
18. **What are the requirements in terms of data security?**
19. **What requirements apply with regard to transparency?**
20. **What does all this mean for the practical approach of medical device providers who want to use AI systems?**

## Content

# Part I: Overview and description of use cases

## 1. Why is the interaction between regulatory affairs, AI and data protection crucial for modern medical technology?

→ The use of artificial intelligence (AI) in healthcare is rapidly revolutionizing medical research and development and treatment of patients. A shortage of specialists, pressure to improve efficiency and the call for ever faster and better diagnostics and therapeutics lead to a strong requirement for digitalization and support of human work by powerful technology. For example, AI-based evaluation software can be used for diagnostic imaging procedures in order to make an initial diagnosis to be checked by the doctor. In the future, AI systems will also be able to use health data to detect emerging or developing diseases even earlier.

AI will lead to completely new methods and possibilities in medicine. However, the risks must not be overlooked. AI systems used in healthcare have to be safe, reliable and efficient. This is the only way to create trust in the new technology. Therefore, new legal and regulatory requirements, along with safeguarding mechanisms, are necessary.

As AI requires large amounts of data in order to be trained and thus constantly improve, data protection also plays an important role in the use of AI in medicine. This is all the more important as patient health data is very sensitive information that requires special protection.

Compliance with the legal requirements of Medical Device Regulation (MDR) and In Vitro Diagnostic Device Regulation (IVDR), the EU's new AI Regulation (hereinafter referred to as the “AI Act”) and data protection requirements are therefore not only necessary compliance tasks for every med tech company, hospital and medical practice. They are nothing less than the very basis for the economic and medical success of new AI-based technologies.

The impact of the AI Act on the daily tasks of med tech companies in terms of regulatory affairs and the legally compliant handling of data leads to new legal problems and many unanswered questions. Users - especially hospitals and medical practices - must also ensure that the new AI technology is used in a legally compliant manner. In this white paper, we therefore shed light on the interaction of the new provisions in the “magic triangle” of MDR / IVDR regulatory requirements, the AI Act and the data protection laws and answer the most important questions on these new topics.

## 2. What would be conceivable use cases in practice?

→ But what does this mean in practice? How could the relationship between regulatory affairs, AI and data protection actually play out? To demonstrate this in a practical way, we will present two fictitious but realistic AI medical devices as possible use cases. We will use these two fictitious products to illustrate the questions and answers in the white paper and what the legal principles presented mean in concrete terms for dealing with new AI medical technology.

**Case 1: The "Blusser" blood pressure monitor**

The first fictitious example product is "Blusser", a blood pressure monitor. This product contains AI software that is embedded in the medical device (so-called "embedded software"). "Blusser" is used by patients at home. The software evaluates the measured blood pressure values and their progression and draws conclusions about possible pathological conditions. If such a condition is detected, the software alerts the patient and prompts him or her to have a medical examination. In this way, the AI integrated in the blood pressure monitor performs preventive diagnostics. The manufacturer is constantly improving the AI through training and regularly creates updates for the software. Patients can then download these updates themselves via Wi-Fi and the home network and install them on the device.

**Case 2: The "NeoplasKI" software**

The second example product is the fictitious software "NeoplasKI". It is used in cancer diagnostics. NeoplasKI is a standalone software, i.e. an independent product that is supplied without hardware. It can be installed on any PC and contains a dynamic AI system. NeoplasKI is designed to create an independent initial diagnosis in order to relieve radiologists in their work. To do this, the software analyzes mammography images and also takes into account the development of the progression by comparing previous images with current ones. The initial diagnosis made by NeoplasKI is then checked and verified by a radiologist. The result of the software is then either confirmed by the radiologist or - if the findings of NeoplasKI are incorrect - modified.

NeoplasKI is also continuously improved by the evaluated imaging and the medical reviews of the initial diagnosis made by the AI, and thus constantly learns.

# Part II: Regulatory Affairs of MDR/IVDR and AI

### 3. When is a medical device or an in vitro diagnostic device an "AI system" within the meaning of the AI Act or rather when does it contain an "AI system"?

→ According to Art. 3 (1) of the AI Act, an "AI system" means a machine-based system

- that is designed to operate with varying levels of autonomy and
- that may exhibit adaptiveness after deployment, and
- that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments.

AI systems are **software-based**. Consequently, medical devices and in-vitro diagnostics (IVD) that are operated without software do not fall under the definition of an "AI system" from the outset and are therefore not subject to the AI Act.

Conversely, medical devices and IVD with software are not automatically regulated by the AI Act. The definition in Art. 3 (1) of the AI Act is intended to distinguish them from conventional software systems or programming approaches that are based exclusively on the rules for the automatic execution of processes defined by natural persons. At its core, an AI system differs from such "simple" software in that the AI system not only processes predefined program sequences (e.g. if-then program code), but also has the **ability to learn, draw its own conclusions or carry out modeling autonomously** (see recital 12 of the AI Act).

A medical device or IVD can already be an **independent AI system**. However, AI systems can also be components of medical devices or IVD alongside other components, either without fixed integration or as an **integrated, embedded system**.

**Practical application to the use cases:** The example product "NeoplasKI" is an AI-supported diagnostic software and thus, as a stand-alone AI system, a medical device. The AI system in "Blusser", on the other hand, is a component of a medical device. "Blusser" contains AI-supported evaluation software that is integrated into a measuring device for certain vital parameters.

## 4. Which types of AI in the meaning of the AI Act are particularly relevant for medical technology?

→ The AI Act classifies AI systems according to risk classes (similar to medical device law).
It distinguishes between the following risk groups:

- Unacceptable risk → **prohibited** AI practices (Art. 5 AI Act)
- High-risk AI systems → **regulated** high-risk AI systems (Art. 6-49 AI Act)
- AI systems with limited risk → only primarily **information obligations** (Art. 50 AI Act)
- AI systems with low or no risk → **no obligations**, only optional self-regulation (recital 165 of the AI Act, Art. 95 AI Act)

## 5. How are medical devices and IVD containing AI systems classified in the risk classification system of the AI Act?

→ According to the risk classification system of the AI Act, medical devices and IVD that are AI systems or contain AI systems (see question 3), are **often high-risk AI systems**. This follows from Art. 6 (1) of the AI Act. Accordingly, a medical device is considered a high-risk AI system if the following two conditions are cumulatively met:

- **First condition:** The AI system is intended for use as a safety component of a product, or the AI system is itself a device, covered by the Union harmonisation legislation listed in Annex I. According to Annex I, Section A, No. 11 and 12, the MDR and the IVDR are such harmonisation legislation. Therefore, if the medical device or IVD consists of the AI system as such (example: diagnostic software), then the first condition for a high-risk AI system is fulfilled. The same applies if the AI system performs safety-related tasks as an embedded or non-embedded subsystem in a medical device or IVD and is therefore to be regarded as a "safety component" of a medical device or IVD (Art. 6 (1) letter a).

- **Second condition:** The product with an AI system being a safety component, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of that product pursuant to the Union harmonisation legislation listed in Annex I. **The latter is the case for medical devices in classes Is, Im and Ir and IVD in class B and above**; only for medical devices in class I (except Is, Im and Ir) and IVD in class A is it sufficient for the conformity assessment procedure if the manufacturer himself assesses conformity, so that no conformity assessment "by a third party" is required. However, standalone software that qualifies as a medical device practically never falls into Class I under the new classification rules, but almost always into higher classes, meaning that AI systems used with such software are regularly high-risk AI systems.

→ Conversely, AI systems **are not high-risk systems** according to these regulations if they

- are only a component (embedded or non-embedded) of a medical device or IVD and are therefore not the product itself and are not a safety component of the medical device/IVD, i.e. do not perform a safety-related function (condition 1 not fulfilled), **or**

- the medical device is a class I device (except classes Is, Im and Ir) or the IVD is a class A device (condition 2 not fulfilled).

In practice, however, the first exception is unlikely to apply. For reasons of patient safety, the term "safety component" will have to be interpreted broadly. According to Art. 3 (14) of the AI Act, a safety component means a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunction of which endangers the health and safety of persons or property. As a result, we believe that any AI that has at least an impact on the safety of the medical device/IVD will fall under this term and thus lead to the classification of the AI system as a high-risk AI system.

**In Annex I you will find a test scheme for the classification of AI in medical devices and IVD.**

**Practical application to the use cases:** "Blusser" and "NeoplasKI" are high-risk systems within the meaning of the AI Act.

"Blusser" is a class IIa blood pressure monitor and therefore requires a conformity assessment by a third party. The AI system is embedded in the monitor and assumes safety-relevant tasks. It is intended to evaluate blood pressure values and thus detect pathological conditions, which serves the safety of the patient. A malfunction could put the patient's health at risk if they rely on the information provided by the "Blusser". In our opinion, the AI software in the "Blusser" should therefore be classified as a "safety component". Both conditions of a high-risk AI are fulfilled.

"NeoplasKI" is an AI-supported diagnostic software. This medical device exhausts itself in the AI system and falls within the scope of the MDR, a harmonisation legislation listed in Annex I of the AI Act. As a standalone software, "NeoplasKI" no longer falls under Class I of the MDR and must therefore be subject to a conformity assessment by a third party; it is not sufficient for the manufacturer to execute such an assessment itself. Both conditions of a high-risk AI according to Art. 6 of the AI Act are also fulfilled here.

## 6. What regulatory requirements apply to medical devices/IVD with AI systems within the meaning of the AI Act?

→ For high-risk AI systems, a conformity assessment procedure with testing, evaluation and issuance of a certificate of conformity with regard to the standards and requirements of the AI Act must be completed before placing the product on the market.

As shown above, medical devices and IVD with AI are usually classified as high-risk AI systems (see question 5). Consequently, they must meet in particular the following requirements in addition to the requirements of the MDR or IVDR in accordance with Chapter III of the AI Act:

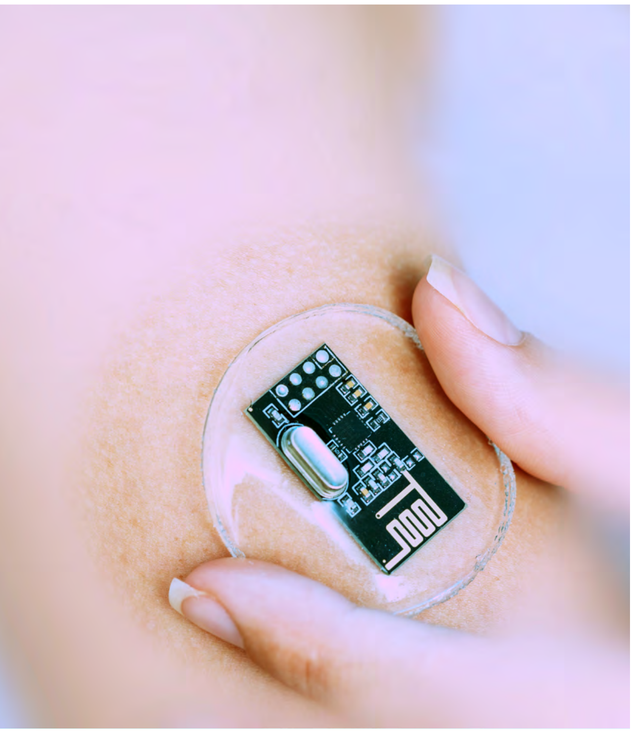
- A **risk management system** must be established, implemented, documented and maintained throughout the entire lifecycle of the AI system. The principle is methodically and structurally similar to the risk management system of the MDR and IVDR, but with particular consideration of AI specifics (Art. 9 AI Act).

- **High requirements for the quality of the data** used to train the model, in particular through suitable data governance and management practices (Art. 10 AI Act).

- The **technical documentation (TD)** must be prepared before the system is placed on the market and must always be kept up-to-date. In this respect, the TD already required for medical devices and IVD must be supplemented by some AI-specific requirements (Art. 11 AI Act).

- High-risk AI systems must technically allow for the **automatic recording of events** (Art. 12 AI Act).

- Fulfillment of **transparency and appropriate information obligations** towards deployers (Art. 13 AI Act).



- High-risk AI systems must be designed and developed in such a way that they **can be supervised efficiently by humans** during the period in which they are in use (Art. 14 AI Act).

- Compliance with an appropriate level of **accuracy, robustness and cybersecurity** (Art. 15 AI Act).

- Providers of high-risk AI systems must also maintain a **quality management system** in accordance with Art. 17 AI Act. However, this largely corresponds to the quality management system defined in ISO 13485 and the MDR/IVDR and is therefore nothing substantially new for manufacturers of medical devices and IVD in terms of methodology and structure.

- The **authorized representatives**, who must exist in accordance with Art. 22 AI Act, have in principle the same obligations as those set out in the MDR/IVDR.

## 7. What do the regulatory principles of the AI Act and of the MDR/IVDR have in common?

→ Overall, the regulatory principles and methodology set forth in the AI Act are very similar to those for medical devices and IVD. In our view, this is an opportunity and a risk for medical device companies at the same time. On the one hand, additional regulatory requirements must be fulfilled for medical devices with AI systems, which is associated with greater effort and therefore higher costs. On the other hand, the basic structures for the additional requirements (e.g. risk management system, technical documentation, quality management in accordance with ISO 13485 etc.) are generally already in place and are not new for companies in the med tech sector - unlike in some cases for other sectors that want to use AI systems. The advantage is that the requirements of the AI Act make it much clearer and more explicit which requirements specifically need to be met by a medical device with an AI system and what must be fulfilled and documented to obtain the necessary certification.

## 8. What is the relationship and interaction between the AI Act and the MDR/IVDR?

→ The interaction between the AI Act and the MDR/IVDR is still not completely clarified. However, Annex I, Section A of the AI Act explicitly mentions in No. 11 the Regulation (EU) 2017/745 (MDR) and in No. 12 the Regulation (EU) 2017/746 (IVDR) as a harmonised legislation. This means in relation to medical devices or IVD with AI systems: If the requirements of the MDR or IVDR are already fulfilled (for example with regard to risk management, technical documentation, conformity assessment and certification, etc.), these MDR/IVDR-related requirements are also deemed to be fulfilled under the AI Act and no longer need to be tested and verified separately. “Only” the requirements of the AI Act for the AI system of the medical device or IVD must be complied with in addition.

Recital 124 and Art. 43 of the AI Act and the characteristics of the harmonized legislation mean that only one conformity assessment procedure is carried out in which the requirements of all relevant legislation (AI Act and MDR or IVDR) are checked.

In concrete terms, this means that suppliers of medical devices with AI systems must comply with **both requirements**, those of the MDR and the AI Act, but only have to perform **one common conformity assessment procedure**. In this procedure, both regulatory approaches are taken into account and the medical device is tested for conformity with these requirements and certified accordingly. The same applies to IVD with regard to the requirements of the IVDR and the AI Act.

## 9. What problems currently exist in the CE certification of medical devices and in-vitro diagnostics with AI in relation to the MDR/IVDR? Can the AI Act solve these problems?

→ Medical devices and IVD require CE marking before they can be placed on the European market or put into service. The CE marking may only be applied if the product meets the essential safety and performance requirements. A conformity assessment procedure ensures this, whereby a Notified Body has to be involved in the conformity assessment procedure for medical products of higher risk classes (for medical devices from class Is, Im and Ir, for IVD from class B).

Until now, Notified Bodies have often been very reluctant to certify medical devices and IVD with dynamic AI because the AI changes as a result of additional learning and the risk assessment and risk-benefit profile of the products can therefore constantly change as well. Similar problems can arise with so-called “black box AI”, where the data input and/or operations are not comprehensible and verifiable for the user (and therefore, in case of doubt, also for the Notified Body). Since it is an essence of AI to autonomously achieve results and draw conclusions where the path to this is not predetermined by programming, AI in medical devices and IVD will often be “black box AI” in this sense, with corresponding problems in the classic conformity assessment of Notified Bodies based on a more or less static product.

Even if this problem is not specifically addressed by either the MDR/IVDR or the AI Act, the AI Act could actually remedy this situation. **The AI Act now contains specific regulatory requirements for the risk assessment and risk control of dynamic AI** (see question 6 above). These mechanisms can now be used to cover precisely those specifics of AI systems in medical devices and IVD that were previously difficult for Notified Bodies to deal with using only the assessment system of the MDR/IVDR.

We assume that the Medical Device Coordination Group (MDCG) will soon issue documents that can be used for medical devices and IVD with AI systems in order to coordinate and map conformity assessment under both the MDR/IVDR and the AI Act. This also should make it easier to convince the Notified Bodies, as a standardized process for medical devices and IVD with AI will then (finally) be available. It is then advisable to align the technical documentation with these documents as far as possible.

# Part III: Data protection and AI

## 10. Does data protection stand in the way of the use of medical devices with artificial intelligence?

→ The answer is clearly no.

It is true that the use of medical devices - especially in combination with artificial intelligence (AI) components - requires special attention in terms of data protection law. On the one hand, it is the unanimous opinion of the data protection supervisory authorities that the use of AI is associated with risks (keyword: lack of transparency, so-called "black box" concept). On the other hand, the GDPR is structured in such a way that the processing of health data is generally prohibited (see Art. 9 (1) GDPR), unless one of the - generally restrictive - exceptions listed in Art. 9 (2) GDPR applies. The question of which legal basis can legitimize the processing of health data to train AI becomes complex. It also becomes complex if an AI component makes independent decisions in subsequent live operation, thereby opening up the scope of application of Art. 22 (1) GDPR.

The combination of these issues in particular can pose a number of challenges for the relevant stakeholders. Nevertheless - as consulting practice shows - the challenges can be mastered well in the vast majority of cases if the necessary test steps are taken into account.

## 11. Who must implement the data protection requirements of the GDPR?

→ Who has to fulfill the requirements set out in the GDPR depends on the distribution of roles under data protection law? While the AI Act provides for a clear allocation of roles for certain constellations and the MDR/IVDR primarily address the manufacturer, responsibility under data protection law can vary greatly from case to case.

In this respect, Art. 4 No. 7 GDPR states that the controller, as the primary addressee of data protection obligations, determines the purposes and means of data processing. While the training phase of an AI-supported medical device is typically the responsibility of the manufacturer, during the application phase - for example when treating a patient - the medical practice or hospital regularly takes on the role of controller. In the application phase, however, the manufacturer can take on the role of a processor within the meaning of Art. 28 GDPR, for example if it processes personal data – e.g. cloud-based and/or through remote maintenance work – on behalf of the user. It becomes particularly exciting when the processor uses usage data for its own purposes, for example to continuously train the AI. In this case, the classic framework of commissioned processing is "broken" and the manufacturer once again assumes the role of a controller - at least for certain processing operations. Whether this leads to separate or joint responsibility of the parties involved is controversial in the legal debate and must therefore be examined very carefully. On the part of the data protection supervisory authorities, the tendency is towards joint controllership (Art. 26 GDPR).

However, it should be noted at this point that none of the above statements are "set in stone" and that a comprehensive examination must always be carried out in each individual case.

**Practical application to the example cases:** Using the example of the medical device "NeoplasKI", it would initially have to be assumed that the manufacturer is responsible for the training process. In particular, the selection of the correct training data and its lawful processing would therefore have to be ensured by the manufacturer of the "NeoplasKI" software.

During the subsequent use phase of "NeoplasKI", on the other hand, the medical practices or hospitals using the medical device would take on the role of controller. However, if the manufacturer of "NeoplasKI" were to gain further access to personal data at this time - for example, to carry out remote maintenance work - it would be assumed that this would constitute commissioned processing. Nevertheless, since the data processed during the usage phase is also to be used for further "training" of "NeoplasKI", there is a (separate or joint) controllership of the manufacturer, as it were, which relates to this very training process. It is therefore a minimum requirement that all parties involved obtain a clear picture of the allocation of roles under data protection law and map these accordingly in the contract.

## 12. How can medical devices with AI be used in compliance with data protection regulations?

→ Despite existing peculiarities, the use of medical devices with AI components is (also) initially an ordinary processing of personal data.

This means that the general principles of Art. 5 (1) GDPR must be observed and appropriate technical and organizational measures must be implemented in accordance with Art. 32 GDPR. The GDPR is expressly designed to be technology-neutral, which is why the mere use of AI does not initially entail any special legal features of its own. In practice, however, supervisory authorities are tending to apply stricter standards to the use of AI - particularly in the sensitive area of health data.

**What does this mean in practice?** As a first step, the company concerned (such as the manufacturer of a corresponding medical device) should consider in which "life cycles" of the AI the processing of personal data plays a role. A distinction is regularly made between different phases of the development and use of an AI - even if overlaps are of course conceivable in practice:

- Development phase
- Training and test phase
- Validation phase
- Deployment phase

For each phase, all data protection requirements must be observed by the respective responsible body. In the development phase, the design and the (future) data processing steps in particular must be considered. In the training and test phase, the selection of the respective training and test data as well as the implementation of the data minimization principle (Art. 5 (1) lit. c) GDPR) are particularly important. In this phase, the decision should also be made (and documented) as to the extent to which anonymized or at least pseudonymized data can be used. When a "fully" trained AI is used later, the transparency of the data processing will be particularly decisive (Art. 5 (1) lit. a) GDPR).

In practice, drafting AI guidance that defines the individual test steps - broken down into the relevant life cycles - has proven successful. Once the respective requirements have been formulated, the checklist principle applies. In this way, compliance with accountability to the data protection supervisory authority (Art. 5 (2) GDPR) is particularly successful.

Further regulatory issues should be considered during the design phase (see Part II of this white paper).

## 13. How can an AI be trained with health data in compliance with data protection regulations?

→ The linchpin of data protection-compliant AI training is the training data used. Where does it come from? Is it of sufficient quality and can bias be ruled out? As a rule, it is not just the "raw data" that is used to train an AI, but this is comprehensively processed (so-called standardization) so that all data used has the same quality characteristics.

If, for example, so-called **supervised learning** is carried out - as is often the case with artificial neural networks for image classification and segmentation - the respective data must first be labeled (also "annotated"). In supervised learning, the AI is presented with data whose result (i.e. the answer to the task to be tested) is already known. The AI then "learns" the relationship between the input and the further weightings required to solve the task through constant repetition. This work step should also be checked as thoroughly as possible so that clear specifications and quality assurance checks exist for the annotation of the training data.

The question of **which legal basis under data protection law** the data processing can be based on is often a difficult one. Several strategies should be considered and verified by the controller in advance:

(1) **Is the origin of the training data known and may this data be used at all?** As already mentioned above, the processing of health data is generally prohibited under Art. 9 (1) GDPR. Since there is no original balancing of interests clause in the scope of application of Art. 9 GDPR (as in Art. 6 (1) lit. f) GDPR), one will often have to deal with consent under data protection law - with the well-known problems of informed consent, voluntariness and purpose limitation.

(2) In addition, the question of whether there is a so-called **change of purpose** within the meaning of Art. 6 (4) GDPR will often have to be answered. If the respective data was originally collected for completely different purposes, for example, the processing of the data for purposes other than those for which it was originally collected must be separately legitimized from a data protection perspective.

(3) Depending on the functionality and architecture of an AI, it may also be necessary **to clarify whether the training data used will continue to be used in the future - for example in live operation**. Does the fully trained AI also use the data originally (only) intended for the training process in its deployment phase? Or is it "only" a fully trained algorithm which - according to the current state of technology - does not allow any conclusions to be drawn about the respective data? Since in the first case there is again a "new" purpose of data processing, some developments and technical questions for the future must already be taken into account in the training phase.

## 14. Which data sets may be used to train an AI?

→ As with any processing of personal data, the selection of the data used must always be based on the specific purpose pursued. This means that - in compliance with the principle of data minimization (Art. 5 (1) lit. c) GDPR) - (only) those personal data may be processed that are actually required to achieve the purpose (**purpose limitation principle**, Art. 5 (1) lit. b) GDPR).

The following points should be considered in this context:

- As a first step, it should always be checked whether **anonymized data sets** can be used for training if necessary or whether pure machine data or synthetic data can be used from the outset. In this case, the GDPR would not apply in the first place, which would represent the "ideal solution" under data protection law.

- If anonymization is not given, not possible or not appropriate, pseudonymization should be considered. **Pseudonymized data** is still personal data. However, pseudonymization is recognized in data protection law as an effective measure that significantly minimizes risk and interference in favour of the data subjects. It is therefore suitable for contributing to a positive risk assessment under data protection law.

- If pseudonymization is not given, not possible or not appropriate, at least the respective data set itself must be examined for **superfluous data points**. In the case of medical imaging data (e.g. CT images), for example, the metadata in the image that allows conclusions to be drawn about the respective hospital or other information could be removed.

Having said this, the dilemma often remains that a sufficiently large amount of data must be processed in order to train an AI. In order to rule out discrimination or other errors, a wide range of data sets (with regard to gender, age, origin, ethnicity, etc.) are regularly processed. The quality of the AI used often increases with the number of training runs carried out. This shows that in many cases it is almost impossible to resolve the conflict between, on the one hand, the need to use large amounts of data to gain as much knowledge as possible and, on the other hand, the obligation to observe the principle of data minimization in accordance with Art. 5 (1) lit. c).

However, sufficient documentation in an AI guidance (see above) can document the underlying considerations for the selection of the corresponding training data and thus make them comprehensible both for a (data protection) supervisory authority audit and for documentation vis-à-vis customers and purchasers. This enables the controller to meet its accountability obligations under Art. 5 (2) GDPR. In addition, such AI guidance can be used to demonstrate compliance with AI-related requirements as part of the technical documentation in the conformity assessment procedure under the MDR/IVDR and the AI Act (see question 6).

Speaking of requirements for training data sets: For its part, the AI Act contains its own requirements in relation to "**data governance**". According to Art. 10 (1) AI Act, high-risk AI systems (which include many medical devices and IVDs with AI elements, see Part II of this white paper) may only be trained with data that meets certain quality criteria specified in Art. 10 (2) – (5) AI Act. For example, **the training, validation and test data sets must be "relevant, representative, accurate and complete"** (Art. 10 (3) AI Act). There is an obvious parallel here to the different data protection requirements and principles in Art. 5 (1) GDPR. According to Art. 5 (1) lit. d) GDPR, personal data must (also) be "accurate and, where necessary, kept up to date" and "every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".

This shows that **regulatory requirements from the AI Act and the MDR/IVDR on the one hand and data protection requirements on the other go "hand in hand" in terms of content**. Nevertheless, caution is required with regard to "mixing" the requirements of the different sets of regulations. This applies in particular to the technical documentation that must be prepared in the conformity assessment procedure in accordance with the MDR/IVDR and Art. 11 of the AI Act. This should not be unnecessarily "thickened" with the documentation required under data protection law. In case of doubt, the structure and content requirements of the MDCG documents should be adhered to. Conversely, however, the technical documentation in accordance with the MDR/IVDR and the AI Act should be easily usable as part of the data protection documentation in accordance with Art. 5 (2) GDPR.

## 15. When is health data anonymized and when is it pseudonymized?

→ As explained above, anonymization is the “best case” under data protection law. Data is personal if it relates to a natural person and it is possible to identify the person directly (e.g. via their name) or at least indirectly (e.g. via an identification number).

**Anonymization** is assumed **if a natural person cannot (or can no longer) be identified**. All clear data or other indirectly identifiable characteristics must therefore be removed from the data record. In contrast, the purpose of **pseudonymization** is to be able to **subsequently identify the respective person** - for example, by assigning a patient ID in clinical studies. Pseudonymized data therefore continues to be personal data, as it is still possible to assign it to the patient, for example via the assigned patient ID.

Where the boundary between “still personal data” and “already anonymized data” lies in individual cases is controversial under data protection law and highly dependent on the individual case. In the Breyer ruling (ECJ, ruling of 19 October 2016, C-582/14), the ECJ defined that it depends on whether there are means that the data processing body

> *“are reasonably likely to be used by the data controller to link the data in its possession with the additional information of another person in such a way that the data controller is able to identify the data subject.”*

Accordingly, for the data controller, this is not personal data if

> *“the identification of the person concerned would be prohibited by law or impracticable, for example because it would require a disproportionate effort in terms of time, cost and manpower, so that the risk of identification would appear to be de facto negligible.” (ECJ, judgment of 19 October 2016, C-582/14, para. 44)*

Whether and when this is the case must always be assessed on a case-by-case basis. Depending on the individual circumstances, a result would therefore be conceivable in which the respective data is (only) pseudonymized for one data processing body (e.g. the controller), but the data recipient cannot identify the persons concerned “by proportionate means” and therefore anonymization exists (at least for them). This legal situation opens up enormous opportunities for players in the healthcare sector to achieve an anonymization effect by technical means. Nevertheless, it always remains a question of the individual case.

## 16. May medical device data records be passed on to third parties?

→ Any transfer of personal data to a third party constitutes data processing that requires a legal basis.

Consent is often the obvious choice. However, it has legal and practical disadvantages. For example, it can be revoked at any time and is often not practical in mass business. Alternatively, there are various scenarios in the medical context in which a patient's data may be permissibly passed on.

If a medical device is used as part of the treatment of a patient, the provider of a medical device who provides the doctor/hospital with cloud and/or maintenance services, for example, typically has the role of processor within the meaning of Art. 28 GDPR. This also applies in principle if the medical device works with AI components.

If the manufacturer of the medical device processes the data beyond the purpose of medical treatment, for example to train the AI, the case is different.

In this case, the manufacturer of the medical device pursues independent (also commercial) purposes that cannot be combined with the original medical treatment. In this case, an explicit legal basis is required - unlike in the case of commissioned processing, where the transfer is privileged under Art. 28 GDPR. The question of whether the manufacturer of the medical device is entitled, without the consent of the patients concerned, to anonymize the patient data provided to it as part of the order processing in order to subsequently use it for its own purposes is controversial. Supervisory authorities take a critical view of this, but there is not (yet) a supreme court ruling on this issue.

## 17. Do manufacturers and users of medical devices that contain AI have to carry out a data protection impact assessment?

→ As a general rule: Yes.

However, this presupposes that the manufacturer and/or the user has the role of the so-called controller under data protection law in the specific individual case. This is because a data protection impact assessment is carried out by the controller of the data processing (not, for example, by the processor).

When exactly a data protection impact assessment is to be carried out is set out in Art. 35 (3) GDPR, among others. According to this, a data protection impact assessment is required in particular if - which will often be the case - extensive special categories of personal data, i.e. in particular health data, are processed. In addition, the data protection supervisory authorities have published a so-called **must list**, which also includes **AI-based processing operations**. Finally, there are general risk-influencing factors that may make a data protection impact assessment necessary without this being explicitly required by law. The combination of the decisive factors here (i.e. the processing of health data and the use of AI components) means that in many cases "a high risk to the rights and freedoms of natural persons" cannot be ruled out at the very least.

However, a different assessment is possible in specific individual cases. If, for example, no or only a small amount of personal data is processed, this may make it unnecessary to carry out a data protection impact assessment. Technical particularities - i.e. the specific type of data processing - can also have a decisive influence on an upstream risk assessment. However, this assessment should then be documented in a so-called threshold analysis in order to be able to prove the supporting considerations to the data protection supervisory authority (keyword: accountability pursuant to Art. 5 (2) GDPR).

**Practical application to the example cases:** Using the example of the medical device "NeoplasKI", the manufacturer would have to carry out a data protection impact assessment for the training process of the AI, while it is the responsibility of the user - the doctor's practice or hospital - to carry out a data protection impact assessment for the use phase. The responsibilities and the resulting obligations must therefore be differentiated according to the respective life cycles of the AI and the relevant influence on data processing.

## 18. What are the requirements in terms of data security?

→ KAI-based medical technology introduces new vectors for cyberattacks due to its unique technical properties.

**Cybersecurity** requirements arise from the MDR/IVDR, the AI Act and the GDPR. However, the new Cyber Resilience Act is not applicable to medical devices under the MDR and IVDR.

Below is an overview:

The **MDR**, which addresses the manufacturer of medical devices, defines cybersecurity requirements in several places. According to Art. 5 (2) MDR, a device must comply with the essential safety and performance requirements set out in Annex I, taking into account its intended purpose. Devices must be designed in such a way that they are safe and effective. This must be based on the "generally recognized state of the art". Annex I Section 14.2. lit. (d) MDR stipulates that devices must be developed in such a way that risks associated with possible negative interactions between software and the IT environment in which it is used and with which it interacts are reduced as far as possible. Furthermore, according to Annex I Section 17.4 of the MDR, the manufacturer must specify minimum requirements regarding the characteristics of IT networks and IT security measures, including protection against unauthorized access, which are necessary for the intended use of the software. In this respect, the **IVDR** contains essentially the same requirements in terms of content and wording as the MDR (see e.g. Art. 5 (2), Annex I Sections 1 and 16.2)

The above regulations remain quite abstract, but are made more specific by the **Medical Device Coordination Group (MDCG) Guideline 2019-16 "Guidance on Cybersecurity for medical devices"** (Link). Its purpose is to provide manufacturers with guidance on implementing the cyber-related requirements of the MDR and IVDR. Although the guideline is not legally binding, it is relevant insofar as it can be used by the ECJ for interpretation in legal disputes. In addition, the Notified Bodies generally check MDR and IVDR conformity on the basis of the MDCG guidance documents, meaning that the structure and content of the technical documentation should comply with the MDCG requirements. Manufacturers should therefore pay appropriate attention to this.

Manufacturers and users can also refer to a **paper recently published by the BSI entitled "AI Security concerns in a nutshell"**. It describes the most important types of cyberattacks that specifically target AI systems and presents possible defense measures for each (Link).

The **AI Act** supplements the requirements of the MDR and IVDR. Providers of high-risk AI systems, which in many cases include AI-based medical devices, must in particular meet the requirements for the robustness and cybersecurity of AI systems defined in Art. 15 AI Act. This includes ensuring that the technical solutions to ensure the cybersecurity of high-risk AI systems, which include virtually all AI systems in medical technology (see question 5), are "appropriate to the circumstances and risks involved". Art. 26 AI Act imposes an obligation on operators of such high-risk AI systems (e.g. hospitals, medical practices) to implement appropriate technical and organizational measures to ensure that the AI systems are used in accordance with the instructions for use.

The **GDPR** defines IT security requirements primarily in Art. 32 GDPR. According to this, the controller (often the hospital or medical practice) and the processor (this may - depending on the case - be the manufacturer of the product, who receives access to personal data remotely, for example) must take “appropriate technical and organizational measures” to ensure a level of protection of personal data appropriate to the risk. The state of the art, implementation costs and the nature, scope, context and purposes of the processing must be taken into account. In addition to Art. 32 GDPR, Section 8a of the BSI Act and the industry-specific security standard (B3S) must be observed for operators of critical infrastructures (which may include hospitals) (Link).

As always in IT security law, regulations - which are usually quite abstract - must be brought to life in practice. This requires interdisciplinary cooperation between lawyers and IT experts.

**Practical application to the example cases:** As already mentioned, the MDR/IVDR initially address the manufacturer of a medical device. The AI Act also imposes certain IT security obligations on providers of high-risk AI systems in particular. It is therefore initially the original task of the manufacturers of “NeoplasKI” or “Blusser” to implement these obligations in the design of their medical devices.

The user of “NeoplasKI” (e.g. the doctor's practice or hospital) also plays an important role, as they are regularly the controller, at least during the use phase. Art. 25 GDPR (“Privacy by Design” and “Privacy by Default”) and Art. 32 GDPR provide for specific obligations in this respect, which reflect technical data protection. However, the problem here is that the user has no original influence on the technical design of the medical product.

These regulations therefore ultimately result in a “selection decision” by the user as to which manufacturer of a medical device **enables** compliance with the requirements of the GDPR in the first place. While this is already required by law for order processing in accordance with Art. 28 GDPR, the aforementioned principles ultimately apply to the entire processing cycle using an AI-supported medical device. From a manufacturer's perspective, it is therefore obvious that legally compliant technology design not only serves to implement its own legal obligations, but can also have a direct impact on the cost-effectiveness of the medical device. The manufacturer of “NeoplasKI” is therefore well advised to take the perspective of the future user into account when designing the medical device. By making it easier for the user to comply with data protection requirements, the manufacturer can gain a real market advantage in this respect.

## 19. What requirements apply with regard to transparency?

→ The principle of transparency plays a prominent role in data protection law. The controller must take this principle into account at several levels, which is why an understanding of data processing can ultimately be regarded as a basic requirement for compliance with the GDPR. However, implementing these requirements can sometimes be difficult, especially when AI components are used, as the functions and decision-making processes of AI are often not readily understandable (the so-called "black box" concept).

Initially, the controller must fully **understand the data processing activities** to effectively implement the formal requirements of the GDPR. This concerns, for example, the entry in the record of processing activities in accordance with Art. 30 GDPR and the performance of a data protection impact assessment in accordance with Art. 35 GDPR. Without the necessary understanding of how the medical device works, it will not be possible for the controller to implement these obligations. In addition, the controller is obliged to provide evidence to the data protection supervisory authority (see Art. 5 (2) GDPR). The aforementioned obligations apply to both the manufacturer and the user of the medical device - in each case insofar as responsibility under data protection law can be assumed.

The principle of **transparency also plays a prominent role in relation to data subjects**. While Art. 13 (1) GDPR already specifies a wide range of information that must be provided to data subjects, any declaration of consent (e.g. from patients) must also be provided "in an informed manner". In both cases, however, the question arises as to how extensive this information must be. Although the details of this are highly controversial, the result will (have to) be an understandable and pragmatic approach. In our opinion, there is no need to provide information about the algorithm behind the AI system itself, as this is to be classified as a trade secret. Nevertheless, it must be made clear to affected persons which processing steps are carried out using an AI and on what basis the output (i.e. the result) of the AI is determined. While the manufacturer must inform all persons affected by the training of the AI system, for example, the user is obliged to inform patients in particular.

In the latter case, however, it is particularly important to clarify how the user of the medical device can obtain this information in the first place. This applies in particular to information on the technical functionality of the AI-supported medical device, which is often not readily available. The AI Act provides a certain "lifeline" in that it imposes high transparency obligations on the provider of a high-risk AI system in Article 13. In particular, it must be ensured that the user can interpret the results of the high-risk AI system and is provided with instructions for use. These instructions for use must contain certain minimum information, whereby an "appropriate level" of transparency must be ensured overall.

Compliance with Art. 13 AI Act also plays a major role in the conformity assessment of a medical device or IVD using AI and is a certification requirement for both the AI system and the medical device or IVD (see question 6).

In addition to this mandatory information, manufacturers of medical devices should provide information that is as transparent as possible from the outset. The main purpose of this is to **enable** the user to implement the obligations of the GDPR in the first place, as already mentioned. If manufacturers of medical devices take the user's questions into account at the design and marketing stage, this can become a real selling point.

## 20. What does all this mean for the practical approach of medical device providers who want to use AI systems?

→ The explanations in this white paper show: **AI systems in medical devices require a multidisciplinary perspective, expertise in numerous specialist areas and, above all, interface skills**. Regulatory knowledge of the MDR and IVDR alone is no longer sufficient for the use of AI in medical devices and IVDs. In practice, compliance with the requirements of the AI Act, the conformity assessment of AI systems and the strong reference to IT and data protection can only be achieved by a team of experts with in-depth specialist knowledge in their respective fields, the ability and willingness to work together intensively and the necessary sensitivity for the consolidation of information and results at the interfaces. Close teamwork between regulatory, medical technology, AI, IT, cybersecurity and data protection experts is required here - at both the legal and technical level.

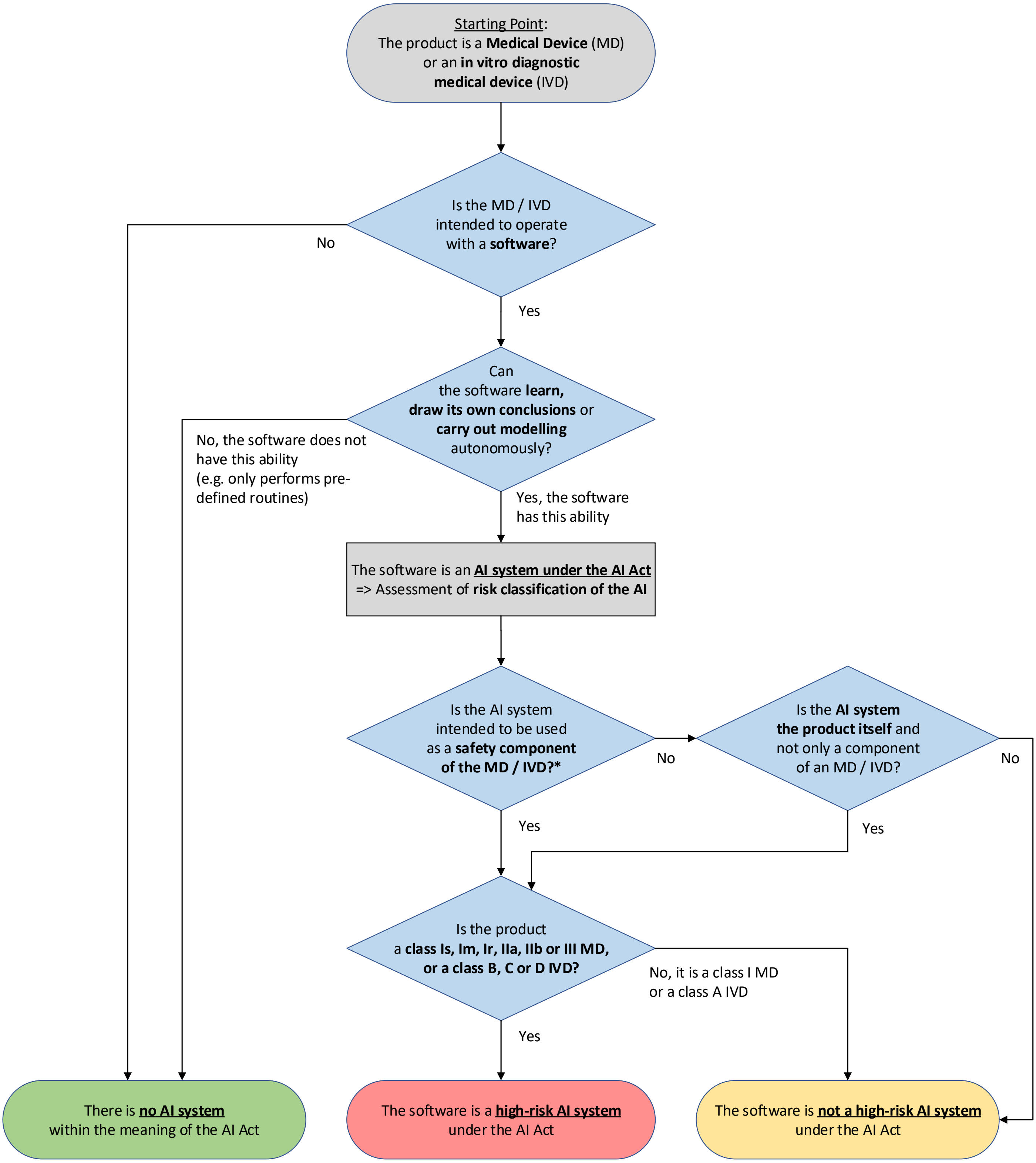
IT knowledge alone will not suffice to comply with the new AI regulations. The conformity assessment procedure and certification system under the AI Act are strongly based on medical device regulation and are a completely new system for the “traditional” IT and data protection sector. In-house teams and consultants who combine expertise in medical device regulation and IT and data protection issues and can therefore deliver holistic solutions from a single source have a clear advantage here.

**For the company organization, this means:**

Regulatory affairs in the age of AI is no longer limited to detailed knowledge of the MDR and IVDR and their practical application - in the future, additional experts will be needed in this area, especially from the IT, cybersecurity and data protection sectors, in order to be fully compliant. When putting together their in-house teams and consultants, manufacturers of medical devices and IVDs with AI systems should therefore ensure that they take a multidisciplinary approach and cover the required interface expertise and work in every product development holistically in this sense from the outset. This avoids problems and disruptions, e.g. within the uniform conformity assessment procedure for medical devices and AI systems, as well as data protection errors in the training phase of the AI or when it is used in practice. Medical devices and IVDs with AI systems offer a unique opportunity for the future for those who position themselves correctly in terms of their people - both internally and externally.

# Test scheme

## Determining the presence of an AI system according to the AI Act and risk classification of the AI system for medical devices and in-vitro diagnostics


Starting Point:
The product is a Medical Device (MD) or an in vitro diagnostic medical device (IVD)
Is the MD / IVD intended to operate with a software?
No
Yes
Can the software learn, draw its own conclusions or carry out modelling autonomously?
No, the software does not have this ability (e.g. only performs pre-defined routines)
Yes, the software has this ability
The software is an AI system under the AI Act
=> Assessment of risk classification of the AI
Is the AI system intended to be used as a safety component of the MD / IVD?*
No
Is the AI system the product itself and not only a component of an MD / IVD?
No
Yes
Yes
Is the product a class Is, Im, Ir, IIa, IIb or III MD, or a class B, C or D IVD?
No, it is a class I MD or a class A IVD
Yes
There is no AI system within the meaning of the AI Act
The software is a high-risk AI system under the AI Act
The software is not a high-risk AI system under the AI Act

*In case of doubt, a component is a safety component if the AI system fulfills a safety function or if its failure or malfunction endangers the health or safety of persons or objects.

Annex II

# Checklist

## on the formal requirements of the GDPR

In order to implement the formal requirements of the GDPR with the greatest possible legal certainty, manufacturers and users of smart medical devices should carry out the following documentation and testing steps in particular. For ease of reading, the term "use of the medical device" is used consistently below. However, the basic data protection requirements must be observed in every life cycle of an AI-supported medical device, i.e. both in the training phase and in the subsequent utilization phase. The requirements of the GDPR therefore address the manufacturer and user of the medical device in equal measure, at least insofar as there is responsibility under data protection law.

**The following questions need to be clarified when using an AI-supported medical device:**

□ Are the main processing operations and data flows using the medical device known and have these been documented?

□ Is there a sufficient (technical) understanding of the basic functioning of the AI components used?

□ Has it been checked whether and to what extent personal data is processed using the medical device?

□ Has it been checked and documented whether and to what extent anonymized, pseudonymized or synthetic data could also be used for the respective intended purpose of the medical device?

□ Has it been checked whether the general principles of Art. 5 (1) GDPR can be (technically) implemented and whether this can be demonstrated to the data protection supervisory authority in accordance with Art. 5 (2) GDPR?

□ Has the existence of a legal basis under data protection law been checked and documented? Has a possible change of purpose pursuant to Art. 6 (4) GDPR been taken into account?

□ Are data subjects provided with meaningful data protection notices in accordance with Art. 13, 14 GDPR?

□ Is there a written rights and roles concept that specifies access to the respective personal data?

□ Are mechanisms provided that enable the exercise of data subject rights in accordance with Art. 15 et seq. GDPR (information, rectification, erasure, etc.)?

□ Has it been checked whether and to what extent automated decision-making is carried out in accordance with Art. 22 para. 1 GDPR and whether this is permitted under data protection law?

□ Has the data processing using the medical device been transferred to the processing directory in accordance with Art. 30 GDPR?

□ Have appropriate technical and organizational measures been taken in accordance with Art. 32 GDPR to safeguard the rights and freedoms of data subjects?

□ Is there an action plan in place to deal with a personal data breach in accordance with Art. 33, 34 GDPR?

□ Has a data protection impact assessment been carried out in accordance with Art. 35 GDPR?

□ Have any contractual relationships with other parties (service providers, affiliated companies, etc.) been concluded and checked for data protection compliance?

□ Has it been checked whether and to what extent a third country transfer within the meaning of Art. 44 et seq. GDPR takes place? Has a transfer impact assessment been carried out?

□ Was the data protection officer involved in the data protection audit at an early stage?

# Our Focus Group Digital Health:

## Master the challenges of digitalisation in the healthcare sector with SKW Schwarz

The digitalisation of society continues to advance, and the healthcare industry is no exception. In fact, in the field of Life Sciences & Health, digitalisation stands as one of the central challenges and opportunities for companies in the coming years. This transformative process demands expertise in the ever-increasing complexity of regulations, a deep understanding of the underlying fields of law and their intersections, combined with the necessary innovative strength and creativity, all of which we, as a law firm, combine.

### Transform the healthcare industry with us:

Our specialists will advise you on your challenges - digitalisation is our core expertise.

We think ahead and, with our focus on Life Sciences & Health, IT & data protection and IP, combine all relevant areas for the digitalisation of the healthcare sector in our "Digital Health" focus group, from expertise in regulatory and compliance, IT law, IP law and data privacy law to procurement, commercial and corporate law. This makes SKW Schwarz your ideal partner in all areas related to "Digital Health". We combine the knowledge and experience of our experts for your digitalisation projects to provide advice from a single source

Innovative business ideas with digital products and services for the healthcare sector have the potential to reshape our society. We understand the needs of the healthcare industry and assist you, whether your company is in the start-up phase or involved in a transaction – always keeping an eye on the bigger picture. Our corporate law specialists work closely with our experts in Life Sciences & Health and IT/data protection law.

Whether it's the digitalization of medical devices, legally compliant solutions for the use of AI, tenders for digital healthcare services or the development of health apps and DiGAs - our team is at your side with comprehensive expertise. We also help you to master the complex legal requirements of social media marketing and digitalization in the hospital sector.

Find out more about our focus group work and get our exclusive whitepapers on healthcare compliance and data protection for medical devices on our landing page. Contact us for further information and let us convince you of our expertise.

# **Our Experts** in Digital Health

**Dr. Oliver Stöckel**
Partner

☎ +49 89 28640-255
✉ o.stoeckel@skwschwarz.de

**Afra Nickl**
Associate

☎ +49 89 28640-255
✉ a.nickl@skwschwarz.de

**Fabian Bauer, LL.M.**
Counsel

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

**Marius Drabiniok**
Associate

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

SKW Schwarz

**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

**20457 Hamburg**
Willy-Brandt-Straße 59
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**