AI-supported DPIA documentation using SDM 3.1

Thomas Werning

AI-supported DPIA documentation using SDM 3.1

Contents

1. Introduction: DPIA, AI and standardisation
2. Role of AI in DPIA documentation – opportunities and limitations
3. Legal framework: When is a DPIA required?
   3.1 DPIA according to Art. 35 GDPR
   3.2 Risk characteristics of AI systems in healthcare
4. SDM 3.1 and its cubical model
   4.1 Processing steps – what happens to the data
   4.2 Processing levels – where the data is processed
   4.3 Assurance objectives – how data protection quality is measured
   4.4 The SDM cube as a risk analysis tool
   4.5 Risk transfer and risk enrichment between levels
5. From GDPR requirements to structured and verifiable TOM with the SDM
6. Formulation aids: How processing and TOM can be described as 'AI-processable'
   6.1 Structured Visualisation and formatting
   6.2 Using AI to fill gaps / generate suggestions
   6.3 Clear assignment to warranty objectives
   6.4 Modularity and reusable building blocks
   6.5 Consistent terminology
   6.6 Risk-related context
   6.7 Machine-readable formats (tables, tools, exports)
7. Practical example: AI voice assistant in hospitals
   7.1 Description of processing and system architecture
   7.2 Start of documentation: purpose, legal basis, involved parties, abstract risks
   7.3 Specific risks and TOM along the warranty objectives
8. Recommendation for data protection officers: TOM documentation for automated DPIA creation
9. Sentence templates, standard texts and AI-supported evaluation
10. Conclusion: SDM 3.1 as a key tool for DPIA in the context of AI

1. Introduction: DPIA, AI and standardisation

Data protection impact assessment (DPIA) is one of the most challenging tools in data protection management – especially when modern, complex and sometimes opaque technologies such as AI systems are used. This is particularly true for healthcare, for example with AI-based voice assistants for patient communication, appointment scheduling or as a first contact in service processes.

In this article, I will repeatedly use the example of '**AI voice assistants in** hospitals'.

In these constellations in particular, data protection risks must be identified at an early stage, evaluated in a structured manner and mitigated by appropriate technical and organisational measures (TOM). The DPIA not only serves the purpose of pure risk identification, but is also a central element of accountability: controllers must be able to demonstrate that they adequately protect the rights and freedoms of data subjects and effectively implement the requirements of the GDPR.

This article shows **how the documentation of the DPIA** can be supported in a practical manner through the **combined use of artificial intelligence (AI)** and the **Standard Data Protection Model (SDM) 3.1**. AI serves as a tool for structuring, consolidating and checking information. SDM 3.1 provides the methodological basis for systematically deriving verifiable measures from legal requirements and documenting them in line with the assurance objectives.

The key points here are that

- **AI remains a tool**, not a decision-maker.
- **The SDM is a method** that helps to record, organise and evaluate information in a structured manner.
- **Risks and measures** are always **assessed** by qualified persons, in particular data protection officers and the DPIA team.

2. Role of AI in DPIA documentation – opportunities and limitations

AI systems can make it much easier to create DPIA documentation. They are particularly helpful when it comes to evaluating extensive technical documents such as system descriptions, directories of processing activities or security concepts, identifying typical risks and vulnerabilities, assigning measures to warranty objectives or checking existing documentation for contradictions and gaps. They can also be used to generate consistent text modules for reports and to standardise the language of existing texts.

For example, AI can automatically generate suggestions for risk-measure mappings from TOM documentation structured according to SDM or insert standardised descriptions into DPIA templates. In this way, parts of the documentation can be automated, resulting in greater consistency in presentation and improved traceability.

At the same time, the limits have to clearly stated. AI cannot make a legal decision as to whether a residual risk is acceptable, nor can it conclusively assess whether the measures chosen are sufficient for a certain level of protection. A DPIA in the sense of accountability cannot be generated fully by AI; responsibility remains with the controller or data protection officer. Furthermore, AI itself is part of the process and is therefore itself subject to the risk analysis.

The goal is therefore not fully automated 'DPIA at the touch of a button,' but rather AI-supported DPIA. In this model, AI primarily takes on tasks such as structured processing, consistency checks and text generation, while the technical and legal assessments is carried out by humans.

3. Legal framework: When is a DPIA required?

3.1 DPIA according to Art. 35 GDPR

Art. 35 GDPR obliges controllers to carry out a DPIA if a form of processing – in particular when using new technologies – is likely to result in a high risk to the rights and freedoms of natural persons due to its nature, scope, circumstances and purposes. This is typically the case when special categories of personal data within the meaning of Art. 9 GDPR are processed on a large scale, when systematic monitoring takes place, when largely automated decision-making processes are used, or when novel or opaque technologies, such as generative AI, are used.

The DPIA itself comprises a systematic description of the planned processing, an assessment of the necessity and proportionality of this processing in relation to the purposes pursued, an assessment of the risks to the rights and freedoms of the data subjects, and a description of the measures envisaged to mitigate these risks and demonstrate compliance with the GDPR.

3.2 Risk characteristics using the example of an AI system in healthcare

When using an AI-based voice assistant in a hospital switchboard, several risk-relevant characteristics occur simultaneously. Health data, such as information on the specialist field or the reason for treatment, is regularly processed when appointments are made. According to Art. 9 GDPR, this data belongs to the categories requiring special protection and is therefore associated with an increased need for protection from the outset, or its processing is prohibited unless special exceptions apply. In addition, the system communicates independently with a large number of patients and communication is largely automated, which increases the scope and frequency of processing. Audio processing and, where applicable temporary or permanent recordings create a monitoring character that affects the confidential communication. Many AI models also operate as black boxes, with their decision-making logic only partially comprehensible, which conflicts with the transparency and traceability expectations of data protection law. Finally, the voice assistant sometimes makes decisions that are directly relevant to care, such as when appointments are made, prioritised or forwarded.

When using an AI-based voice assistant in a hospital switchboard, several risk-relevant characteristics are **cumulatively** present:

1. **Processing of health data**
   In the context of appointment scheduling, particularly sensitive health data (e.g. specialisation, reason for treatment) is regularly processed.

2. **Extensive, automated processing**
   The system communicates independently with a large number of patients. Communication is largely automated, which increases the scope and frequency of processing.

3. **Potential monitoring character**
   Audio processing and possible recordings may give rise to a monitoring character. This poses a particular risk to the confidentiality of communication.

4. **Use of new generative AI technologies**
   Many AI models operate as black boxes. Their decision-making logic is difficult to understand, which makes the transparency and traceability of processing difficult.

5. **Partially automated decisions relevant to care**
   Decisions about appointment scheduling, prioritisation or referral, for example, can have a direct impact on medical care.

Taken together, these characteristics lead to a presumably high risk, making it imperative to carry out a DPIA.

The positive lists and guidance provided by the supervisory authorities, in particular the publications on DPIA pursuant to Art. 35 GDPR, also confirm this classification in comparable constellations.

4. The SDM 3.1 and its cubical model

The Standard Data Protection Model (SDM) 3.1 acts as a bridge between abstract legal requirements and concrete technical and organisational measures. It translates the requirements of the GDPR and systematically links them to processing steps and levels. At the heart of this methodology lies the SDM cube, which maps the various dimensions of processing in a three-dimensional model.

4.1 Processing steps – what happens to the data

The SDM distinguishes between **nine processing steps** that map the life cycle of data: collection, preparation, storage, processing, use, provision, merging, restriction, disposal

In practice, these steps can be grouped into **four phases**:

1. **Collection**
2. **Making available** (in particular storing, restricting)
3. **Use** (processing, using, providing, merging)
4. **Deleting/disposing**

Each step can involve its own risks. For example, errors occuring during data collection, while unauthorised access is possible during provision.

4.2 Processing levels – where the data is processed

Processing is considered at **three levels** in the SDM:

- **Level 1: Specialist procedures**
  Business processes and procedures – e.g. 'Making an appointment at the hospital'.
- **Level 2: Specialist application**
  Software and applications used to implement the specialist procedure – e.g. the AI language assistance system.
- **Level 3: Infrastructure**
  Technical basis such as servers, networks, cloud services, platforms

This separation helps to distinguish between **functional risks** (in the process flow) and **technical risks** (system and infrastructure level) while still considering them in conjunction with each other.

4.3 Warranty objectives – how quality of data protection is measured

The SDM derives **seven assurance objectives** from the GDPR (in particular Art. 5 GDPR):

- **Data Minimisation** – Only data that is absolutely necessary for the specified purpose is processed.
- **Transparency** – Data subjects and controllers can understand processing operations; information and disclosure obligations are fulfilled.
- **Unlinkability** – Data from different contexts is not combined in an impermissible manner or evaluated across contexts.
- **Intervenability** – Data subjects can effectively assert their rights.
- **Integrity** – Protection against unauthorised or unintentional alteration of data.
- **Confidentiality** – Protection of personal data against unauthorised access or disclosure.
- **Availability** – Data and systems must be reliable and available for use in a timely manner.

These objectives form the benchmark for assessing whether processing is compliant with data protection regulations and adequately secured. For each combination of processing step and processing level, a check is carried out to determine whether the assurance objectives have been achieved.

4.4 The SDM cube as a risk analysis tool

Combining the **processing steps**, **processing levels** and **assurance objectives** creates the three-dimensional **SDM cube**. Each 'small cube' represents a precisely definable section of the processing: a specific processing step, at a specific level, taking into account a specific assurance objective. This reveals where risks arise in the process and how they should be addressed with measures.

The SDM cube ensures that no dimension of processing is overlooked. Risks can be **identified at the level** and **addressed precisely** through documented TOM. Specialist procedures, specialist applications and infrastructure are not viewed as separate silos, but are analysed during their interaction with each other – which is absolutely essential, especially in modern AI systems.

4.5 Risk transfer and risk enrichment between levels

A frequently underestimated but central added value of the SDM cube is that it makes **risk transfers between levels visible**. Risk analysis is not carried out in isolation for each level, but takes into account mutual dependencies and possible 'infections' between the levels: requirements arising from the specialist procedure at level 1 – such as medical, organisational or legal requirements – must be consistently transferred to the specialist application at level 2 and to the technical infrastructure at level 3. If, for example, the specialist procedure 'appointment scheduling in hospitals' does not allow complete conversation recordings in order to comply with the principle of data minimisation, this must be ensured technically in the application through appropriate configuration and architecture. If the specialist procedure requires patients to be able to change or delete appointments at any time, the application/infrastructure must provide appropriate interfaces and authorisations. **In this way**, **the requirements from level 1 are passed down** and specified in technical and conceptual terms.

However, the risk transfer also works in the other direction: processing that is initially harmless at level 1 can suddenly reach a significantly higher risk level due to technical features at levels 2 or 3, even though the technical purpose remains unchanged. For example, a simple appointment scheduling process becomes high-risk processing if it is implemented by an AI-based voice assistant that uses external cloud components, employs generative models, processes audio recordings and has limited transparency in its decision-making logic. The same applies if the underlying infrastructure is based on a cloud provider that transfers data to third-party countries or whose logging systems are not fully controllable. This increases the risks for the entire business process, even if the business application has been developed 'cleanly' from a functional perspective.

The three-dimensional structure of the SDM cube systematically shows where risks arise, how they intensify along the levels, and where TOM should be applied to secure the processing as a whole. **The cube makes it clear that processing is only as secure as its most vulnerable level and that risks can spread both from top to bottom and from bottom to top.** This is particularly important in the context of AI because many risk-relevant factors are not rooted in the process but in the technical implementation. The reciprocal transfer of risk explains why AI processing is often classified as high-risk processing, even though the technical process has remained unchanged.

5. From GDPR requirements to structured and verifiable TOM with the SDM

SDM translates the abstract requirements of the GDPR into concrete, verifiable requirements and measures. The starting point is the legal standards, in particular Art. 5 GDPR with the principles of processing and accountability, Art. 25 GDPR with the concept of data protection through technology design and data protection-friendly default settings, Art. 32 GDPR with the requirements for the security of processing, and Art. 35 GDPR with the obligation to conduct a data protection impact assessment for high-risk processing.

The SDM approach can be described in three steps:

Step one: Assigning legal requirements to warranty objectives
First, the legal requirements are assigned to the warranty objectives. The aim is to translate each abstract legal requirement into one or more verifiable requirements.

- **Data minimisation** – Art. 5(1)(c) GDPR (data minimisation), Art. 5(1)(b) GDPR (purpose limitation)
- **Transparency** – Art. 5(1)(a) GDPR (transparency), Art. 12–14 GDPR (information obligations), Art. 15 GDPR (right of access)
- **Unlinkability** – Art. 5(1)(b) GDPR (purpose limitation), Art. 5(1)(c) GDPR (data minimisation), Art. 6 GDPR (legal basis for each purpose)
- **Intervenability** – Art. 12–23 GDPR (rights of data subjects), Art. 24(1) GDPR (obligations of the controller to implement), Art. 5(1)(a) GDPR (good faith)
- **Integrity** – Art. 5(1)(f) GDPR (integrity), Art. 32(1) GDPR (protection against alteration)
- **Confidentiality** – Art. 5(1)(f) GDPR (confidentiality), Art. 32(1) GDPR (access controls, TOM)
- **Availability** – Art. 32(1)(b) and (c) GDPR (recoverability, resilience), Recitals 49 and 83 GDPR

Step two: Derivation of generic measures for each assurance objective
Generic measures are now defined for each protection objective, i.e. a 'target set' of TOM that are typically suitable for achieving the respective objective.

- **Data minimisation**: Objective: Process as little personal data as possible.
    - Specifying and defining the purpose before processing begins
    - Reduction of mandatory fields and input (only necessary data)
    - Pseudonymization or anonymisation where possible
    - Role concepts that only display necessary data
    - Deletion and storage limitation concepts, including automated deletion routines
    - Avoidance of permanent storage (e.g. transient storage, edge processing)
    - Privacy-friendly default settings (privacy by default)

- **Transparency**: Objective: Traceability of processing for data subjects and controllers.
    - Complete, easily understandable data protection notices
    - Documentation system for processing activities
    - Logging of processing steps (logging)
    - Procedure for processing requests for information
    - Labelling and description of automated systems, algorithms, AI logic
    - Clear internal guidelines and procedural instructions

- **Unlinkability**: Objective: No unauthorised merging of data from different contexts.
    - Strict separation of purposes in specialist procedures and databases
    - Use of context separation (e.g. client separation)
    - Segmentation of data sets, separate key management
    - Prevention of excessive profiling
    - Prohibition of cross-system identifiers
    - Role-based visibility: users only see context-related data
    - Checks to determine whether new processing could lead to a loss of purpose limitation

- **Intervenability:** Objective: Data subjects can effectively exercise their rights.
    - Standardised processes for data subject rights (access, erasure, rectification, objection)
    - Technical implementation options: marking, restriction, blocking, deletion
    - Workflows for internal processing of data subject requests
    - Interfaces for rectification or erasure in IT systems
    - Mechanisms for processing revocations (e.g. revocation of consent)
    - Monitoring of deadlines (1 month according to Art. 12(3) GDPR)
    - Clear responsibilities (‘owner’ for data subject rights)

- **Integrity:** Objective: Protection against unauthorised or accidental alteration of data.
    - Use of cryptographic methods (hashing, signatures)
    - Dual control principle for critical changes
    - Authorisation concepts with change and write protection
    - Version and change management
    - Logging of all changes (tamper protection)
    - Validation and plausibility checks on entries
    - Ensuring data accuracy through quality controls

- **Confidentiality:** Objective: Protection against unauthorised access and disclosure of data.
    - Authentication (MFA), authorisation, role and rights concepts
    - Data encryption (storage + transport)

    - Network security measures (firewalling, segmentation, VPN)
    - Access restrictions (need-to-know principle)
    - Training to prevent social engineering
    - Confidentiality agreements and commitment to data secrecy
    - Secure storage and transport of data carriers

- **Availability:** Objective: Data and systems must be available for use when needed.
    - Backup and recovery processes (including tests)
    - Redundant system architecture, clusters, failover systems
    - Monitoring of systems, failure and incident management
    - Emergency and crisis management plans
    - Protection against ransomware (e.g. immutable backups)
    - Physical security (fire, burglary, water and power protection)
    - Service level management (response times, recovery times)

Step three: Conversion into concrete, verifiable TOM for individual processing
These generic measures are now applied to the specific procedure. **Each measure is described in such a way that its implementation can be objectively verified**, for example by providing information on the encryption technology used, the frequency of backups, the structure of the authorisation concept or the design of the logging system. The **SDM reference measures catalogues** provide a valuable basis for checking whether the existing set of measures corresponds to the legally required target state. For the DPIA, this means that the risk analysis can be carried out in line with the assurance objectives, that concrete TOM are stored for each identified risk, and that traceability for audits and supervisory authorities is made considerably easier.

6. Formulation aids: How processing and TOM can be described in a way that is 'AI-processable'

An essential step towards **AI-supported DPIA creation** is to describe processing activities and TOM in such a way that they can be easily evaluated not only by humans but also by AI systems. The more standardised and structured the description, the easier it is to automatically analyse and evaluate the content and transfer it into report structures.

6.1 Structured presentation and formatting

In order to document TOM in a machine-readable format that is optimally usable for AI systems, a structured and uniform presentation is recommended. Each measure should be recorded in a consistent format, such as a tabular or modular description with fixed fields for the protection goal addressed, the name of the measure, a description of how it works, the purpose or risk addressed, the relevant processing step and processing level, and, if applicable, its classification as a technical or organisational measure and its implementation status. Such standardised documentation not only makes it easier for people to quickly find their way around, but also helps AI systems in particular to reliably recognise content. For example, if the protection goal and measure name are clearly separated fields, this information does not first have to be extracted from continuous text. A clear assignment to the processing step and level further increases the precision of the automated risk analysis. The SDM offers a method and orientation here, in which each 'sub-cube' with its requirements can be addressed by the coordinate system.

6.2.Using AI to fill gaps / generate suggestions

Structured TOM descriptions based on this system also form the basis for AI systems to identify gaps in the set of measures and make meaningful suggestions for additions. Once processing has been documented in this form, AI can, for example, determine that no measures have yet been defined for certain risks, that measures exist without a traceable assignment to protection goals, or that certain combinations of protection goals, processing steps and levels have not been addressed at all. It can also point out inconsistent information, for example if a protection goal has been chosen inappropriately or a measure has been assigned to the wrong level. AI can also contribute suggestions from reference catalogues and best practices and – for example for AI-specific scenarios – suggest additional TOM, such as logging or audit mechanisms. **The system systematically identifies areas where documentation is incomplete or unbalanced,** for example, where many measures exist to protect confidentiality, while transparency or intervenability are only addressed in a rudimentary manner.

AI can systematically help to:

- identify missing assignments to protection goals, processing steps or levels,
- providing information when a risk exists without an associated measure or vice versa,

- suggesting further measures that are customary in the industry or provided for in the SDM catalogue of measures,
- identify inconsistent information (e.g. incorrect level, inappropriate protection goal),
- make recommendations on how to complete the documentation ('Measures are missing in the 'Edit' step for the protection goal 'Integrity''),
- supply industry- or technology-related TOM (e.g. suggestions for AI-specific logging or audit mechanisms).

6.3 Clear assignment to assurance objectives

When describing individual measures, it should always be clear which assurance objective is the primary focus. This can be done using explicit fields such as 'Protection objective: Confidentiality' or integrated into the description, for example by describing the purpose of the measure in relation to the objective. An AI can then systematically compile and evaluate all measures relating to a specific protection objective and integrate them into DPIA reports. This also makes it easier for human evaluators to determine whether a protection objective is sufficiently covered by measures or whether gaps remain.

6.4 Modularity and reusable building blocks

It makes sense to describe each TOM as modularly as possible. Collective measures, in which access control, encryption and logging are combined in a single text, for example, make both human and machine evaluation more difficult. It is better to separate these aspects into separate measures, each addressing a main protection goal. A modular structure facilitates the reuse of measures in different processing operations and enables AI to assign building blocks to specific risks and reuse them in different contexts.

6.5 Consistent terminology

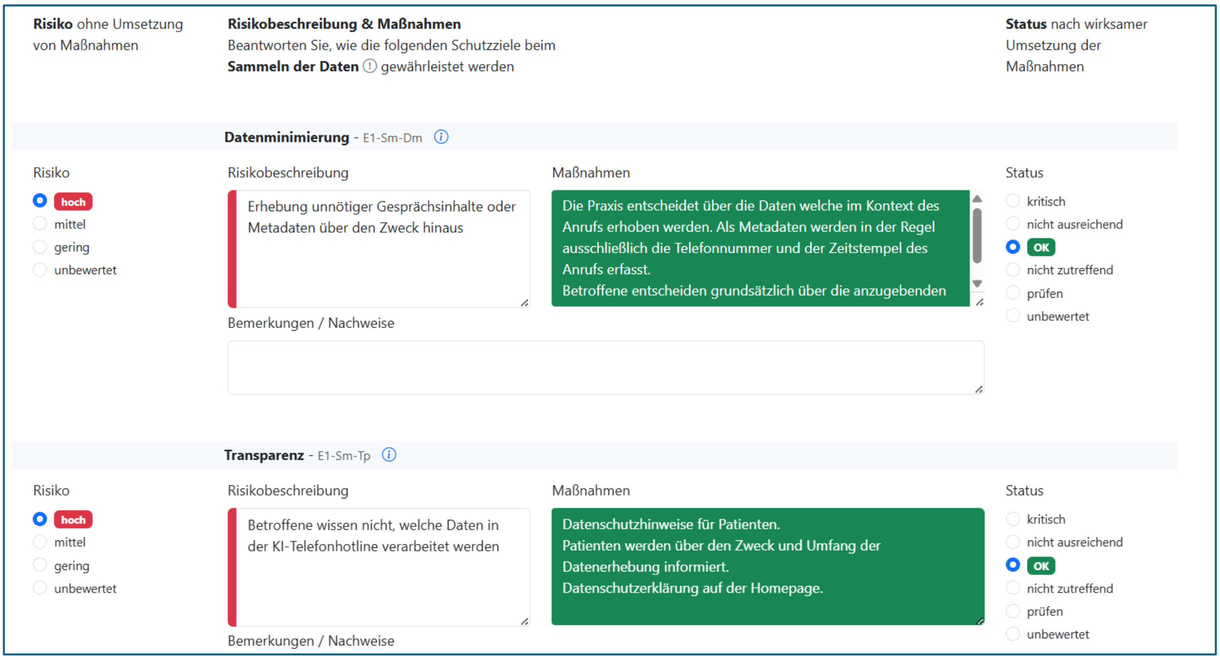
Another building block for AI-processable documentation is consistent and standardised terminology. Terms such as 'health data', 'access control', 'encryption', 'pseudonymisation' or 'logging' should always be used in the same way in a document, rather than varying constantly. The more closely the choice of terms is based on established standards such as BSI basic protection, ISO standards or the SDM itself, the easier it is for AI systems to classify content and link it to external knowledge sources. Inconsistent terms, on the other hand, lead to semantically identical measures being treated as different objects, which makes evaluation more difficult.

6.6 Risk-related context

The relationship to a specific risk should be apparent for each measure. A description such as 'restricted access to voice recordings to protect against unauthorised access to patient data' directly links the measure to the risk. This enables AI to automatically link risks and measures, compare risk lists with lists of measures, and identify gaps. This connection is also essential for the DPIA itself, as its aim is precisely to raise awareness of risks and demonstrate the effectiveness of risk mitigation measures.

6.7 Machine-readable formats (tables, tools, exports)

In addition to readable documentation in classic document formats, a machine-readable format should be maintained, e.g. in the form of tables (Excel, CSV), data models in a data protection tool or standardised exports from data protection management software. Processing directories, TOM, risks and DPIA modules should be linked via a uniform schema so that AI systems can access this structured data directly without first having to analyse complex continuous text. Such a structure also facilitates further development towards automated interfaces to IT systems.



Source: https://www.MoeWe-Datenschutz.de – query of risk and measure

7. Practical example: AI voice assistant in hospitals

7.1 Description of processing and system architecture

In this practical example, an AI-based voice assistant is used to make appointments via telephone in a hospital. The system conducts dialogues with patients in natural language, takes appointment requests, reschedules or cancels existing appointments, and answers simple organisational questions. In the background, the assistant accesses the hospital information system (HIS) to determine available appointments or assign patient data, for example.

Technically, the solution is based on components for speech recognition and speech synthesis, AI-supported dialogue control, and interfaces to calendar and patient databases. Depending on the design, external cloud services, such as for speech processing, are also integrated.

Looking solely at the specialist procedure of 'appointment scheduling', the risk initially appears to be rather low. However, the integration of an AI infrastructure, especially in combination with cloud services, significantly increases the risk. The SDM cube shows that significant additional risks arise at the level of the specialist application and infrastructure, but that their effects extend to the entire procedure. The DPIA must therefore consider the overall procedure in the interaction of all levels.

7.2 Start of documentation: purpose, legal basis, parties involved, abstract risks

The starting point for documentation is the **purpose of the processing**. In this example, the purpose is to handle appointment scheduling and management in the hospital by telephone. This purpose is fundamentally legitimate and is in the interests of both patients and the hospital. However, the level of risk changes significantly depending on the type of technical implementation, i.e. the use of AI and cloud components, the sensitivity of the data processed – especially health data – and the degree of automation of communication.

The second step is to establish **the legal basis**. Without a valid legal basis, data processing in compliance with data protection regulations is not possible. It is necessary to explain which standards are relevant, such as Art. 6(1)(b) GDPR for the fulfilment of the treatment contract in connection with appointment-related processes and, if applicable, Art. 9(2) GDPR for the processing of health data. At the same time, it must be explained how these legal bases relate to the purpose and whether consent is required for individual sub-processing operations, such as recording conversations or specific cloud usage.

Subsequently, **access and participants** are described. This includes which internal and external actors are involved in the processing – for example, the hospital itself, external IT service providers, cloud providers or the manufacturer of the AI system. The roles and responsibilities of these actors must be described, whether they act as controllers, processors or sub-processors, and how data transfers are contractually secured, for example through processing agreements and technical and organisational commitments.

On this basis, an **abstract risk analysis** can be carried out in the sense of a **threshold test**. This involves assessing whether the nature and scope of the processing, the categories of data concerned, the use of new technologies and possible monitoring aspects are likely to pose a high risk to the rights and freedoms of the data subjects. In the present example, this is the case, so that the obligation to carry out a DPIA must be affirmed. This abstract consideration is then deepened in the DPIA by a concrete risk analysis along the lines of the warranty objectives.

7.3 Specific risks and TOM in line with the assurance objectives

Specific risks are now identified **for each guarantee objective** and assigned **appropriate TOM**.

- **Data minimisation:** *Risk:* More data is collected than is necessary for making an appointment, e.g. complete recordings of conversations including medical details, even though only the name, date of birth and desired specialist area may be necessary for booking an appointment. *Measures:* The system has been designed so that **only necessary information** is requested. Conversations are **not recorded in full;** instead, the relevant data points (appointment, patient data) are extracted and stored directly. Audio recordings are **deleted immediately** after speech recognition or are not persisted at all. In addition, it is configured which entries are mandatory and which are voluntary in order to avoid data overload. These measures ensure that the principle of data minimisation is upheld and that no unnecessary personal data is collected.
- **Availability:** *Risk:* Patients may be unable to make appointments due to a system failure (service unavailable) or booked appointments may be lost. In a hospital, lack of availability can also affect care. *Measures:* The service is operated in a **highly available architecture**. This means that redundancies exist – such as multiple server instances and fallback routines in case a server fails. In addition, all appointment bookings are stored **transactionally** in the hospital's central database and synchronised with the hospital information system. If the AI assistant is unavailable (e.g. during maintenance), a **fallback to human staff** is set up so that callers can be seamlessly transferred to an employee. Regular **backups** of appointment data and a disaster recovery plan round off the precautions. This ensures the constant availability and resilience of the service in accordance with Art. 32 GDPR.
- **Integrity:** *Risk:* The processed data (e.g. appointment time, patient name) could be incorrect or altered without authorisation. Voice assistant systems carry the risk of **recognition errors** – for example, an incorrect date being understood and entered. Malicious manipulation (attackers changing appointment or patient data) is also conceivable. *Measures:* Several controls have been built in to ensure data integrity. Firstly, the assistant asks for **critical information to be confirmed** – for example, the recognised appointment with the date/time is read back to the patient and confirmation

is requested in order to catch input errors. Secondly, **change logs** are kept: every appointment booking or change made by the AI is logged with a timestamp and AI ID so that subsequent changes can be checked. Unauthorised changes are prevented by **access restrictions** – for example, the AI only has write access to appointment fields, but not to other patient data. Finally, regular **data validations** (comparison between the appointment schedule and the speech recognition log) ensure that recognised texts and stored data are consistent. These measures ensure the accuracy and integrity of the processing results.

- **Confidentiality:** *Risk:* Unauthorised persons could eavesdrop on or intercept sensitive information mentioned in the conversation (medical information, personal data). As this involves health data, a breach of confidentiality would be particularly serious. There is also a risk that **employees or external parties could gain unauthorised access to system data** (e.g. audio files or transcripts). *Measures:* Strict **access controls** have been put in place to ensure confidentiality. Audio processing runs on isolated systems that only authorised administrators have access to. All stored data (such as extracted appointment and patient data) is stored **with strong encryption** (database encryption, TLS for transmission). The speech data is processed in the working memory during recognition and is not stored persistently. In addition, the voice assistant is configured so that it only stores general appointment data, but does **not** archive the exact wording of **conversations**. Call centre employees only see the results generated by the system (appointment confirmation), but not a recording. In addition, the service was subjected to a **penetration test** to ensure that no unauthorised external access is possible. In summary, these TOM significantly reduce the risk of a breach of confidentiality by ensuring that only authorised persons have access to the data and that intercepted data is unusable for third parties.

- **Unlinkability:** *Risk:* The data collected in the appointment assistant could be merged with other databases, e.g. to create profiles of patients (e.g. combining appointment data with medical records or marketing data). This would violate the **principle of purpose limitation**, as data from the appointment scheduling system would be used for purposes other than those for which it was intended. *Measures:* The service has been **logically separated from other systems.** Although necessary integration with the appointment calendar takes place, **no** further **transfer** of appointment data to marketing or analytics tools occurs. There are clear **purpose restrictions:** the data collected (reasons for appointments, available slots, etc.) is used exclusively for appointment management. **Pseudonymisation** also prevents patient identities from being directly identified via the appointment scheduling system – for example, cases used to analyse utilisation rates are stored without names. If there are interfaces to other hospital services, these are designed **with data protection agreements and technical barriers** in place so that only aggregated or anonymised information flows (e.g. statistics on the number of calls per week, but no personal content). In this way, the company ensures that no unauthorised linking of personal data from different sources takes place.

- **Transparency:** *Risk:* Patients may be left in the dark **about whether** and **how** their data is being processed by AI. In particular, it is important to avoid patients believing that they are talking to a human being when it is actually a machine – this would constitute deception with regard to data processing. The lack of records of the processing would also impair traceability. *Measures:* At the start of each call**, proactive information** is **provided** that this is an automated assistant and the purpose of the call (appointment scheduling) and the processing of the data mentioned are explained. In addition, callers receive a **data protection notice,** such as a reference to the hospital's data protection website, where data processing is explained in detail. All queries and responses from the system are **logged internally** so that it is possible to analyse later which data was processed and when. These logs can be made available to the data protection officer for review or in the event of requests from the supervisory authority. In addition, the procedure has been transparently documented in the hospital's directory of processing activities. Patients have the option of obtaining **information** about the processed data **retrospectively** by contacting the data protection team. These measures make the processing transparent for data subjects and auditors and meet the requirements of Art. 5(1)(a) and Art. 12 GDPR.
- **Intervenability:** *Risk:* Without special precautions, patients could have difficulty exercising **their rights** in connection with the voice assistance system. For example, a patient should have the option of cancelling a booked appointment or requesting the correction of an incorrectly entered name. If the system were inflexible in this regard, data subjects would effectively be restricted in their rights. *Measures:* The service is integrated in such a way that **manual intervention** is possible at any time. Patients can select an option in the telephone menu to be put through to a human employee if, for example, they want to make corrections. Every appointment made via AI is also **confirmed** to the patient by text message or email**,** with the option to cancel or change the appointment via a link. If a patient **revokes** their **consent** (if such consent was required) or generally exercises their right to erasure, the hospital has processes in place to specifically find and delete all data stored in the voice assistant relating to that person. In addition, employees have been trained to immediately respond to requests such as *'I do not want the conversation to be recorded'* – for example, by immediately stopping the recording or using a manual workflow. The DPIA also took emergency scenarios into account: e.g. what happens if the AI does not understand a request – in this case, intervention is possible through automatic forwarding to a colleague. All in all, the processes are designed in such a way that data subjects retain full control over their data and can exercise their rights under Articles 16–19 GDPR without great effort.

This example shows how **each assurance objective addresses practical risks**. By identifying the risks for each objective and taking appropriate countermeasures, a comprehensive TOM package was created for the provider. It is important that the measures were **documented** and described in a structured manner in line with the protection objectives – for example, the DPIA was able to show how **each identified risk** was **reduced to an acceptable residual level by a specific measure**. The **SDM methodology** helped the data protection team to consider all relevant aspects: from IT security (CIA protection objectives) to data protection principles (data minimisation, purpose limitation) and data subject rights. This made it possible to create the DPIA more efficiently and justify it to management and the supervisory authority in a comprehensible manner.

8. Recommendation for data protection officers: TOM documentation for automated DPIA creation

The combination of SDM methodology and AI support results in concrete recommendations for action for operational and regulatory data protection officers. It is important to always keep in mind that the **requirements** stem **from processing** and the legal situation and that SDM and AI are merely tools to map these requirements more efficiently and consistently.

Your own TOM catalogue should be structured consistently along the seven assurance objectives. A protection-goal-based structure, which provides a separate chapter for each protection goal, makes it easier to identify gaps and take targeted corrective action. This makes it immediately apparent if, for example, transparency measures are significantly weaker than confidentiality measures.

Datenschutzerreichungsgrad

Schutzziel	Anteil	Total	kritisch	fehlt	erfüllt	prüfen	unbearbeitet	n. z.
Datenminimierung	51 %	66	0	6	29	1	21	9
Transparenz	48 %	73	0	4	29	1	27	12
Nichtverkettung	52 %	43	0	2	22	1	17	1
Intervenierbarkeit	44 %	45	1	1	16	0	18	9
Integrität	60 %	141	0	19	73	1	29	19
Vertraulichkeit	68 %	185	1	17	114	1	34	18
Verfügbarkeit	63 %	112	2	12	64	0	24	10
Total	61 %	278	3	29	150	3	59	34

Source: https://www.MoeWe-Datenschutz.de – comprehensive evaluation of TOM

In addition, it is advisable to create a risk-based mapping for essential processing operations. For each relevant risk, the affected protection goal is named, the associated measure is presented and the remaining residual risk status is assessed. Such an assignment, which represents a kind of 'mini-DPIA' for each processing operation, facilitates later integration into more comprehensive DPIA processes and makes accountability under Art. 5(2) GDPR tangible. AI can help to uncover missing assignments or inconsistencies and suggest typical additions, but it does not replace human evaluation.

It also makes sense to work with modular, reusable measures. Many TOM – such as strong authentication, logging of administrative access or a standardised deletion concept – occur in numerous processing operations. If these modules are maintained centrally and referenced in different contexts, consistency increases and changes can be rolled out efficiently to all affected processing operations.

The use of data protection management software can help to link processing directories, risks, TOM and DPIA according to SDM logic. Import and export functions make it easier to provide structured data for AI systems. Nevertheless, it should be clear that software solutions support documentation but do not automate responsibility and evaluation. Future automations via MCP or API connections, which read out systems and update TOM lists, for example, will only simplify the process but will not change the legal requirements.

Ultimately, the quality of the documentation depends largely on the qualifications of the people involved. Specialist departments, IT, information security and data protection officers should be trained in SDM logic and know how to describe measures in a way that is protection-oriented and AI-processable . Regular checks (**PDCA)**, for example through reviews by the data protection officer, ensure that the documentation is complete, consistent and equally usable for both humans and machines.

9. Sentence templates, standard texts and AI-supported evaluation

If documentation structured according to specific standards is available, preferably SDM-based and machine-readable, AI-supported procedures can be used in a targeted manner. Information can be checked for contradictions, for example if processing is described as cloud-free, but external APIs are listed at the same time. AI can suggest further risks and measures based on reference catalogues or known best practices and pre-formulate, standardise or linguistically revise existing texts.

A particularly effective approach is the use of sentence templates. Here, standardised formulations are developed. The AI then simply inserts the specific key data for the respective processing into these templates. In practice, this could mean that a formulation such as ‘To ensure confidentiality in the 'storage' processing step at the infrastructure level, the database is protected by ...’ is used and the AI adopts the specific technical measures from the TOM catalogue.

As an example, the following prompt was used

> *Objective: The output should contain a complete matrix of all SDM coordinates, with each entry containing a correctly formulated sentence according to the following sentence template: {Practice} [for {target object}] {MODAL VERB} <Result> {Action word} (TAGs) (Notes)*
> *a. Add an explanation of why a particular modal verb was chosen for the question.*
> *b. Evaluate whether the question is answered by the measures described and justify your answer with references if possible.*

to generatet he following report::

SDM-Ebene	Phase	Gewährleistungsziel	Satz (nach Schablone)	TAGs/Hinweise	Begründung Modalverb	Bewertung Erfüllung
E1 – Verarbeitungstätigkeit	Sm – Erheben	Dm	Verarbeitungstätigkeit „**Terminvereinbarung per Telefonat**" für Gesprächs- und Termindaten MUSS die Erfassung auf vorab freigegebene, zweckgebundene Telefonate zur Terminvereinbarung und auf autorisierte Personen beschränken.	[E1][Sm][Dm][TELEFONIE] [TERMIN][FREIGABE]	MUSS, weil bei der Erhebung von Gesprächs- und Termindaten (inkl. evtl. sensibler Angaben) ein hohes Risiko besteht und die Begrenzung auf notwendige, legitimierte Anrufe verbindlich geregelt werden muss.	Weitgehend erfüllt, sofern nur legitimierte Mitarbeitende Termin-Telefonate führen und nur dafür erforderliche Daten erhoben werden; Wirksamkeit regelmäßig prüfen.
E1 – Verarbeitungstätigkeit	Sm – Erheben	Tr	Verarbeitungstätigkeit „**Terminvereinbarung per Telefonat**" für betroffene Anrufende MUSS zu Beginn des Telefonats klar über die Erfassung der Daten zur Terminvereinbarung informieren und die Rechtsgrundlage dokumentieren.	[E1][Sm][Tr][HINWEIS] [RECHTSGRUNDLAGE] [TERMIN]	MUSS, weil Transparenz nach DSGVO zwingend ist und Betroffene vor Beginn wissen müssen, dass ihre Angaben zur Terminvereinbarung verarbeitet werden und auf welcher Rechtsgrundlage.	Weitgehend erfüllt, wenn ein standardisierter Hinweis im Begrüßungsdialog erfolgt und Rechtsgrundlage (z. B. Vertrag/Anbahnung) dokumentiert ist.
E1 – Verarbeitungstätigkeit	Sm – Erheben	Nv	Verarbeitungstätigkeit „**Terminvereinbarung per Telefonat**" für Termin- und Kommunikationsdaten MUSS die Speicherung in getrennten Speicherbereichen regeln und eine automatische Profilbildung aus Terminhistorie und weiteren Kommunikationsdaten verhindern.	[E1][Sm][Nv][TRENNUNG] [PROFILBILDUNG] [TERMIN]	MUSS, weil aus Termin- und Kommunikationsmustern leicht Profile entstehen können; nur verbindliche Trennung und Verknüpfungsbegrenzung gewährleisten Nichtverkettung.	Weitgehend erfüllt, wenn Termindaten im Kalendersystem und sonstige Telefon-Metadaten technisch/organisatorisch getrennt verarbeitet und nicht automatisch zu Profilen zusammengeführt werden.
E1 – Verarbeitungstätigkeit	Sm – Erheben	Iv	Verarbeitungstätigkeit „**Terminvereinbarung per Telefonat**" für Termindaten MUSS eine Widerspruchsmöglichkeit vor weiterer Verarbeitung sowie einen Prozess zur nachträglichen Änderung oder Löschung vereinbarter Termine auf Wunsch der betroffenen	[E1][Sm][Iv] [WIDERSPRUCH] [TERMINÄNDERUNG] [LÖSCHPROZESS]	MUSS, weil Betroffene ihre Rechte (Widerruf, Berichtigung, Löschung) bzgl. Termindaten effektiv wahrnehmen können müssen und dies verbindliche Prozesse erfordert.	Weitgehend erfüllt, sofern Anrufende problemlos Änderungen/Stornierungen geltend machen können und ein dokumentierter Prozess zur Anpassung/Löschung der Termindaten existiert.

Example output result of an evaluation using a sentence template

If an AI uses such sentence templates and a well-maintained database with a processing directory, TOM catalogue and risk register, it can automatically fill in large parts of a DPIA report. This shifts the role of the data protection officer more towards technical review, assessment of residual risks and approval of the final DPIA. At the same time, it becomes possible to formulate reports in a manner appropriate to the target audience, for example in a more condensed, riskoriented language for management or in a technically detailed presentation for IT. AI can help **to translate the legal and technical requirements into concrete, target group-oriented instructions** without diluting the core content of the DPIA.

10. Conclusion: SDM 3.1 as a key tool for the DPIA in the AI context

Advancing digitalisation and the increasing use of AI systems, particularly in healthcare, are increasing the pressure to carry out DPIA efficiently, transparently and in a legally compliant manner. The Standard Data Protection Model (SDM) 3.1 is proving to be a key tool for translating the requirements of the GDPR into assurance objectives, deriving consistent TOM setups, systematically identifying and assessing risks, and structuring documentation in such a way that it can be processed by both humans and AI.

For data protection officers, this means that TOM documentation and DPIA are moving closer together methodologically. AI can prepare and standardise large parts of the documentation work, while the role of the DPO shifts more towards qualitative assessment and control. Particularly when AI is used in healthcare – as in the example of the voice assistant – it is clear that SDM helps to understand innovation and data protection not as opposites, but as compatible goals. Clear, structured and verifiable documentation strengthens patient rights, supports supervisory authorities in their audits and enables those responsible to account for their decisions.

At the same time, it remains clear that **the actual complexity** of a DPIA **does** not **arise** from the SDM or the GDPR, but **from the processing** itself. The GDPR, in particular Articles 5, 25, 32 and 35, sets out the material standards, and the respective specialist processes entail their own specific risks and protection requirements. In this context, the SDM is 'only' a method – a structured framework that helps to systematically record and review these requirements and translate them into appropriate TOM. It does not replace a legal review and does not create any additional requirements, but rather makes the existing specifications visible, comprehensible and auditable.

AI is also not a decision-maker, but remains a support tool. It is used for consistency checks, identifying gaps, creating and standardising texts, and structuring complex information. Legal assessment, risk decisions and the selection of appropriate measures remain human tasks. In the future, it is conceivable that automation – for example, via MCP or API connections – will read technical information directly from systems and feed it into structured DPIA processes. This could lead to TOM catalogues, processing directories or system logs being automatically updated and integrated into DPIA modules. However, this does not change the basic principles: **the requirements come from the law, the risks from the specific processing, the SDM provides the structure, and AI supports the preparation, not the decision.**

SDM 3.1 is the methodological basis that enables AI systems to create DPIA documentation and risk assessments in a structured, consistent and verifiable manner. This allows even complex processing operations to be designed in a manner that is compliant with data protection regulations, trustworthy and transparent.

Data protection officers are transitioning from document hunters and gatherers to strategic risk managers and evaluators of complex systems.

--

Thomas Werning has been working in the field of data protection, internet marketing, and digitalization for over 25 years. He is the managing director of werning.com GmbH and MoeWe Datenschutz GmbH. For him, data protection is also about treating other people's data with respect and digital responsibility within companies.

He is a founding member of UGSDM e.V. and a board member of the Professional Association of External Data Protection Officers (FED e.V.).

Sources and further information:

1. User Group Standard Data Protection Model: www.ugsdm.de

2. Einstiegshilfe in die Methode des Standard-Datenschutzmodell (SDM) https://www.werning.com/artikel/einstiegshilfe-in-die-methode-des-standard-datenschutzmodell-sdm/

3. Art. 35 GDPR – Data protection impact assessment, available at: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679

4. Data Protection Conference (DSK): Brief paper No. 5 – 'The data protection impact assessment pursuant to Article 35 GDPR', version dated 17 October 2017.

5. Standard Data Protection Model – SDM Version 3.1: 'Standard Data Protection Model – A method for data protection consulting and auditing based on uniform guarantee objectives', published by the Conference of Independent Data Protection Supervisory Authorities of the Federal Government and the Länder.

6. Federal Commissioner for Data Protection and Freedom of Information (BfDI): 'FAQ on Data Protection Impact Assessment', available online at: https://www.bfdi.bund.de

7. BSI: 'IT-Grundschutz Compendium', Federal Office for Information Security, current edition (e.g. Edition 2023).

8. European Data Protection Board (EDPB): Guidelines 4/2019 on Data Protection Impact Assessment (DPIA), version 2.0, adopted on 10 October 2019.

9. Data Protection Conference (DSK): Guidance on AI and Data Protection, Version 1.0 dated 20 December 2023.

10. GDD e.V. – Society for Data Protection and Data Security: 'Practical Guide to DPIA', 2022 edition.

11. Bavarian State Office for Data Protection Supervision (BayLDA): 'AI in Healthcare – Data Protection Requirements', information sheet 2023.

12. Schrems II – ECJ, judgment of 16 July 2020, C-311/18, 'Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems'.

13. European Commission: EU-US Data Privacy Framework – Adequacy Decision of 10 July 2023, available at: https://commission.europa.eu

14. OpenAI: Data Processing Agreement (DPA), documentation on GDPR-compliant use via the API (as of 2024).

15. Bitkom: Guide 'Artificial Intelligence and Data Protection – Recommendations for Action for Companies', version 2023.