Annex 1

Questionnaire according to section 4 para. 6 of the DiGAV

In this questionnaire, the manufacturer has to declare the fulfilment of the requirements as set out in section 4. The manufacturer confirms the fulfilment of the requirements by checking the column "applicable". The terms regarding Data Protection as well as Data Security - Basic Requirements have to be met by all digital health treatments. The requirements Data Security - Additional Requirements for Digital Health Applications demanding a very high level of protection, have to be met by any Digital Health Application that was identified through the analyses of the necessary level of data protection as requiring a very high level of protection.

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
Data Protection					
1.	General Data Protection Regulation as applicable law	The processing of personal data by means of the Digital Health Application and their respective manufacturers is subject to the Regulation (EU) 2016/679 as well as (if applicable) further data protection provisions.			
2.	Consent	Is prior to the processing of personal and related data a freely given, specific and informed consent of the respective data subject according to the purposes designated in section 4 para. 2 of the data processing obtained?			Consent is not obtained, as the purpose of the processing results from a Digital Health Application manufacturer`s legal obligation.
3.	Consent	Is the giving of consent and declarations by the data subject always explicit, i.e. through an active, unambiguous action by the data subject?			Consent is not obtained, as the purpose of the processing results from a Digital Health Application manufacturer`s legal obligation.
4.	Consent	Can the data subject withdraw the prior given consent easily, barrier-free, at any time and in an easy-to -understand way with effect to the future?			Consent is not obtained, as the purpose of the processing results from a Digital Health Application manufacturer`s legal obligation.
5.	Consent	Is the data subject prior to giving consent informed about the right and possibility to withdraw the given consent at any time?			Consent is not obtained, as the purpose of the processing results from a Digital Health Application manufacturer`s legal obligation.
6.	Consent	Before giving consent, has the data subject been informed in a clear, comprehensible, user-friendly and appropriate manner for the target group, which categories of data are processed for which purposes by the Digital Health Application or the Digital Health Application manufacturer?			Consent is not obtained, as the purpose of the processing results from a Digital Health Application manufacturer`s legal obligation.

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
7.	Consent	Can the data subject access the texts of the given consents and declarations at any time from the Digital Health Application or from a source referenced from the Digital Health Application?			Consent is not obtained, as the purpose of the processing results from a Digital Health Application manufacturer`s legal obligation.
8.	Purpose limitation	Is the processing of personal data by the Digital Health Application conducted exclusively for the purposes mentioned in section 4 para. 2 sentence 1 or based on other statutory data processing justifications pursuant to section 4 para. 3?			
9.	Data minimization and Adequacy	Are the personal data processed through the Digital Health Application adequate for the purpose and limited to what is necessary for the purposes of the processing?			
10.	Data minimization and Adequacy	Has the Digital Health Application manufacturer ensured that the purposes of the processing of personal data by the Digital Health Application cannot be achieved adequately through other, more data-efficient [meaning with less data] means to the same extent?			
11.	Data minimization and Adequacy	Are health-related data stored strictly separately from data exclusively required for the accounting of services?			
12.	Data minimization and Adequacy	Does the manufacturer of the Digital Health Application ensure that staff entrusted with non-product-related tasks do not have access to health-related data?			
13.	Data minimization and Adequacy	Unless the use of the Digital Health Application is limited to a private IT system of the user the following questions arise: ▪ Were respective usage scenarios explicitly considered in the Data Protection Impact Assessment? ▪ Is the insurance holder expressly informed that the use of the Digital Health Application in a potentially unsafe environment might possibly be associated with security risks that cannot be fully addressed by the Digital Health Application manufacturer? ▪ If the Digital Health Application is used on an IT system not only used by the insurance holder, is the - even temporary - storage of health-related data on this IT system entirely prevented? ▪ Are data, which are filed and recorded locally on the IT system, deleted after the end of the user-session - even if the user has not explicitly terminated the session? (e.g. by shutting down the IT system?)			The usage of the Digital Health Application is limited to a private IT system of the user.

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
14.	Integrity and Confidentiality	Does the Digital Health Application provide adequate technical and organizational measures to protect personal data against accidental or unlawful destruction, deletion, alteration, disclosure or illegitimate forms of processing?			
15.	Integrity and Confidentiality	Is the exchange of data between the terminal device of the data subject and external systems controlled by the Digital Health Application consistently encrypted according to the state of the art?			No personal data are exchanged between the terminal of the data subject and external systems.
16.	Accuracy	Does the Digital Health Application provide technical and organizational measures to ensure that personal data processed through the Digital Health Application are accurate and up to date?			
17.	Accuracy	Does the manufacturer undertake all reasonable measures to ensure that personal data that are inaccurate in relation to the purposes for which they are processed are erased or rectified immediately?			
18.	Necessity	Will the personal data collected through the Digital Health Application be stored only as long as it is absolutely necessary for the fulfilment of the promised functionalities of the Digital Health Application or for other purposes directly resulting from legal obligations?			
19.	Necessity	Are personal data not stored after the purposes according to section 4 para. 2 sentence 1 to 4 have been fulfilled?			The purposes of storage and the maximum storage period shall be separately justified by the manufacturer, stating the reasons why these purposes legitimize the further storage of personal data.
20.	Data Portability	Does the Digital Health Application manufacturer provide mechanisms by which the data subject can exercise the right to data portability from within the Digital Health Application and retrieve in an appropriate format the personal data concerning him/her provided by the data subject to the Digital Health Application or transfer it to another Digital Health Application?			
21.	Information Obligation	Is the privacy statement of the Digital Health Application easy to find, accessible and freely viewable via the application website?			

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
22.	Information Obligation [Information to be provided]	Does the Digital Health Application`s privacy notice contain all relevant information on the manufacturer and its data protection officer, on the purpose of the Digital Health Application, on the categories of data processed for this purpose, on the manufacturer's handling of this data, on the right to withdraw prior given consent, on the possibilities for exercising the data subject's rights at any time, and does the manufacturer of the Digital Health Application adequately implement any additional information obligations arising from Articles 13 and 14 of the Regulation (EU) 2016/679?			
23.	Information Obligation [Information to be provided]	Once the Digital Health Application is installed, is the Digital Health Application privacy notice easy to find from within the Digital Health Application or within the Digital Health Application?			
24.	Information Obligation [Information to be provided]	Can the data subject obtain access from the manufacturer of the Digital Health Application to the personal data stored about him or her to the extent specified in Article 15 of the Regulation (EU) 2016/679?			
25.	Information Obligation [Information to be provided]	Does the privacy notice of the Digital Health Application contain a transparent erasure concept that regulates the procedure for the withdrawal of consent and uninstallation of the Digital Health Application, as well as the handling of claims for the erasure of data and for the restriction of its processing and meets the requirements of Articles 17 to 19 of the Regulation (EU) 2016/679?			
26.	Information Obligation [Information to be provided]	Is the data subject entitled to request the Digital Health Application manufacturer to rectify inaccurate personal data concerning him or her and to complete incomplete personal data concerning him or her?			
27.	Information Obligation [Information to be provided]	Is the data subject informed before the deletion of the user account of any data that may be lost as a result and of the right to data portability pursuant to Article 20 of the Regulation (EU) 2016/679?			

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
28.	Data Protection Management	Has the Digital Health Application manufacturer implemented a procedure for regular review, assessment and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing, covering all systems and processes used in connection with the Digital Health Application?			
29.	Data Protection Management	Has the manufacturer of the Digital Health Application imposed confidentiality obligations on all persons who have access to personal data as a result of their activities?			
30.	Data Protection Impact Assessment and Risk Management	Has the manufacturer of the Digital Health Application for the Digital Health Application carried out a Data Protection Impact Assessment and transferred the risk analysis carried out in the process into the documented processes of risk management, according to which a continuous re-evaluation of threats and risks takes place?			
31.	Data Protection Impact Assessment and Risk Management	Does the manufacturer of the Digital Health Application ensure that personal data breaches are reported to the regulatory authority within 72 hours of the breach becoming known to him?			
32.	Data Protection Impact Assessment and Risk Management	Does the manufacturer of the Digital Health Application implement the requirements of Article 34 of the Regulation (EU) 2016/679 in order to notify data subjects in case of any data breaches?			
33.	Documentation Obligation	Has the manufacturer documented the data protection guidelines applicable to the company and trained its employees in their implementation?			
34.	Documentation Obligation	Does the manufacturer of the Digital Health Application implement measures to ensure that it is possible to subsequently check and establish whether and by whom personal data have been entered, modified or erased?			
35.	Documentation Obligation	Can the manufacturer of the Digital Health Application prove at any time that the required consent of the data subject was given for the processing of personal data to be carried out, unless the data processing is carried out on another legal basis?			

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
36.	Processing by Processors	Is personal data not disclosed by the Digital Health Application or the manufacturer of the Digital Health Application to third parties at all or only to processors who have sufficient trustworthiness and liability, implement appropriate mechanisms to protect transferred data and have a binding contractual relationship with the manufacturer which precludes any reduction in the promises made to the insurance holder?			
37.	Data Transfer to Third Parties	Is no personal data relating to the Digital Health Application or the manufacturer of the Digital Health Application passed on to third parties, unless this is directly necessary for the fulfilment of purposes under section 4 para. 2 sentence 1 No. 1, or for compliance with statutory provisions and is limited to these purposes?			
38.	Data Processing abroad	Is the processing of health data and personally identifiable stock and traffic data carried out exclusively in Germany, in another Member State of the European Union, in a state treated as equivalent to that Member State under section 35 para. 7 SGB I, or on the basis of an adequacy finding under Article 45 of the Regulation (EU) 2016/679?			
39.	Further Protection Goals	Is it technically impossible to chain personal data across two or more Digital Health Applications, or does a chain of data across two or more Digital Health Applications require explicit, separately obtained, informed consent of the data subject?			The Digital Health Application does not provide a technical means of linking or exchanging data with other Digital Health Applications.
40.	Further Protection Goals	Is it guaranteed that a disclosure of information of the data subject or about the data subject to the public or to a group of persons, that cannot be defined by the data subject, does not occur at all or only as a result of an explicit, proactive act of the data subject, based on information appropriate to the target group about the nature of the information disclosed and the possible circle of recipients?			The Digital Health Application does not support the disclosure of information of or about the data subject to the public or to a group of people that cannot be defined by the data subject.

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
Data Security					
Basic/Standard requirements that apply to all Digital Health Applications					
1.	Information Security and Service Management	Has the manufacturer of the Digital Health Application implemented an information security management system (ISMS) in accordance to ISO 27000 series or BSI standard 200-2 or a comparable system and can present a corresponding recognized certificate or comparable proof at the request of the Federal Institute for Drugs and Medical Devices?			The application day is prior to 1. January 2022
2.	Information Security and Service Management	Does the manufacturer of the Digital Health Application have a structured analysis of the protection requirements under consideration of the damage scenarios, such as "violation of laws/regulations/contracts", "violation of the right of informational self-determination", "violation of personal integrity", "impairment of the performance of tasks" and "negative internal or external effects", whereby the results indicate a normal, high or very high protection requirement for the Digital Health Application according to the definition of the BSI standard 200-2, and can the manufacturer, at the request of the Federal Institute for Drugs and Drug Addiction, provide such analysis of the protection requirements?			
3.	Information Security and Service Management	Has the manufacturer of the Digital Health Application implemented and documented release, change and configuration management processes, taking into account the requirements of Regulation (EU) 2017/745, which ensure that extensions and adaptations of the Digital Health Application developed by itself or on its behalf have been sufficiently tested and explicitly released before going in production?			
4.	Prevention of Data Leaks/Breaches	Has the Digital Health Application manufacturer ensured that the communication of the Digital Health Application with other services is technically limited to such extent that no unintended data communication [through which personal data is likely to be transferred] can take place while using the Digital Health Application?			

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
5.	Prevention of Data Leaks/Breaches	Is at least transport encryption in accordance with the BSI's minimum standard for the use of Transport Layer Security (TLS) pursuant to Section 8 para. 1 sentence 1 of BSI Act used for all data communication between different system components of the Digital Health Application taking place via open networks?			The Digital Health Application does not trigger data communication over open networks.
6.	Prevention of Data Leaks/Breaches	Does the Digital Health Application verify the authenticity of the accessed services each time the internet accessible functions of the Digital Health Application are used, before personal data are exchanged within these services?			The Digital Health Application does not include any functionality accessible via the internet.
7.	Prevention of Data Leaks/Breaches	Has the Digital Health Application manufacturer ensured that the Digital Health Application does not generate unwanted log or help files?			
8.	Prevention of Data Leaks/Breaches	Has the Digital Health Application manufacturer ensured that the Digital Health Application does not generate error messages that may reveal confidential information?			
9.	Authentication	Before accessing the Digital Health Application, do all persons using the Digital Health Application have to authenticate themselves using a method appropriate according to the protection requirements of the respective data processed by the Digital Health Application?			
10.	Authentication	Are appropriate technical measures in place to ensure that data used to authenticate a person using the Digital Health Application are never exchanged over insecure transportation channels?			
11.	Authentication	Does the Digital Health Application use or include a central authentication component [implemented with established standard components], which is solely permissible for initial authentication and whose trustworthiness can be verified by services of the Digital Health Application?			
12.	Authentication	Does the Digital Health Application require that a person using the Digital Health Application can only change the data used for his or her authentication if sufficient information is provided to verify the authenticity of that person?			

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
13.	Authentication	Where authentication takes place using a password: ▪ Does the Digital Health Application force all individuals using the Digital Health Application to use strong passwords according to a password policy that includes a minimum password length and limits failed login attempts to a certain number? ▪ Is it guaranteed that passwords are never transmitted or stored in plain text? ▪ Is the changing or resetting of passwords being logged and is the person concerned - if suitable contact data is available - immediately informed about the resetting or changing of the password?			Authentication does not take place using a password.
14.	Authentication	Where the Digital Health Application stores authentication data on a terminal device or in a software component located on such terminal device: Is the explicit consent of the person using the Digital Health Application requested ("opt-in") and is this person informed of the risks of the function?			The Digital Health Application does not store authentication data on a terminal device or software component on such terminal device.
15.	Authentication	Where information about the identity or authenticity of the person using the Digital Health Application or the authenticity of the Digital Health Application components is shared between Digital Health Application components via dedicated sessions ("sessions"): ▪ Is all session data, both in flight and at rest, protected by technical measures appropriate to the security requirements of the Digital Health Application and is it guaranteed that any session IDs used are chosen randomly, with sufficient entropy and through established procedures? ▪ Are all sessions established in a single instance of a Digital Health Application invalidated with the termination or suspension of use of the Digital Health Application, and can the person using the Digital Health Application also force the explicit invalidation of a session? ▪ Do sessions have a maximum validity period and are inactive sessions automatically invalidated after a certain time? ▪ Does the invalidation of a session result in the deletion of all session data and is it guaranteed that a session, once invalid, cannot be reactivated even if individual session data is known?			The Digital Health Application does not use sessions.

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
16.	Access Control	Does the Digital Health Application ensure that any access to protected data and functions is subject to a credential verification process ("complete mediation"), which ensures, in case of access by the operational staff of the Digital Health Application manufacturer, a dedicated authorization component is used for all protected data ("reference monitor" or "secure node/application"), which requires prior secure authentication of the accessing person?			
17.	Access Control	Are all permissions assigned restrictively initially and by default, and can permissions only be widened by controlled processes, which include effective checks and control mechanisms with redundant supervision for changing the permissions of operational staff of the manufacturer of a Digital Health Application?			
18.	Access Control	Where the Digital Health Application provides for different user roles: Can each role only access functions of the Digital Health Application with the rights necessary to perform the functions associated with that role?			The Digital Health Application does not provide for different user roles.
19.	Access Control	Does the manufacturer of the Digital Health Application ensure that access to functions of the Digital Health Application as well as data by the manufacturer's operational staff is only possible via secure networks and access points?			
20.	Access Control	Do all access control errors and malfunctions result in a denial of access?			
21.	Integration of Data and Functions	Can the insured holder move exclusively within the Digital Health Application's trust domain or can only trustworthy external content verified by the Digital Health Application manufacturer be used from within the Digital Health Application and, in this case, is the insured person informed when the Digital Health Application's trust domain is left?			
22.	Integration of Data and Functions	Where the Digital Health Application allows the user to upload files: Is this function restricted as much as possible (e.g. exclusion of active content), does a security check of the content take place and is it guaranteed that files can only be stored in the predefined path?			The Digital Health Application does not allow the upload of files.

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
23.	Logging	Does the Digital Health Application perform complete, traceable, tamper-proof logging of all security-related events - i.e. the secure identification, authentication and authorization of persons and organizations?			
24.	Logging	Is logging data automatically evaluated in order to detect or proactively prevent security-relevant incidents?			
25.	Logging	Is access to logging data secured by appropriate permission management and restricted to a few authorized persons and defined purposes?			
26.	Frequent and secure updating	Does the manufacturer inform the data subject (e.g. via push mechanisms or before the launch of the Digital Health Application) when a security-related update of the Digital Health Application has been made available for installation?			
27.	Secure De-Installation	If the Digital Health Application is uninstalled, will all data and files - including caches and temporary files - stored on IT systems in the data subject's possession and created by the Digital Health Application be deleted?			The Digital Health Application is a web-based application only.
28.	Hardening	Where services of the Digital Health Application are accessible via web protocols: ▪ Are unnecessary methods of the used protocols deactivated for all services that can be accessed via open networks? ▪ Are the permitted character encodings restricted as much as possible? ▪ Are limits on access attempts in place for all services accessible via open networks? ▪ Is it guaranteed that no security-relevant comments or product and version information are disclosed? ▪ Are unnecessary data deleted regularly? ▪ Is it guaranteed that these services are not indexed by search engines? ▪ Are absolute local paths always avoided? ▪ Is a retrieval of source codes precluded?			The Digital Health Application does not include any web protocol accessible services.

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
29.	Hardening	Where the Digital Health Application processes data that are provided by the user or sources not controlled by the Digital Health Application: ▪ Is such data considered potentially harmful and validated and filtered accordingly? ▪ Is the verification of such data performed on a trustworthy IT system? ▪ Is incorrect input (if possible) not handled automatically, or are corresponding functionalities implemented to prevent misuse? ▪ Is such data encoded in a form that ensures that the malicious code is not interpreted or executed? ▪ Is such data separated from concrete requests to data-retaining systems (e.g. via stored procedures) or are data requests explicitly secured against attack vectors favored by such data?			The Digital Health Application does not process data that is generated by the user or by sources not controlled by the Digital Health Application.
30.	Hardening	Is consistently ensured that errors in the Digital Health Application are handled and lead to the termination and, if necessary, rollback of the initiated functions?			
31.	Hardening	Is the Digital Health Application protected from automated access by appropriate protection mechanisms, if such does not realize intended usage possibilities of the Digital Health Application?			
32.	Hardening	Are configuration files relevant for the secure operation of the Digital Health Application protected against loss and tampering by appropriate technical measures?			The Digital Health Application does not use configuration files respectively those are not relevant for the secure operation of the Digital Health Application.

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
33.	Use of Sensors and External Devices	Where the Digital Health Application directly accesses sensors of a mobile device and/or external hardware (e.g. near-body sensors): ▪ Did the manufacturer of the Digital Health Application determine under which general conditions sensors or connected devices can be installed, activated, configured and used and is the compliance with these general conditions ensured as far as possible before executing such corresponding functionalities? ▪ Does the Digital Health Application ensure that sensors and connected devices are set to their default configuration during installation or initial activation for the Digital Health Application that complies with a documented security policy? ▪ Can the insurance holder use the Digital Health Application to directly reset sensors and devices to a default configuration that complies with a documented security policy? ▪ Is the exchange of data between the Digital Health Application and directly controlled sensors or devices only possible after the installation and configuration of the sensors or devices is complete?			The Digital Health Application neither accesses sensors of a mobile device nor external hardware.
34.	Use of Sensors and External Devices	Where the Digital Health Application exchanges data with external hardware (e.g. body sensors): ▪ Are the procedures for installing, configuring, activating and deactivating this hardware described in a manner appropriate to the target group and, as far as possible, secured against operating errors? ▪ Is there mutual authentication between the Digital Health Application and external hardware? ▪ Is data exchanged between the Digital Health Application and external hardware only in encrypted form after an initial handshake? ▪ Is it guaranteed that all data stored on external hardware will be deleted when the Digital Health Application is uninstalled or when it is no longer used? ▪ Has the Digital Health Application manufacturer documented how to securely deactivate the connected hardware without data loss or sensitive data remaining on the device?			The Digital Health Application does not exchange data with external hardware.

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
35.	Use of Third-Party-Software	Does the manufacturer maintain a complete list of all libraries and other software products used in the Digital Health Application that have not been developed by the Digital Health Application manufacturer itself?			
36.	Use of Third-Party-Software	Does the manufacturer ensure, by means of suitable methods of market observation, that previously unknown risks to data protection, data security or patient safety arising from these libraries or products are promptly identified?			
37.	Use of Third-Party-Software	Has the manufacturer established procedures to be able to implement appropriate measures such as blocking the app and notifying users immediately in the event of such identified risks?			
Additional requirements for Digital Health Applications with very high protection demands					
1.	Encryption of Stored Data	Are personal data - processed on IT systems that are not at the personal disposal of the user - only stored encrypted on these systems?			
2.	Penetration Test	Has the producer of the Digital Health Application carried out a penetration-test for the version of the Digital Health Application (including all backend components) to be included in the register pursuant to section 139e para.1 SGB V, that takes common attack vectors such as clickjacking or cross-site-request-forgery into account?			
3.	Penetration Test	Has the manufacturer of the Digital Health Application documented the results of the conducted penetration-tests, the results of the implementation of the measures or recommendations and, if necessary, transferred them to suitable management systems?			
4.	Authentication	Is two-factor authentication enforced at least for the initial authentication of all persons using the Digital Health Application?			
5.	Authentication	If the Digital Health Application allows a fallback option to One-factor authentication: ▪ Is the person using the Digital Health Application made aware of the risks involved and is such fallback activated only after the consent of the user has been confirmed by an active action? ▪ Is the person using the Digital Health Application able to deactivate this fallback option at any time from within the Digital Health Application?			The Digital Health Application does not allow a fallback option to One-factor authentication.

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
6.	Authentication	Will the Digital Health Application be able to support authentication of persons with statutory health insurance as the persons using the Digital Health Application via an electronic health card with contactless interface by 31 December 2020 at the latest?			
7.	Authentication	Where the Digital Health Application provides a user role for healthcare providers: Can the Digital Health Application support, by 31 December 2020 at the latest, authentication of healthcare providers as the persons using the Digital Health Application via an electronic health professional card with a contactless interface?			The Digital Health Application is not intended for use by healthcare providers.
8.	Measures against DoS and DDoS	Are messages (XML, JSON, etc.) and data sent to Digital Health Application services accessible via open networks audited against defined schemes?			The Digital Health Application does not exchange data with or between services accessible via open networks.
9.	Embedded Web Server	If components belonging to the Digital Health Application use web servers e.g. for administration or configuration: ▪ Is the web server configured as restrictively as possible? ▪ Are only the required components and functions of the web server installed or activated? ▪ If possible, is the web server not hosted under a privileged account? ▪ Are security-relevant events recorded? ▪ Is the access only after authentication possible? ▪ Is any communication with the web server encrypted?			The Digital Health Application does not use a web server.

Annex 2

Questionnaire regarding sections 5 and 6

In the following questionnaire, the manufacturer has to declare the fulfilment of the requirements according to sections 5 and 6. The manufacturer shall confirm the fulfilment of the requirements by checking the column "applicable" or, if the below stated justification is applicable, by checking the column "not Applicable".

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
Interoperability					
Is the insurance holder able to export all data processed by the Digital Health Application in an interoperable format from the Digital Health Application?					
1.	Section 5 para. 1 and section 6	Yes, the data processed via the Digital Health Application can be exported from the Digital Health Application in an interoperable format by the insurance holder from 1 January 2021 at the latest and made available to the insurance holder for further use. The export is carried out according to a specification of contents of the electronic patient file according to section 291b para. 1 sentence 7 SGB V or in a format (syntax, semantics) recommended in the Vesta directory of gematik[2], provided that suitable specifications have already been available for at least one year at the time of application. If this is not the case, the export will be carried out in an open recognized international standard or in a profile disclosed by the manufacturer above an open recognized international standard or above a standard registered in the Vesta directory. If an open recognized international standard or a disclosed profile above an open recognized international standard or above a standard registered in the Vesta directory is used, the manufacturer has applied for the inclusion of the standard or profile in the Vesta directory.			

[2] The German company for telematics applications of the health card (*Deutsche Gesellschaft für Telematikanwendungen der Gesundheitskarte*) is referred to as "**gematik**".

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
Can the insurance holder export the data processed via the Digital Health Application from the Digital Health Application in a form usable for care?					
2.	Section 5 para. 1 and section 6	Yes, the insurance holder can export relevant extracts of the health data processed via the Digital Health Application, in particular on therapy courses, therapy planning, therapy results and data evaluations carried out, from the Digital Health Application for his or her care from 1 January 2021 at the latest. The export shall be in a human-readable and printable format and shall take into account the care context in which the Digital Health Application is typically used in accordance with its intended purpose.			
Does the Digital Health Application have standardized interfaces to personal medical devices?					
3.	Section 5 para. 1 and section 6	Yes, the Digital Health Application is capable of capturing data from medical devices used by the insured or sensors worn by the insured for the measurement and transmission of vital signs (wearables), and for this purpose supports a disclosed and documented profile of the ISO/IEEE 11073 standard or another disclosed and documented interface (syntax, semantics), which is either listed in the Vesta directory or for which a corresponding application has been submitted by the manufacturer, no later than 1 January 2021.			Within the scope of the intended use of the Digital Health Application, it is not intended that the Digital Health Application exchanges data with medical devices used by the insured or with sensors worn by the insured for measuring and transmitting vital signs (wearables).
Are the standards and profiles used to achieve interoperability of the Digital Health Application published and can be used without discrimination?					
4.	Section 5 para. 1 and section 6	Yes, the standards and profiles used to achieve interoperability of the Digital Health Application are published or linked on the application website and can be used without discrimination and implemented by third parties in their systems.			

Hot Topics

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
Resilience					
Is the Digital Health Application resilient to malfunctions and misuse?					
1.	Section 5 para. 2	Yes, a sudden power failure does not lead to a loss of data.			
2.	Section 5 para- 2	Yes, a sudden failure of the internet connection does not lead to a loss of data.			
3.	Section 5 para. 2	Yes, the Digital Health Application checks/validates the plausibility of measurements, inputs and other data from external sources.			The Digital Health Application is not capable of collecting data from medical devices or sensors or other external sources, nor does it foresee the input of data.
4.	Section 5 para. 2	Yes, the Digital Health Application includes functions for testing and/or calibration of connected medical devices and sensors.			The Digital Health Application is not able to collect data from medical devices or sensors.
Consumer protection					
Does the user of the Digital Health Application receive all the information necessary to decide whether to use such application before committing to any obligations towards the manufacturer or any third person?					
1.	Section 5 para. 3	Yes, in the information regarding the Digital Health Application on the sales platform or on the application website, the functional scope is comprehensively described and the medical purpose is displayed to the full extent.			
2.	Section 5 para. 3	Yes, the Digital Health Application information on the sales platform or on the application website clearly indicates which features are available with the download or the use of the application and which features can or must be purchased at what price, e.g., as in-app purchases or forwarding of functions.			
Is the compatibility of the Digital Health Application with systems and devices communicated transparently?					
3.	Section 5 para. 3	Yes, the Digital Health Application manufacturer will publish on the application website a list of compatibility commitments regarding operating system versions and mobile devices, web browsers and web browser versions, and other required or optional devices, and will keep this list updated.			
Does the manufacturer publish the medical purpose of the Digital Health Application?					
4.	Section 5 para. 3	Yes, the medical purpose according to Article 2 No. 12 of Regulation (EU) 2017/745 or section 3 No. 10 of the Medical Devices Act in the version valid up to and including 25 May 2020 is published in the imprint of the Digital Health Application.	4.		

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
Are the conditions of use of the Digital Health Application designed to be consumer-friendly?					
5.	Section 5 para. 4	Yes, the Digital Health Application is ad-free.			
6.	Section 5 para. 3	Yes, the Digital Health Application does not contain non-transparent offers such as automatically renewing subscriptions or time-limited special offers.			
7.	Section 5 para. 3	Yes, the Digital Health Application includes measures to protect against accidental In-App purchases or does not offer In App purchases at all.			
Does the manufacturer of the Digital Health Application implement measures to support users?					
8.	Section 5 para. 5	Yes, the manufacturer provides a free German-language support service to assist users with the operation of the Digital Health Application, which answers user queries within 24 hours at the latest.			
Usability and Accessibility					
Is the Digital Health Application simple and intuitive to use?					
1.	Section 5 para. 5	Yes, the usability style guides of the respective platform for mobile applications have been fully implemented, or alternative solutions have been implemented for which user tests have shown a particularly high degree of user-friendliness.			The Digital Health Application is not offered via a platform for mobile applications.
2.	Section 5 para. 5	Yes, the ease and intuitive usability of the Digital Health Application was confirmed in tests with focus groups representing the target group.			
3.	Section 5 para. 6	Yes, from 1 January 2021 at the latest, the Digital Health Application will provide operating aids for people with disabilities or support the operating aids offered by the platform.			

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
Support for Service Providers					
Does the Digital Health Application inform and support medical practitioners and other healthcare providers involved in its use?					
1.	Section 5 para. 7	Yes, the manufacturer of the Digital Health Application provides information for integrated service providers in which the supplementary use of the app by a service provider and the underlying roles for service provider and patient are clearly described.			No involvement of service providers is envisaged for the use of the Digital Health Application.
2.	Section 5 para. 7	Yes, the manufacturer of the Digital Health Application provides information for integrated service providers describing how to explain the use of the Digital Health Application to the insured in the context of therapy.			No involvement of service providers is envisaged for the use of the Digital Health Application.
3.	Section 5 para. 7	Yes, the user can activate his own data access for healthcare providers to be included or transmit data in a secure manner to service providers.			No involvement of healthcare providers is envisaged for the use of the Digital Health Application.
Quality of Medical Content					
Is the Digital Health Application based on secure medical knowledge and does it make it transparent?					
1.	Section 5 para. 8	Yes, the medical content and procedures implemented in the Digital Health Application are based on the commonly recognized professional standard.			
2.	Section 5 para. 8	Yes, the manufacturer has established appropriate processes to keep the medical content and procedures implemented in the Digital Health Application up-to-date.			
3.	Section 5 para. 8	Yes, the sources for the medical content and procedures implemented in the Digital Health Application, such as guidelines, textbooks and studies, are published and referenced in the Digital Health Application or on a website linked from the Digital Health Application.			
4.	Section 5 para. 8	Yes, the studies conducted using the Digital Health Application are published and named in the Digital Health Application or on a website linked from the Digital Health Application.			
5.	Section 5 para. 8	Yes, the health information provided in the Digital Health Application is up-to-date and based on commonly accepted professional standards.			The Digital Health Application does not provide any health information.
6.	Section 5 para. 8	Yes, the manufacturer has established appropriate processes to keep the health information provided in the Digital Health Application up-to-date.			

No.	Topic	Requirement	Applicable	Not Applicable	Legitimate Justification of "Not Applicable"
7.	Section 5 para. 8	Yes, the sources of the health information provided in the Digital Health Application are published and referenced in the Digital Health Application or on a website linked from the Digital Health Application.			The Digital Health Application does not provide any health information.
8.	Section 5 para. 8	Yes, the health information presented in the Digital Health Application is tailored to the target group.			The Digital Health Application does not provide any health information.
9.	Section 5 para. 8	Yes, the health information is provided on an individual/ad hoc basis and in the context of the respective use of the Digital Health Application.			The Digital Health Application does not provide any health information.
10.	Section 5 para. 8	Yes, in the Digital Health Application didactic methods are implemented to enhance and strengthen the health knowledge offered.			The Digital Health Application does not provide any health information.
Patient Safety					
Does the manufacturer implement appropriate measures to improve patient safety?					
1.	Section 5 para. 9	Yes, the manufacturer clearly states on the distribution platform or before the web application is launched for which users and indications the Digital Health Application is not to be used, provided there are restrictions.			
2.	Section 5 para. 9	Yes, in the Digital Health Application, the user is provided with context-sensitive information on risks and advice on appropriate measures to mitigate or avoid such.			
3.	Section 5 para. 9	Yes, in the context of critical measurements or analysis results, the Digital Health Application clearly indicates the need for or the appropriateness of consulting a doctor or another health care provider.			
4.	Section 5 para. 9	Yes, the Digital Health Application recommends the user to stop using the app or to change the use of the app when a defined state is detected.			
5.	Section 5 para. 9	Yes, for all values entered into the app by the user or collected via connected medical devices or sensors or taken from other external sources, consistency parameters are defined within the Digital Health Application, in order to verify such values before using them.			
6.	Section 5 para. 9	Yes, error alerts in the Digital Health Application are designed in a way that the user is able to understand how the malfunction occurred and how he can help to avoid it in the future.			

For further questions don't hesitate to contact our specialists:

Julia Kaufmann, LL.M.
julia.kaufmann@bakermckenzie.com

Dr. Frank Pflüger
frank.pflueger@bakermckenzie.com

Dr. Holger Lutz, LL.M
holger.lutz@bakermckenzie.com

Dr. Michaela Nebel
michaela.nebel@bakermckenzie.com

Prof. Dr. Michael Schmidl, LL.M
michael.schmidl@bakermckenzie.com

Florian Tannen
florian.tannen@bakermckenzie.coma

David Pfahler
david.pfahler@bakermckenzie.com

Baker & McKenzie - Partnerschaft von Rechtsanwälten und Steuerberatern mbB

Berlin
Friedrichstrasse 88/Unter den Linden
10117 Berlin
Tel.: +49 30 2 20 02 81 0
Fax: +49 30 2 20 02 81 199

Dusseldorf
Neuer Zollhof 2
40221 Dusseldorf
Tel.: +49 211 3 11 16 0
Fax: +49 211 3 11 16 199

Frankfurt am Main
Bethmannstrasse 50-54
60311 Frankfurt / Main
Tel.: +49 69 2 99 08 0
Fax: +49 69 2 99 08 108

Munich
Theatinerstrasse 23
80333 Munich
Tel.: +49 89 5 52 38 0
Fax: +49 89 5 52 38 199

www.bakermckenzie.com

Get Connected:

This client newsletter is prepared for information purposes only. The information contained therein should not be relied on as legal advice and should, therefore, not be regarded as a substitute for detailed legal advice in the individual case. The advice of a qualified lawyer should always be sought in such cases. In the publishing of this Newsletter, we do not accept any liability in individual cases.

Baker & McKenzie - Partnerschaft von Rechtsanwälten und Steuerberatern mbB is a professional partnership under German law with its registered office in Frankfurt/Main, registered with the Local Court of Frankfurt/Main at PR No. 1602. It is associated with Baker & McKenzie International, a Verein organized under the laws of Switzerland. Members of Baker & McKenzie International are Baker McKenzie law firms around the world. In common with terminology used in professional service organizations, reference to a "partner" means a professional who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.