Data protection compliance checklist

What is this checklist for?

This checklist is drawn up on the basis of analysis of the relevant provisions of European law. Although European law aims at harmonizing the provisions of national legislation across Europe, all analysed provisions of international and European law can be specified or limited by the national laws of the countries where the relevant medical app is developed and tested. It consists of an expanded checklist of legal requirements and their explanation in the context of mobile health apps, and incorporates a questionnaire on the national implementing legislation.

This legal compliance checklist is developed in order to:

1. help developers using the FI-STAR platform to build and test an in a way compliant with the existing legal requirements of data protection;
2. educate the developers and other parties involved the existence and content of these requirements;
3. point out the importance of seeking local legal counsel's advice on how the relevant European law is implemented by the national law.

This checklist is to be used as an information tool, in close cooperation with local legal counsel. **It is not meant as legal advice.**

Whom is the checklist for?

The checklist is meant for the teams building, testing and implementing the apps, including medical professionals, technical developers and legal advisors.

Does your app involve personal data?

Data protection law requirements apply only when 'personal data' as defined by the Data Protection Directive is processed. If your app does not involve personal data, the data protection rules do not apply. Note that although there is one EU definition of personal data, it may be applied differently across EU member states. If your country is the UK, check this helpful reference guide offered by the UK Information Commissioner's Office. A rule of thumb based on the Article 29 Working Party approach is that data is 'personal' if you or anyone else can reasonably likely single out a person (not necessarily by name) on the basis of that data, using state-of-the-art technology.

Does your app involve processing health data?

It is likely that medical or lifestyle apps process personal data related to health. To determine if your app involves processing personal data related to health in a sense of the Data Protection law, check the FI-STAR decision tree.

The law at the heart of it

- EU Data Protection Directive
- Opinions of Article 29 Working Party, an EU advisory body in the field of data protection

DATA PROTECTION CHECKLIST

1. PERSONAL DATA PROCESSED

Identify personal data[1] that is to be processed (collected, stored, analysed, transferred, deleted, etc.) by the app:

- What health data[2] is to be processed?
- What non-health data is to be processed?
- Indicate if other special categories of personal data ('sensitive personal data'), revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or regarding sex life, that are to be processed.

Does the experimentation involve processing of other categories of personal data that enjoy special protection under the national law of your country (e.g. national identification number)? If yes, specify which ones and give reference to the relevant legal provision.

2. PURPOSE SPECIFICATION

Article 6(1)(b) of the General Data Processing Directive requires that personal data must be "collected for specified, explicit and legitimate purpose." Any new purpose of data processing should be additionally specified.

For each type of personal data processed, specifically state why processing personal data is necessary: e.g. to enable functionalities of your app (e.g. to manage the user's diabetes condition you need to know the glucose intake); to install an app on the user's device, unique identifier of the device is necessary; to enable a purchase of the app, you may need a credit card number; a medical app used as a part of medical treatment may need to process health data for the purposes of treatment, and others.

Be specific enough in your purpose statement. 'Data is needed to improve our services' is not specific enough.

The purpose of processing has to be lawful.

[1] **Personal data** is "any information relating to an identified or identifiable natural person ('data subject')." (Article 2(a) Data Protection Directive)

[2] **Health data** is personal data concerning health (Article 8 Data Protection Directive).

3. DATA CONTROLLER: IDENTIFYING WHO BARES COMPLIANCE RESPONSIBILITIES

It is important to identify who (a natural person, e.g. an official, or a legal entity) acts as a so-called 'data controller.' Data controller bears most of the responsibility for compliance and violations of the data protection law.

A **data controller** is a person or entity who determines the purposes and means of the processing of personal data (Article 2(d) Data Protection Directive). In other words, controller is the one who decides if and how personal data will be processed for a particular purpose.

In contrast, **processor** does not determine if and how data will be processed, but acts on behalf of the controller (e.g. a subcontractor who merely stores the data on his servers and does nothing to the data beyond the controller's orders).

This role is to be assigned *pragmatically*, i.e. based on the factual influence. Note that more than one person or entity may act as a controller at the same time with regard to the same data, data processing operation or data processing purpose.

The fact that **an app user** consented and agreed to the terms of use before using the app, and uploaded the data himself, does not exempt the app provider from responsibility and his role as a controller. It is highly likely that an app provider is a (co-)controller and bear data protection obligations and responsibilities.

For *each purpose* identified under Step 2, identify who the controller is.

If there is more than one entity involved, pay special attention to how the decision-making and data protection responsibilities are divided among them. This can be done by way of an agreement between the two parties.

State the name and address of the organization as stated in its founding charter.

Appoint a representative of the data controller who will be in charge of data processing within the use case experimentation and whom data subjects can contact with their objections and requests: indicate his name and contact details.

4. PURPOSE LIMITATION / SECONDARY USE OF DATA

Personal data must not be further processed in a way incompatible with the original purpose(s) of collection **('the compatibility principle'**), with the only exception "for historical, statistical or scientific purposes" (Article 6 (1) of the Directive)

EU Member States understand what is compatible or incompatible differently: some strictly (purpose of collection is the only permissible the purposes of use); others more flexibly (the purpose of use is different from the purpose of collection, but is not incompatible).

In the context of the health apps, this principle is of special relevance when:

1) the app involves personal data previously collected for other purposes: existing patients' files or records on a hospital, national or regional scale; data from other apps, such as FitBit); or
2) when personal data collected by the app can be used or transferred to another system, e.g. electronic patients' records, marketing companies, other platforms of apps, etc. for purposes other than the purposes of collection.

How does the national law of your country implement this provision?

- Does the national law (and / or the practice of the national data protection authority) apply the compatibility principle strictly, or flexibly?
- Does the national law in your country provide for additional safeguards for secondary use of personal data or scientific research?
- If yes, what are those safeguards?

Does your app make use of personal data from other systems, apps, databases or platforms?

Does your app transfer personal data collected to a party or system that uses these personal data for purposes other than the purposes specified in Step 2?

If you answered 'YES' to either one of these questions, **you may be in violation of the data protection law**. Explain, with reference to the provisions of national law, how you comply with the compatible use principle.

5. PROPORTIONALITY OF DATA PROCESSING

Personal data must not be processed *excessively* in relation to the purposes of collection or further possessing (Article 6(1)(c) Data Protection Directive). This is the '**proportionality'** principle.

Among others, this means that personal data is collected, further processed and kept only in so far as it is necessary for and proportionate to the indicated purpose of processing. The standard of proportionality is stricter for health- and other sensitive data.

Personal data must be kept in an identifiable form for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Exceptions can be made by national laws for historical, statistical or scientific use.

How does the national law of your country implement these provisions? Give references to the relevant legal provisions.

Consider how processing personal identifiable data (e.g. as opposed to non-identifiable and anonymous) and health data and other sensitive data (if applicable):

a. is necessary for the purpose indicated in step 2;
b. is proportionate / not excessive in relation to the purpose indicated in step 2
c. if the same purpose can be achieved without processing personal data, or processing less data or for a shorter period of time (or storing locally on the user's device as opposed to on the cloud?).

What is the time period within which it is necessary and proportionate to keep personal data to achieve the purpose indicated in step 2?

What will happen to these data after this period expires / the purpose has been achieved? Will the data be erased or anonymised?

6. DATA QUALITY

Personal data must be "accurate and, where necessary, kept up to date; … data which are inaccurate or incomplete [for the purposes of processing] are erased or rectified." (Article 6(2)(d) Data Protection Directive)

How does the national law of your country implement this provision? Give reference to the relevant legal provision.

When answering this question, pay special attention to explaining how you ensure quality of data when:

- it is transferred to the (hospital, regional or national) electronic health records subject to special access, correction and erasure regime; or
- when it is collected by means of a questionnaire filled in by the patient;
- when it is collected/accessed via a third party, providing access to such data, or via a third party device, App or other technology.

Are there and if yes, which procedures are in place to erase and / or rectify inaccurate / not up-to-date data?

7. LEGITIMATE GROUND OF PROCESSING OF NON-SENSITIVE DATA: UNAMBIGUOUS CONSENT

All personal data may only be processed when one of the *legitimate grounds* is present (Article 7 or 8 Data Protection Directive). This is *in addition* to being processed for a lawful purpose.

Legitimate grounds for **personal data generally** are Article 7(a)-(f) of the Directive. In the context of consumer eHealth apps the ground which is most likely to be used is consent (Article 7(a) Data Protection Directive).

Data subject's consent means must be:

- freely given
- specific (among others, to the particular purpose of processing) and
- informed.
- It must be an "indication of [the data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Article 2(h) Data Protection Directive).

Some national laws require that consent is given in a particular form, e.g. written.

National laws in some Member States provide for a right to withdraw consent. In this case, withdrawing consent should be as easy as giving it.

How does the national law of your country implement these provisions? Give reference to the relevant legal provision.

Free consent

Consent is 'free' when it comes as a result of a "voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other. Any consent given under the threat of non-treatment or lower quality treatment in a medical situation cannot be considered as 'free'."[3]

In a medical context – where data is processed as a "necessary and unavoidable consequence of the medical situation", it is misleading to legitimise this processing through consent. **Consent to undergo a certain medical treatment does not equate "consent" necessary for processing health data.[4]**

Free consent means that the data subject can withdraw the consent without detriment.[5]

Specific

Consent is 'specific' when it relates to a well-defined, particular situation. A 'general agreement' to the processing does not constitute specific consent.[6]

Informed

[3] WP 131, p. 8

[4] WP 131, p. 8

[5] Article 29 Working Party. 2001. Opinion 8/2001 on the processing of personal data in the employment context" (WP 84), section 10.

[6] WP 131, p. 9

The data subject should give consent based on an understanding of the processing event(s) and their possible implications, as well as of the consequences of refusing consent. Information rights of the data subject play a key role in ensuring informed consent.[7]

It is important that the consent is given for a specific purpose of experimentation within a framework of your use case, clearly distinguishable and separate from other instances of consent, e.g. to participate in the clinical investigation.

Some national data protection authorities do not regard consent as appropriate ground of legitimate processing in the employer-employee relationship or other cases of power imbalance between a data controller and a data subject. If you intend to process employee data, it is important to verify what the national law and practice is (in addition to consulting a local legal counsel, possibly, by contacting the national data protection authority). If consent can be used for processing employee data (and data in other situations of unequal powers), under what conditions should it be done? In any case, special attention should be paid to guaranteeing that the consent is freely given, e.g. that there will be no negative consequences if a data subject refuses to consent. Free consent means that the data subject can withdraw the consent without detriment.[8]

Which ground of processing of non-sensitive data do you rely on for data processing?

How do you ensure that the consent of the data subjects (patients, their family members, medical professionals and other staff) is unambiguous, freely given, specific and informed?

[7] WP 131, p. 9

[8] Article 29 Working Party. 2001. Opinion 8/2001 on the processing of personal data in the employment context" (WP 84), section 10.

8. LEGITIMATE GROUND OF PROCESSING HEALTH- AND OTHER SENSITIVE DATA: EXPLICIT CONSENT

Health data may only be processed if one of the grounds in Article 8 of the Directive is present.

In the context of consumer-oriented eHealth apps the ground which is most likely to be used is *explicit consent* (Article 8(2)(a) Data Protection Directive).
IMPORTANTLY, the national laws of Member States may provide that health- and sensitive data cannot be processed on the grounds of the data subject's consent.

In addition to *explicit*, **the data subject's consent** for processing health- (and other sensitive) data means must meet the general requirements for consent (see step 7)

Consent to undergo a certain medical treatment or participate in a clinical investigation does not equate "consent" necessary for processing health data.[9]

How does the national law of your country implement these provisions? Give reference to the relevant legal provision.

Explicit

This is an additional criterion to the general requirements of consent under Article 7 of the Data Protection Directive, specific of sensitive data. Consent under Article 8(2) must be explicit (therefore exclude the 'opt-out solutions'). Consent in particular must explicitly relate to the sensitive nature of health data and demonstrate that the data subject is aware that he / she renounces the special protection (ban on processing) of health data.[10]

The requirement of explicit consent must be respected regardless the practical difficulties connected to obtaining it. In any case, the controller must be able to demonstrate that the consent is valid.[11]

In order to receive a full impression of the requirement of explicit consent one has to refer to the national legislation of the Member States: (a) Article 8 (2)(a) allows the Member States to implement the Directive in a way that not even express consent can lift the general prohibition to process health data. (b) The form in which such explicit consent must be given varies from Member State to Member State. In some states such consent must be written whilst in others there is no such a requirement.

Free

Consent is 'free' when it comes as a result of a "voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other. Any consent given under the threat of non-treatment or lower quality treatment in a medical situation cannot be considered as 'free'."[12]

In a medical context – where data is processed as a "necessary and unavoidable consequence of the medical situation", it is misleading to legitimise this processing through

[9] WP 131, p. 8

[10] WP 131, p. 9

[11] WP 131, p. 9

[12] WP 131, p. 8

consent. **Consent to undergo a certain medical treatment does not equate "consent" necessary for processing health data.**[13]

Free consent means that the data subject can withdraw the consent without detriment.[14]

Which ground of processing of health and other sensitive data do you rely on for data processing?

How do you ensure that the consent of the data subjects (patients, their family members, medical professionals and other staff) is explicit, freely given, specific and informed?

[13] WP 131, p. 8

[14] Article 29 Working Party. 2001. Opinion 8/2001 on the processing of personal data in the employment context" (WP 84), section 10.

9. DATA SUBJECT INFORMATION RIGHTS

Data controller has to inform data about data processing. When data processing is based on the data subject's consent, the information must be provided before obtaining this consent, e.g. in a consent form.

When data is **collected from the data subject**, *at least* the following information must be provided to the data subject, except where he already has it (Article 10 Data Protection Directive):

(a) the identity of the controller;
(b) the intended purposes of processing;
(c) any further information such as
- who received the data (recipients and categories of recipients)
- whether or not answering a questionnaire is obligatory or voluntary; possible consequences of failure to reply;
- the existence of the right of access to and the right to rectify personal data.

When data is **not collected from the data subject**, e.g. but not only when existing health or other records are used, *at least* the following information must be provided to the data subject except where he already has it (Article 11(1) Data Protection Directive):

a) the identity of the controller;
b) the purposes of processing;
c) any further information such as
- the categories of data
- who received the data (recipients and categories of recipients)
- the existence of the right of access to and the right to rectify personal data.

The information has to be provided **at the time of data recording** or not later than the time when personal data is first disclosed to a third party (if data processing involves such disclosure).

When personal data is processed for the statistical purposes or scientific research and is not collected from the data subjects, an **exception** from these information requirements can be made only if:
- providing such information is impossible or would involve disproportionate effort, or
- recording or disclosure is expressly laid down by law (Article 11(2) Data Protection Directive).

How does the national law of your country implement these provisions? Does it name additional information that needs to be provided to the data subject?

Give reference to the relevant legal provisions.

Does the national law of your country require mandatory recording or disclosure of personal data that your app processes, e.g. in a medical context, recording of all health data in a hospital, regional or national patient file or health data database? If yes, what relevant safeguards / requirements does the national law provide? Do you meet those requirements?

It is recommended that in *smart environments* and especially when health- and other sensitive data is concerned, "apps must clearly and visibly inform their users about the existence of these access and correction mechanisms".[15]

In case an *automated decision* is taken on the basis of the compiled data (e.g. concerning patient's condition fit or not fit for further treatment), the data subject – patient or user, etc. – needs to be informed about the logic behind those decisions.[16]

Do you collect personal data directly from data subjects (patients, their family members, medical and other personnel, employees)? Specify which data and the instances of such collection.

How do you inform data subjects?

Does your use case involve personal data not collected from data subjects (patients, their family members, medical and other personnel, employees) but available from a different source (e.g. existing hospital-, regional-, national patient files and health records)? Specify which data and the sources and instances of such collection.

How do you inform data subjects?

If you do not inform data subjects, specify:

- how data subjects obtained the required information, or
- how informing data subjects is impossible or requires a disproportionate effort, or
- recording or disclosure that you do not inform about is prescribed by law, and how you comply with the requirements / safeguards laid down by such law.

When informing the data subjects about the identity of the data controller, provide the following information:

- the name and address of the organization as stated in its founding charter;
- designated representative of the data controller who will be in charge of data processing within the use case experimentation and whom data subjects can contact with their objections and requests: indicate his name and contact details.

[15] WP 202, p. 25

[16] WP 202, p. 25

10. OTHER CONTROL RIGHTS

The data controllers must enable data subjects – patients, employees, etc. – to exercise their rights of access, rectification, erasure and the right to object to data processing or block personal data that is incomplete, inaccurate or processed unlawfully (Pursuant to Articles 12 and 14 of the Data Protection Directive).

How does the national law of your country implement these provisions? Does the national law establish additional requirements and / or procedures with regard to these control rights? Are there any exceptions to these control rights? Give reference to the relevant legal provisions.

More specifically, in smart environments "apps must clearly and visibly inform their users about the existence of these access and correction mechanisms" which should be "simple but secure online access tools", available preferably "within each app, or by offering a link to an online feature."[17] These tools are especially important in case sensitive data is processed (e.g. health data) and have to be accompanied by proper identify verification mechanisms that should not lead to an additional, excessive collection of personal data.[18]

In case an automated decision is taken on the basis of the compiled data (e.g. concerning patient's condition fit or not fit for further treatment), the data subject – patient or user, etc. – needs to be informed about the logic behind those decisions.[19]

When data processing is based on consent, the users should be provided with the possibility to withdraw their consent in a simple and not burdensome manner. Preferably the option of consent withdrawal should be available through the above mentioned easily accessible **tools of the app interface**.

It must be possible to un-install apps and thereby remove all personal data, also from the servers of the data controller(s).

Consider what procedures and interface tools will be available to the data subjects to exercise their rights of access, rectification, erasure and the right to object to data processing or block personal data processed or intended to be processed for the purposes of experimentation within your use case trial.

[17] WP 202, p. 25

[18] Ibid.

[19] WP 202, p. 25

11. CONFIDENTIALITY OF PROCESSING

Any person who has access to personal data must not access or provide access to, delete or otherwise process these personal data "except on the instructions of the controller" except when the law requires otherwise (e.g. for law enforcement purposes) (Article 16 of the Data Protection Directive). This is called principle of **confidentiality.**

Note that once an employee or other person acting under the controller's authority begins to process personal data outside of the scope of the controller's instructions, he himself becomes a controller and may be held liable for the data protection violations and resulting damages.

How does the national law in your country implement this provision? Does it contain any additional requirements of confidentiality?

Consider how you ensure that personal data involved in the app is processed only as authorized, according to the principle of confidentiality?

Such measures may include but are not limited to:

- confidentiality obligation incorporated into a labour contract or a separate agreement signed by the staff;
- staff training on the matters of data protection and personal data handling, specifically, health- and other sensitive data handling,
- etc.
- See also step 12 – 'Security'

12. SECURITY OF PROCESSING

Data controller must ensure that personal data is secure, e.g. protected from unauthorised processing, including its destruction, alteration, disclosure and loss (Article 17(1) of the Data Protection Directive). This requires both **organizational** and **technical measures**. These measures should be taken both at the stage of designing your app and when it is running and used.

To identify appropriate measures, consider the privacy and security risks involved, the state of art of technology, and the cost of implementation (Article 17(1)). Note that the privacy risks are higher when the app is processing health and other sensitive data.

These measures should be documented for the purposes of proof (Article 17(4)).

A controller has an obligation to ensure – by way of a contract or other legal act (Article 17(3)) – that not only the controller but also data processors acting in his interests provide such 'sufficient guarantees in respect of the technical security measures and organisational security measures governing the processing to be carried out' (Article 17(4)).

How does the national law in your country implement these provisions? Give a reference to the relevant legal provisions.

The FI-STAR Data Protection Impact Assessment flowchart may be a useful tool here. Several points are of special significance:

- Processing health data implies **higher risks** for the data subject in case of unauthorized processing. This necessitates **stricter security measures**.
- Security measures must be incorporated in the design of the processing system and process, a principle known as *privacy-by-design*.[20]
- In multilayered structures such as (health) apps on smart devices, security measures have to be taken by all actors involved,[21] on all layers of platform and infrastructure.
- Compliance with the security obligations requires 'an ongoing assessment of both existing and future data protection risks.'[22]
- Effective mitigating measures have to be employed including data minimization.[23]

Many private and public bodies have issued recommendations regarding the organizational and technical security measures. A way to comply with the security obligations would be to use **data security standardization** schemes. Using such standards contributes to establishing whether or not the data controller abides by the data security obligations.[24]

Identify the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access and other unlawful processing of personal data associated with your use case trial.

What organizational measures have you taken / will you take to mitigate these risks?

What technical measures have you taken / will you take to mitigate these risks?

Do you use any standardization scheme in the field of data security? Which ones?

How have you documented / how will you document the security measures taken (e.g. in a data security plan)?

[20] Robinson, et al., 'Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office', p. 9.

[21] WP 202, p. 18

[22] WP 202, p. 18

[23] WP202

[24] ENISA, 'Information security certifications. A Primer: products, people, processes' Deliverable 2.1.5/2007, p. 11

13. NOTIFICATION OBLIGATION / DATA PROTECTION OFFICIAL

The data controller must **notify data processing** to the national data protection authority **before** carrying out such processing (Article 18 (1) Data Protection Directive). You can find contact information of the data protection authority in your country here.

National laws may provide for exceptions, e.g. when the data controller appoints a data protection official (e.g. Data Protection Officer).

The contents and procedure of the notification are to be determined by the national law of the member States.

If the processing in question presents 'specific risks' as identified by the national laws of the Member States, the national data protection authority will check this processing prior to their start (**prior checking – step 14**).

How does the national law in your country implement these provisions?

Identify the national data protection authority in your country.

Contact information of your national DPA is to be found here.

Check the national notification procedure. What information needs to be provided in the notification?

Is it useful to appoint a Data Protection Officer instead? This **data protection official** is an independent official within the organization responsible:

- for ensuring the internal application of the national data protection law;
- for keeping the register of processing operations carrying out by the controller.

Some countries **require the appointment of a data protection official**.[25]

Does the national law of your country allow for appointment of a data protection official (e.g. Data Protection Officer)?

Does the national law of your country require for appointment of a data protection official (e.g. Data Protection Officer)?

Does the national law of your country exempt from a notification obligation if a data protection official (e.g. Data Protection Officer) is appointed?

Has your organization (acting as the data controller for the purposes of this use case trial) appointed a Data Protection Official pursuant to the national law governing this position?

[25] e.g. Article 4f German Federal Data Protection Act.

Does data processing qualify for any such exemption?

14. PRIOR CHECKING

In case the national data protection authority is **not notified**, and the data processing in question is likely to present **specific risks** as determined by the national law, the appointed data protection official must conduct prior checking of the data processing operation in question and consult the national data protection authority in case of doubt (Article 20(1),(2) data Protection Directive).

How does the national law in your country implement these provisions?

Which data processing situations present specific risks to the rights and freedoms of the data subjects according to the national law in your country? In particular, do these situations of specific risks include processing of health data?

If processing personal data by your app is a situation presenting 'specific risks' as defined by the national law, has the data protection official appointed by your organization (acting as the controller for the use case trial) conducted or will he/she conduct prior checking?

Consider that such prior checking may result in advice to alter organisational or technical aspects of the data processing by your app or avoid it altogether.