Data Policy

Data Subject Rights

Allow and foresee means for your users to access their data stored in your system.

Allow the user to make changes or correct the stored data. Except if the app developer cannot access, change or delete the personal data (e.g.: stored on the user's device).

Inform the patient with all relevant information in relation to their rights.

Data Portability

Allow the user the right to obtain any personal data related to them in a structured, commonly used and machine-readable format and to transmit these data to another app.

Data Storage

You may no longer store personal data than necessary for the functionalities of the app. Deletion of data must be clearly communicated to the user.

After expiration, data should be deleted even if the user does not do so him/herself. Deletion of data must be clearly communicated to the user. (You may also choose for anonymization but strict rules imply)

You must ask the users whether they want to delete their personal data locally or remote, when they wish to uninstall the app from their device.

Data Processing

For data processing, performed by a 3rd party, these general rules apply:

1. Only make the data available after informing appropriately the user.
2. You must enter in a binding legal agreement with the third party, specifying:
    - The purposes for which they may use the data. This must be aligned with the information in 1.
    - Forbid the 3rd party any other processing.
    - Demand sufficient security obligations for the 3rd party, aligned with your own security measures.
    - Liability of the 3rd party regarding potential damage suffered by the app's users.

3. You must consider data transfer restrictions under applicable EU data protection laws. For restrictions to transfer data outside EU/EEA you must consider:
    - Locations are countries which are covered by an adequacy decision of the EC[1].
    - 3rd party has provided appropriate contractual guarantees (EU model contracts[2] or Binding Corporate Rules[3]).

Keep in mind that you are liable towards your users regarding any incidents with 3rd parties that cause them harm!

Data Breach

A data breach occurs when personal data is subjected to an incident leading to accidental or unlawful destruction, loss, alteration, disclosure or access to personal data.

This is the checklist to go through to avoid data breaches:

1. You should evaluate whether the (breached) data is personal data.
2. You should check whether there is an obligation to notify a Data Protection Authority (DPA) in a specific country or countries. As from May 25 of 2018 this is mandatory across the EU.
3. You should check the deadline to make such a notification to the DPA. As from May 25 of 2018, this needs to be done in the EU not later than 72 hours after becoming aware of the breach.
4. You should check the requirements for notification. As from May 25th of 2018, data breach notifications in the EU include:
    a. Description of the nature of the personal data breach (categories & approx. numbers of persons affected, categories & approx. number of personal data records affected).
    b. Communicate name and contact details of Data protection officer or contact point that can be reached.
    c. Description of consequences.

d. Description of the measures taken or proposed to address the personal data breach or mitigate its effects.
e. You should check if there is an obligation to notify affected individuals. As of May 25th, of 2018, in EU you need to notify data breaches to individuals without undue delay. This message needs to include: all items in 4. You are not obliged to notify individuals if:
    i. You have implemented appropriate technical and organizational protection measures (e.g. Encryption, etc.).
    ii. You have taken subsequent measures which ensure that the high risk to the rights and freedoms of the app users is no longer likely to materialize.
    iii. It would involve disproportionate effort. In that case, a public communication is mandatory.
    iv. You should address the cause of the breach as soon as possible and avoid further breaches.

---

[1] For an overview of countries with adequacy decisions, see External Links#Adequacy Decison

[2] For an overview of permitted contracts, see External Links#Permitted Contracts

[3] For an overview of BCRs, see External Links#Overview of BCRs