NTT DATA

Data Protection
6 Takeaways for Developers

While developing an app or a product you have to think about how your app or product will process user's data. Feel free to use the following 6 takeaways to ensure that your developing is data protection compliant, by design and by default.

1. COLLECTING DATA

Think before collecting any data. On this point, collect the minimum personal data necessary for the tasks that you want the app or product to perform.

Collecting personal data just in case you might need it later is a bad practice and must be avoided. To perform tests, please try consider using personal data only if the same result cannot be achieved with non-personal data (e.g. the so-called "dummy data").

The "Data minimization" and "purpose limitation" principles shall be your guide in developing. Never heard of them? Take a read of GDPR Article 5, is not as complex as you may think and it could change your way to approach programming.

2. DATA RETENTION

Do not store personal data for longer than is necessary and be ready to delete them in compliance with the information provided to the users in the notice, once they are no longer needed.

Users may not want their data to be stored in a database once it is not necessary anymore. Please try consider developing functionalities that allow data subjects to permanently delete in a quick and simple way their personal data as well as any account they may have set up with you.

Before collecting the data, define in advance and enforce a good data retention strategy in compliance with the one issued by your company, if available.

3. CONSENT

Provided that consent is necessary in order to process the personal data collected through the app or product, make sure to give data subjects a granular choice. Allow data subjects to easily review and change their decisions once the app or product is installed and in use.

Provide the data subjects with a single and obvious place to go to configure the various settings within the app or product and give them privacy-friendly defaults, it should be as quick to disable a setting as it was to enable it and set up a feature to permanently delete personal data and any account set up.

4. INFORMATION NOTICES

Data subjects must be properly informed in advance about what will happen to their personal data.

Use clear, simple language that is audience appropriate. Try using good graphical design, including use of colors and symbols to help data subjects to better understand – on this point the Italian DPA has released a set of symbols that can be used to make the information notices more clear.

For apps, provide relevant information in ways that better suits the small screen and touch-based interface of a typical mobile device.

5. ACCOUNTABILITY

Consider the types of data your app or product might process and think about how these could affect a data subject of the app or product at the design stage.

Assign responsabilities to the owners of the different activities or processes for fulfilling the principle of privacy by design. Document any stage of the development of the app or product and how data protection related aspects have been addressed during the development phase and subsequently once the app or product is released.

Know where and how data will flow when your app or product is used, and who is in control of the data throughout their lifecycle.

You are also responsible to assess the level of compliance of the IT components that you use.

6. SECURITY BY DESIGN AND BY DEFAULT

Research good security practices and apply them to the design of your app or product and the design of any central servers that the app or product communicates with.

We suggest to use encrypted connections for transmitting usernames, passwords and any particularly sensitive information, including device IDs or other unique IDs. Where passwords are used, ensure they are appropriately salted and hashed.

Pay attention to security vulnerabilities unique to your environment of operation, especially in the mobile app environment, and conduct security vulnerability scanning and penetration testing on your app or product and central servers before roll-out.

Implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.