A Compact Guide for Start-ups

qLegal A Journey in Dataland

Embedding Privacy by Design and Default

APP

You just developed a new mobile app or a wearable device and you can't wait to make it through market launch? Admit it. The last thing you worry about is whether you comply with the Data Protection Act 2018 ('DPA' in short). You will draft a privacy notice later and you are good to go!

Wrong!

Although you might think your responsibilities as an SME are less when it comes to data protection, that's not the case! There is one fundamental obligation in particular that might ruin all the hard work you and your innovative team have done. It is called 'Privacy by Design and Default' and is enshrined under articles 25(1) and 25(2) of the UK GDPR and 57 of the DPA accordingly.

Explaining Privacy by Design and Default

Did You Know?

The European GDPR is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review. The UK GDPR sits alongside the DPA and the key principles, rights and obligations remain the same.In relation to transfers of personal data between the UK and the EEA, the European Commission has issued an adequacy decision to allow for these when appropriate safeguards are in place.

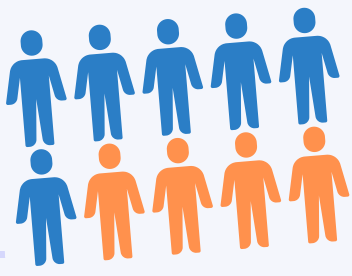
At a high-level, "Data protection by design and by default" requires you to put in practice appropriate technical and organisational measures to implement data protection principles effectively and safeguard individual rights. It requires you to consider privacy requirements from the first stages of product development, take the necessary steps and pre-configure default settings to ensure you process personal data in the most privacy-friendly way throughout the life cycle of it.

Privacy by Design and Default might look like an extra burden for an SME with limited budget and few employees, but it can significantly mitigate potential risks and save you from penalties, whilst also making your product more competitive. But how?

A Compact Guide for start-ups

qLegal A Journey in Dataland

Destination: Gaining Consumer's Trust



6/10 Europeans do not trust online businesses, while **8/10** would like to better control their personal data (European Commission,'The GDPR: New Opportunities,New Obligations'2018).

In an increasingly privacy-aware consumer market, data protection compliance is not just a tick-box exercise for SMEs but instead provide a competitive advantage that could be part of the product marketing strategy.

The Basics 1: Passport control

The most important first step for companies is to clarify whether they are data controllers or data processors because this will significantly impact their obligations. Essentially, the data controller determines the purposes for and means by which personal data is processed. So, if your organisation decides the 'why' and 'how' data should be processed it is the data controller– this is likely to be the case if you developed an app. The data processor processes personal data only on behalf of a data controller and is often a third party external to the organisation.

The Basics 2:Preparing your suitcase

Personal Data

The UK GDPR and DPA apply only to personal data. In practice, anything that could identify an individual even indirectly (IP addresses included) falls under personal data. **For your journey in Dataland you just need to bring personal data!**

Ok Startuppers, with a controller's passport in hand and a suitcase full of personal data, let the journey begin!

A Compact Guide for Start-ups

qLegal A Journey in Dataland

How to implement Privacy by Design and Default

Roadmap

Data Mapping

Initially the company needs to become aware of all the personal data it will collect from each app user and what is planned for this data. This exploration will be useful to perform a risk analysis, decide whether a Data Protection Impact Assessment is necessary and create a robust process for the storage, use and deletion of this data.To demonstrate compliance keep a written record and review it regularly.

Data Minimisation

After determining the types of personal data you plan to collect, the next phase is to doubt the need of each type of data collection. Data Controllers should limit the collection of personal data to what is strictly necessary to accomplish the specified purpose. The rule is simple:If the app can work without this data you should not collect it in the first place. For different sub-purposes a granular collection of data is recommended.

Unlinkability

The app should be isolated from the platform as much as possible;usage data concerning the app should not be communicated to the platform provider.

Timing Matters

Timing is crucial to ensure compliance. Besides implementing a retention policy (the shorter, the better) and the establishment of operational mechanisms to ensure everything is deleted properly, employees should access users' personal data on a 'need-to-know' basis and 'by default' personal data should be collected only during the use of an app instead of constantly.

Default Settings

The objective of default settings is to ensure fundamental principles of data minimisation and storage limitation from the first usage of the app,when the user has no choice (especially for 'wired-in' functions).Since many users will never change the default setting, it will govern the usage of the app to a great extent. For customisable functions, privacy by default is interlinked with privacy by design as apps should refrain from using design patterns that can lead users towards privacy-intrusive choices.

Be transparent. Inform.

Before the App installation and during the use of the app, the user must remain informed on what personal data will be collected and how it will be used. Be as clear as possible and inform users on the reasons you need to collect their data and their rights under data privacy law.

Make it visual and user-centric

For data subjects to have full control of their personal data,an effective user interface is necessary. Let your designers unleash their creativity and let the data subjects become informed and control the default settings whenever they want to. From dashboards, icons and just-in-time notices to animation videos the sky is the limit!

Gather feedback & apply changes

Once the UI designs are approved, start user testing. Conduct surveys to identify whether the user finds it too difficult to understand or change the settings and amend accordingly.

Dynamic Compliance

Compliance with data protection laws is not a one-off exercise. Keep in mind that with every use of the app more personal data is collected and with every new feature new default measures should be put in place. Regular monitoring and review are necessary.

Launch

After everything is checked, the first journey in Dataland is completed and you are ready for the next exciting destination: Market Launch!

For a compact overview of how the GDPR (that is reflected in the DPA) affects start-ups see our toolkit at:

http://www.qlegal.qmul.ac.uk/media/law/docs/The-Impact-of-the-GDPR-on-UK-Start-ups-Toolkit.pdf

A Compact Guide for Start-ups

qLegal A Journey in Dataland

Extra tips to keep in mind:

End to end security

The CIA triad (confidentiality, integrity and availability) should be implemented throughout the life cycle of the data (collection, classification,destruction etc).

Cyber-secure

Besides end to end security within the app, the company should take all technical and organisational measures to protect itself from cyber attacks (training of employees included).

Embed a privacy culture

In SMEs staff can be trained early on in relation to the UK GDPR and DPA, creating a culture that focuses on commitment to data privacy and continued improvement. Annual refresher training is essential.

Effective communication

Establishing accessible, simple and effective means of communication,and complaints for the owners of the data ('data subjects'). For user's that want to exercise their rights, secure online access tools within the app are recommended.

Insert clauses in contracts

Amend your customer or third-party contracts and include data protection clauses to set out how each party will process personal data. Note that if you are a data controller, you are accountable for the actions of each data processor. Carefully check if data processors and third-parties have robust data privacy compliance and necessary measures in place before you sign a contract with them. Double-check if an international transfer of personal data (outside the UK) may takes place and update your contract as well as your transfer mechanism as needed.

Demonstrate compliance

Even when it is not mandatory, record keeping is an essential tool for good data governance. In addition, the more your business grows the less likely you are to be exempt from record keeping requirements. As SMEs are more agile to new procedures, it would be advisable to start recording processing activities from an early stage so when the time comes, your employees will already be experienced in this area, making compliance with data privacy laws easier in the long-term.

qLegal provides pro bono legal advice to start-ups and entrepreneurs on data protection, intellectual property, corporate and employment law. If you want us to offer you a tailored advice, you can see our qLegal website for more details and to book your appointment.

Date produced: 22 September 2021

Author: Christina Varytimidou, LLM candidate in Technology, Media and Telecoms Law at QMUL.