Data protection

Privacy in mobile apps

Guidance for app developers

ico.
Information Commissioner's Office

Privacy in mobile apps

Guidance for app developers

Contents

Introduction

The Data Protection Act (DPA) exists to protect individuals' privacy. Just as with any other business or project, you need to comply with the DPA when developing a mobile app.

A typical mobile ecosystem contains many different components, including mobile devices themselves, their operating systems, plus apps provided through an app store. In many ways these are simply developments of earlier concepts that have been used on less portable computer hardware for years. However, the mobile environment has some particular features that make privacy a pressing concern:

- Mobile devices such as smartphones and tablets are portable, personal, frequently used and commonly always on.
- A mobile device typically has direct access to many different sensors and data, such as a microphone, camera and GPS receiver, together with the user's combined data including email, SMS messages and contacts.
- There are many different app configurations possible, and it is not necessarily obvious how an app deals with personal information behind its user interface.
- Mobile devices often have small screens, typically with touch-based interfaces. This can make it more challenging for apps to effectively communicate with app users.
- Consumers' expectations of convenience can make it undesirable to present a user with a large privacy policy, or a large number of prompts, or both.

In light of these issues, this guidance has been produced to help app developers comply with the Data Protection Act 1998 and ensure users' privacy.

Additionally, an organisation based outside of the UK that develops apps for the UK market, should consider that its users in the UK will clearly expect any apps they use to respect their privacy according to the DPA.

While a typical mobile device would be a smartphone or tablet, this guidance can also be applied to other devices using similar app technology, for instance living-room devices such as smart TVs or games consoles.

Throughout, the guidance concentrates on the issues most specific to the mobile environment, and includes references to more detailed

guidance where relevant. The ICO's 'Guide to data protection' is a good starting point if you need guidance on data protection in general.

As with all aspects of software, privacy is much easier to consider from the outset of a project rather than as an afterthought. This concept is often referred to as 'privacy by design'. The following sections will help ensure that you consider the relevant issues right from the start of your app development.

Users will have more confidence in apps that clearly respect their privacy. Users may uninstall or remove apps that contain surprises about how their personal data is used.

Will your app deal with personal data?

The DPA is concerned with personal data and how it should be dealt with. 'Personal data' is defined under the DPA as follows:

> "personal data" means data which relate to a living individual who can be identified—
>
> (a) from those data, or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

Remember that this definition of personal data is not limited to information typically considered a traditional identifier, such as an individual's name or a photograph of their face. A good example in the mobile environment would be a unique device identifier such as an IMEI number: even though this does not name the individual, if it is used to treat individuals differently it will fit the definition of personal data.

Example

Your app's main purpose is to display maps. These maps are downloaded by a mobile device from your central server. They are then later used on the device, when there may be no network connection available.

You realise that analytics would be useful to see which maps are being downloaded by which users. This in turn would allow you to make targeted suggestions to individual users about which other maps they might want to download.

You consider using the following to identify individuals who download the maps:

- the device's IMEI number;
- the MAC address of the device's wireless network interface; and
- the mobile phone number used by the device.

You realise that any of those identifiers may constitute personal data, so for simplicity you decide not to take on the responsibility of dealing with them yourself.

Instead, you decide to gain users' consent for the map suggestions feature. When a user consents, they are assigned a randomly-generated unique identifier, solely for use by your app.

Although unique identifiers of this type *may* in some cases not be personal, they certainly *can* be personal, and so must be dealt with accordingly when you design your app. If you are unsure about whether the data you're dealing with is personal, it will likely be simpler to treat it as personal data from the start.

See the relevant section in the 'Guide to data protection' for more information.

If you do deal with personal data, then you must fulfil certain requirements in the DPA.

Who will control the personal data?

It's vital to know where and how data will flow when your app is used, and who is in control of the data throughout the lifecycle of

the app. Without this knowledge it will be extremely difficult to ensure you comply with the DPA.

Be clear on whether you are, or will be, in control of any of your users' personal data. The term 'data controller' is defined in the DPA as follows:

> "data controller" means […] a person who […] determines the purposes for which and the manner in which any personal data are, or are to be, processed;

So if you, or your organisation, decide how personal data is dealt with, this means that you will be a data controller.

For instance, if you are distributing an app whose code purely runs on the mobile device and does not collect or transfer data elsewhere, then you are unlikely to be a data controller with regard to that app.

If however, your app sends a user's personal data elsewhere for processing, be clear and transparent about where this is and who will be in control of the transferred data.

Remember that apps are often designed much like webpages, whether the content comes from the device itself or from an internet-accessible resource. Don't let this get in the way of clarity and transparency as to where and how personal data is being processed.

Here are some examples of different situations and who would qualify as a data controller:

Example scenario	Who is the data controller?
Simple note-taking: your app allows the user to make simple notes and store them on the device for later reference. The notes may or may not contain personal data.	The user remains in control of any personal data created by the app, so there is no other data controller in this case.
Social media: your app allows users to share information with each other,	You will be the data controller for any personal data received by the central server.

including suggesting friends based on contacts stored on the user's devices. This is achieved by designing your app to communicate with a central server which is under your control. You do not use 3rd-party advertising, instead providing advertising yourself.	
Social media (cloud hosted): As above, except that the central server is hosted on infrastructure belonging to a cloud provider	You will be the data controller for any personal data received by the central server. The cloud provider is a 'data processor'.
Advertisement-funded game: your app is a free-to-download game, which funds itself by including adverts provided by a 3rd party ad network. The ad network may use personal data to deliver advertising based on previous browsing interests (online behavioural advertising).	The ad network is a data controller, but as the developer you will likely have a duty to inform your users of what personal data will be collected, how it will be used, by whom, and what control your users can exercise.
Reviews: your app is designed solely to submit user reviews to a 3rd-party reviews website which is not under your control.	The organisation responsible for the reviews site is a data controller for any personal data submitted to it. As the developer, you are not a data controller, but you should nevertheless explain clearly what happens to the data that your app submits.

If you are a data controller, you need to register with the ICO, unless your organisation is exempt. The ICO provides a self-assessment which can help you decide whether or not registration is necessary for your organisation. It is an offence to fail to register when you are required to do so.

Remember that even though it is possible to contract out tasks such as website hosting, the responsibility for data protection always rests with the data controller. If you are a data controller, choose a service provider carefully; the DPA requires that you have a written

contract with them (as a 'data processor' under the DPA) which includes security requirements. The DPA defines the term 'data processor' as follows:

> "data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

You should also be aware that if any personal data is to be transferred outside the European Economic Area (EEA), you will have to demonstrate that there will be adequate protection for it. More information on security requirements and international transfer can be found in the sections on Principle 7 and Principle 8 in the 'Guide to data protection'.

You are responsible for understanding the behaviour of any software components that you incorporate into your app. For instance, some app development frameworks include code for the purpose of advertising, which may process personal data.

If you're developing an app on behalf of a client, you may well not be a data controller. However your client will need to comply, so you should still consider privacy and security as part of your development process. Depending on your relationship with the client, you may also be a data processor under the DPA. If this is the case, then expect the client to insist on a written contract which covers appropriate security measures.

What data will you collect?

You should only collect and process the minimum data necessary for the tasks that you want your app to perform. Collecting data just in case you may need it in future is bad practice, even when the user has consented to provide that information. It's also in your interest not to hold data you don't need because this automatically reduces the risk that you might accidentally lose or mishandle it.

Additionally, you must not store personal data for longer than is necessary for the task at hand. You should therefore define retention periods for the personal data you will hold.

Set aside time in the design stage to consider the data types your app might access, collect or transmit and think about how these could affect a user of the app.

For each data type you want to collect, record how important it is to the overall purpose of your app, and what justification you have for collecting it. Record where that data may be transmitted. For each identified data type you should also consider the potential impact on the app user if that data were to be misused. In order to do this you should know how many times or how frequently it will be processed and how long the data needs to be stored for. You should also consider the accuracy and how easy it might be to identify a particular individual or device from that data.

You should aim to use the least privacy-intrusive data possible.

Example

Your social media app can upload existing images from a mobile device to your central server, and you want to avoid collecting unnecessary personal data.

You ensure that, by default, your app strips out unnecessary metadata from each image before it is uploaded, which may include the creation date or location of the image (stored in Exif format).

Example

Your app uses GPS location services to recommend interesting activities near to where the user is. The database of suggested activities is kept on a central server under your control.

One of your design goals is to keep the amount of data your app downloads from the central server to a minimum. You therefore design your app so that each time you use it, it sends location data to the central server so that only the nearest activities are downloaded.

However, you are also keen to use less privacy-intrusive data where possible. You design your app so that, by default, the device itself works out where the nearest town is and uses this location instead, avoiding the need to send exact GPS co-ordinates of the user's location back to the central server. Users who want results based on their accurate location can change the default behaviour.

Pay particular attention to what personal data you may be collecting if your app is aimed at children. The potential harm caused by

inappropriate collection of personal data will be greater if the child is not old enough to fully understand the significance of providing their personal data.

You should allow your users to permanently delete their personal data and any account they may have set up with you. You should only make an exception if you are legally obliged to keep the data.

If you want to collect usage or bug report data, this may well be possible, but typically must be done in either (or both) of two ways:

(1) with informed consent from the user; or

(2) using anonymised data (so that no personal data is collected).

Remember that if you rely on anonymisation, it must be performed thoroughly so that there is negligible risk of re-identifying a user from the data. For more detail on how this can be done, see the ICO's 'Anonymisation code of practice'. Further resources are provided by the UK Anonymisation Network (UKAN).

If you do choose to anonymise data, remember that this does not remove your responsibility for data minimisation; you should first collect the minimum personal data necessary, before anonymising. You should make effective use of the available permissions or other mechanisms in the operating system you are developing for. Your app should only request access to the sensors, services or other data which are necessary. If the operating system does not give you the granularity you require then you can provide additional information to users about exactly why a specific permission is needed.

All these steps are typical of a privacy impact assessment (PIA), a tool that the ICO encourages data controllers to use when planning their projects. The PIA for a given project can be made simpler or more complex, depending on the size and nature of the project. More guidance is available in the 'Privacy impact assessments code of practice'.

A privacy impact assessment can also be used as an input into any subsequent security assessment that you perform. If a PIA clearly defines what personal data should be kept confidential, then any security assessment can make reference as to whether the app does in fact ensure confidentiality of the relevant data.

How will you inform your users and gain consent?

Users of your app must be properly informed about what will happen to their personal data if they install and use the app. This is part of Principle 1 in the DPA which states that "Personal data shall be processed fairly and lawfully". For processing to be fair, the user must have suitable information about the processing and they must to be told about the purposes. Fairness is also about using information in ways that people would reasonably expect.

If you have performed a privacy impact assessment, then you could consider publishing it in order to increase transparency and further establish trust. Your organisation likely has little to lose: the work will already have been done, after all. More generally, the more background information you can make readily available about how your app works, the better informed your users can be.

Privacy information has typically been provided by many organisations via a privacy policy. However, there is no requirement for this information to be contained solely in one large document. In fact, in the mobile environment, this approach can be a hindrance. The relevant information can be provided in ways that better suit the small screen and touch-based interface of a typical mobile device.

The ICO's 'Privacy notice code of practice' is a general guide to drafting clear and informative notices. However, there are certain issues which are particularly important in a mobile environment.

Important points for providing notices or information in your mobile app:

- Use plain English.
- Use language appropriate to your audience. For example, an app to help school children with Maths homework should use language a child can understand.
- Transparency about purpose is crucial. Don't just say *which* data you want, say *why*. Operating system (OS) permissions on their own are unlikely to be sufficient (although future mobile OS developments may change this).
- Make relevant privacy information available as soon as practicable. Ideally this would be done before the user downloads the app, and could be done via an app store or via a link to your privacy policy. Where you provide privacy information *after* an app is downloaded and installed, make

sure that this is done *before* the app processes the relevant personal data.

- If appropriate, use a 'layered' approach where the most important points are summarised, with more detail easily available if the user wants to see it.

Figure 1a: Example of a short statement from a layered privacy policy

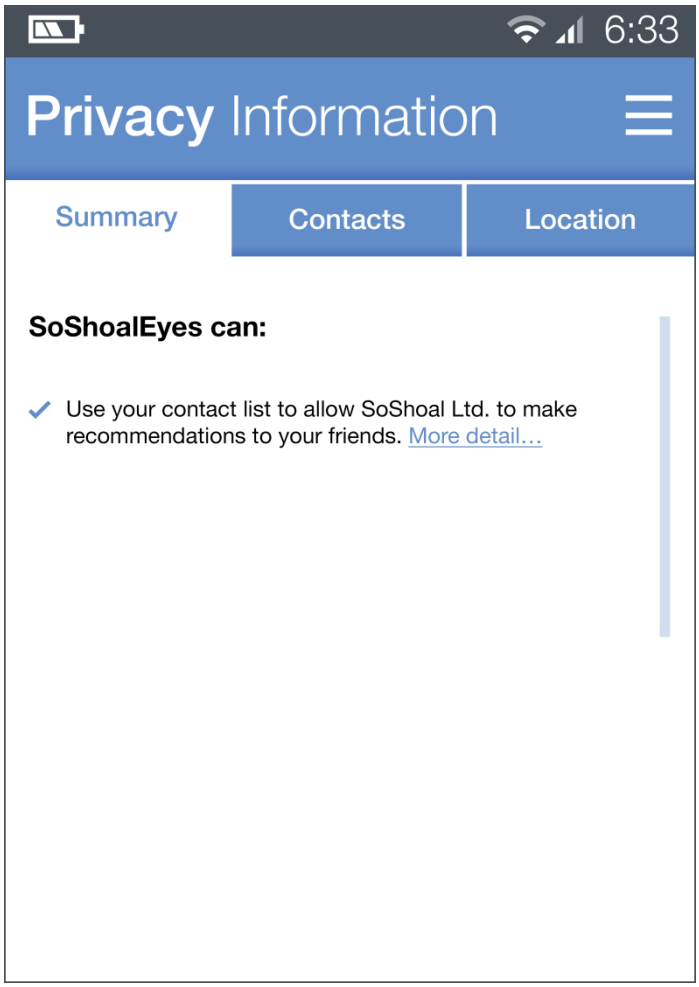
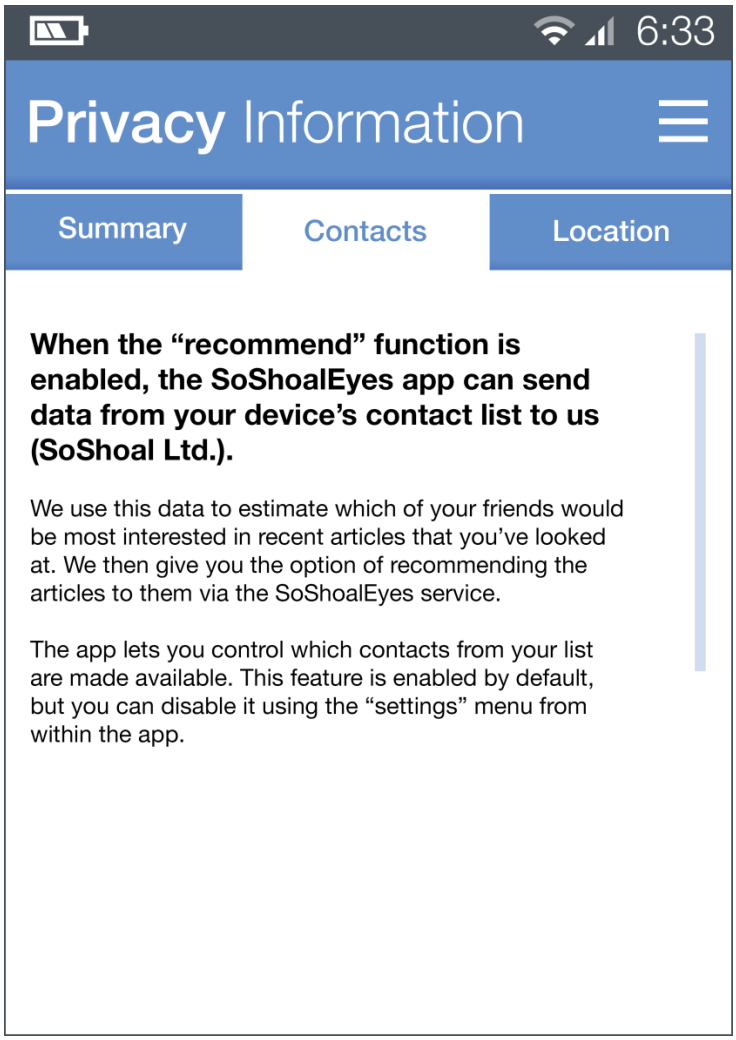
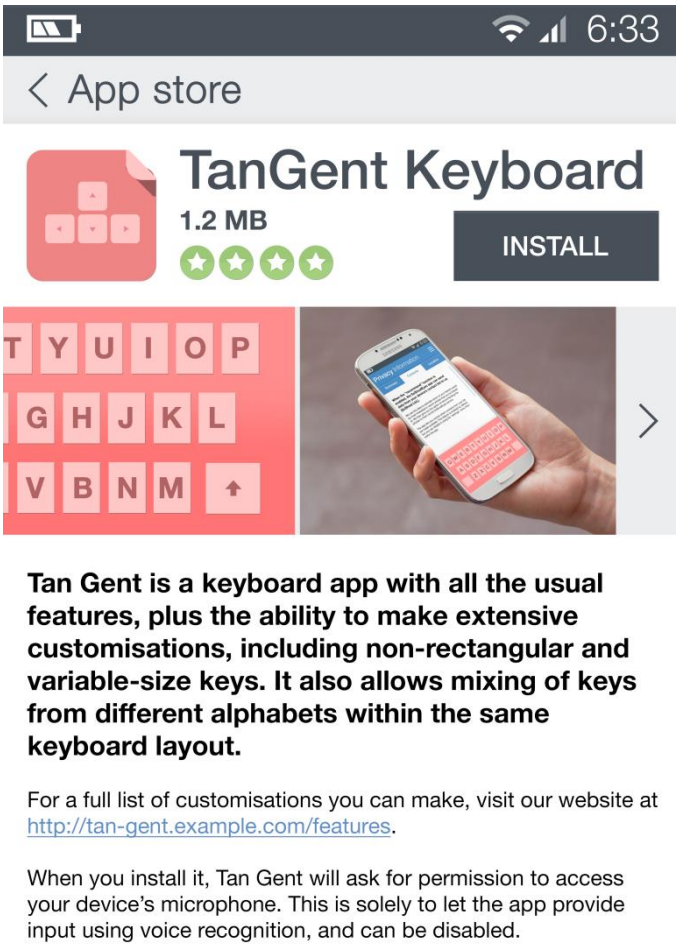


Figure 1b: Corresponding longer statement from a layered privacy policy



- Good graphical design, including use of colours and symbols, can help your users understand better.
- Take into account the entire user experience, including browsing the app store, where applicable. If the user has already been provided with relevant information in the app store page, there may be no need to repeat this information at installation. Remember that this may not be the case when the app is made available through other methods, for instance with default apps that come pre-installed with the device, or 'side-loaded' apps which are not made available through a reputable app store.

Figure 2: Example of providing relevant privacy information from within an app store



- If you develop for multiple platforms, ensure that you take account of any differences between mobile platforms and their respective app stores –information and features provided by one platform are not necessarily provided by another.
- Pay particular attention to highlighting any actions that would be unexpected or considered onerous by the user. Conversely, do not hide important information or otherwise mislead the user.

Example

The developer of a music player app wants the app to pause music playback when the device receives or makes a phone call. In order to do so, the app must request permission to monitor the state of incoming or outgoing calls.

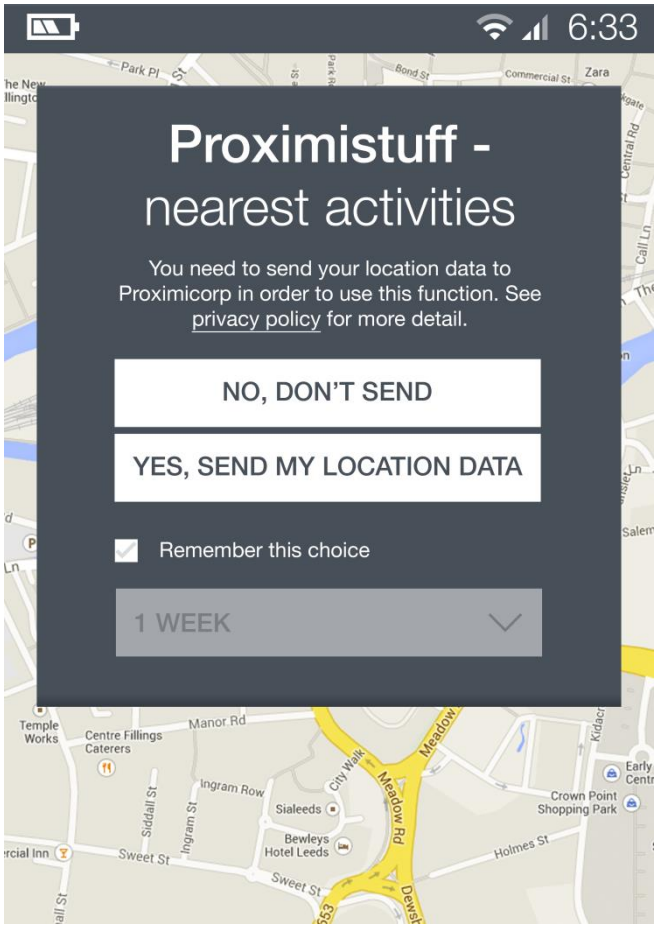
The app developer notices that the precise permission he requires is part of a larger package of functions which must all be granted permission by the user. This means that the app developer could potentially access functions or data on the device which are not strictly necessary for the original purpose of the app (eg the permission to listen to or record calls).

The app developer recognises this risk and provides a statement in the app store description:

"In order to pause music playback when you receive or make a telephone call the app needs access to the phone functions."

- Saying what you *won't* do may help make your intentions clear.
- You don't need to state what would be obvious to a reasonably-informed user. If you are designing an app to make delivery orders, it will be obvious to the user that providing the delivery address is necessary to provide the desired service. You would only need to highlight collection of this data if it were going to be used for other, non-obvious purposes.
- Consider just-in-time notifications, where the necessary information is provided to the user just before data processing occurs. Notifications like this could be particularly useful when collection more intrusive data such as GPS location, or for prompting users about features of an app that they are using for the first time. You could avoid excessive notification by remembering the user's choice for a certain time period before reminding them again.

Figure 3: example of a just-in-time notification.



- Remember that if your app passes data onto another organisation, this will require adequate information to be provided too. This includes networks that provide Online Behavioural Advertising (OBA); in fact, these networks may impose a contractual obligation for you to inform users or gain consent.
- If your app is supported by advertising make this clear to your users and give information relating to any analytics you might have included within the app. One alternative is to offer a paid-for version of the app with advertising removed.

Remember that the information you provide to comply with the DPA can also contribute to your compliance with other laws. For instance, it may be important to ensuring your contract terms are fair. See the section 'Some other important legal considerations'.

If you are acting as a data controller, it is fundamental that you identify yourself and give your app users a simple means to contact you. The major app stores allow developers to include an email

address and website address in the app catalogue. Make sure you monitor this contact method and respond effectively to any queries, including bug and feature requests. If you have an external website you should make sure all of the relevant information is also available here.

Remember that as a data controller, you will have a legal responsibility to respond to a user if they make a written request for a copy of their personal data that you hold. This is called a 'subject access request' and includes requests made by email or through social media. The ICO's 'Subject access code of practice' provides more detail. In order to reduce the number of formal subject access requests you receive, you might consider providing users with routine access to their personal data, perhaps through an online service.

Finally, even if you are not acting as a data controller, providing a contact method is advisable in order to establish user trust.

How will you give your users feedback and control?

Give users a granular choice where possible. This allows the user to make meaningful decisions rather than giving the user a single 'all or nothing' choice.

Allow your users to easily review and change their decisions once the app is installed and in use. Give them a single and obvious place to go to configure the various settings within the app and give them privacy-friendly defaults. It should be as quick to disable a setting as it was to enable it.

If your app processes personal data in an unexpected way or is of a more sensitive nature you might need to consider the use of additional 'just-in-time' notifications or other alert systems to inform the user what's happening. For example, if geo-location services are running in the background or you are uploading data to the internet, consider using clear and recognisable icons to indicate that this is occurring and where necessary the option to stop (eg to cancel an upload).

Appendix provides further examples of how you can give your users better feedback and control over their personal data.

How will you keep the data secure?

Research good security practices and adhere to them, both in the design of your app and the design of any central servers that the app communicates with.

Where passwords are used ensure they are appropriately salted and hashed on any central server. In usage cases such as a password manager app, where the password cannot be hashed, explain clearly to the user what this means.

Take advantage of encrypted connections to ensure security of data in transit, by using SSL / TLS for instance. You should always use encrypted connections for transmitting usernames, passwords and any particularly sensitive information, including device IDs or other unique IDs.

If your app stores data for later use, you should consider using encryption to do so. The method of encryption, if any, should be appropriate to the sensitivity of the data. Depending on the circumstances, you may choose to rely on the operating system's ability to enable encrypted storage.

Use tried and tested cryptographic methods, rather than implementing your own cryptography. Whether the purpose is for transmission or storage, research the most appropriate cryptographic methods and use established implementations of them.

Similarly, avoid writing your own code to perform functions which have well-established implementations that you can re-use (in-app billing or app updates, for example).

You should be particularly careful if your app accesses data from other apps or locations; respect the sensitivity of the data in the context of its original purpose, not solely in the context of your app.

Example

Your app is designed to allow employees to view and edit corporate documents while on the move. The documents are accessed over a Virtual Private Network (VPN) so that the app can contact an internal file server as if the employee were in the office.

The internal file server is hosting some documents that contain commercially sensitive information as well as personal data. To mitigate the consequences of a burglary at the office, the server uses full-disk encryption and is physically locked in a secure server room.

As the app may be used to view the same files, you decide to apply similar restrictions, including:

- no ability to save the document to the device unless encrypted storage has been enabled; and
- restricted ability to take screenshots of the document viewer app.

In addition to the type of vulnerabilities that occur online or in computing generally, pay attention to vulnerabilities which are more relevant in a mobile apps environment, such as:

- *Inter-app injection flaws* – in the same way that a web application may be vulnerable to, say, SQL injection, an app might be vulnerable to injection when accepting input from other apps. Ensure that when your app does accept input, it is sanitised in a way that's appropriate for the task at hand.
- *Failure to properly check SSL / TLS certificates* – merely using the encryption provided by an SSL / TLS connection does not provide a guarantee of a secure connection. You also need to verify the identity of the party you're communicating with, by checking the certificate as well. If you use certificate pinning rather than obtaining a certificate from a trusted certificate authority, ensure it is correctly set up.
- *Misconfiguration of SSL / TLS on a central server* – ensure that any central server only enables strongly-encrypted connections and has a valid SSL / TLS certificate. The limited interface on a mobile device may not make the security status of an SSL / TLS connection obvious. If the mobile device checks the connection properly and then rejects the connection due to a poorly configured central server, your app may be rendered useless.

Dependent on the privacy and security risks involved, consider security testing both your app and any central servers before roll-out. Vulnerability scanning or more in-depth penetration testing, or both, will alert you to potential problems. Providing you pay proper attention to any issues raised and address them, security testing will provide assurance as to the security of your app.

How will you test and maintain your app?

The install process and the requesting of device permissions will be important areas to test. Consider what a new user will see when they install your app and see what permissions it requests. Remember to test all the platforms you're developing for.

After any changes to your app's code, test to ensure that the app's behaviour is as expected and still matches with the plan you created in the design phase. It can be very easy to make modifications during development which might appear to be minor but have a significant impact on data protection.

For example, you could speed up an activity by removing a touch of the screen, but this touch may have been relied upon to provide evidence of user consent being granted.

More generally, where your app gives users a choice on whether to permit or deny access to personal data, make sure you test the user experience in both scenarios. Check that a decision to deny access does in fact have the desired effect and that your app does not go on to use the personal data anyway.

If you produced a privacy impact assessment earlier, review it and re-publish it where applicable.

Once the app is made available to users you should continue to ensure that you are living up to your promises. For example, check data is not being retained beyond your stated retention period and that the security mechanisms you are using are still up to date and relevant, especially as operating systems introduce new features. Similarly, as the state of the art progresses, look out for better, more privacy-friendly ways of performing the same tasks.

Inform users (and give them a choice) about any changes to the purpose or scope of your data collection. You will normally need to seek users' consent regarding any new data processing, unless you have another clear legal basis for the processing.

If you are made aware of a security vulnerability in your app, take action to protect your users. This would typically involve fixing the issue in the app's code and issuing an updated version of the app. It should also include, where possible, notifying users of known-vulnerable versions of the app so that they can protect themselves by upgrading.

If you become aware of an actual security breach of systems you are responsible for, take swift and appropriate action to remedy the problem. This could include notification of affected users or forcing password resets. You should consider reporting the breach to the ICO according to the 'Guidance on data security breach management'.

Some other important legal considerations

The ICO also regulates parts of the Privacy and Electronic Communications Regulations (PECR) which will be relevant to your app if it is designed to:

- send email, SMS text messages, or voicemail messages;
- make phone calls;
- set cookies or other tracking elements; or
- engage in 'viral' marketing campaigns.

If you are thinking of making an app that performs any of these actions, you should be aware of the restrictions in PECR, which cover calls, texts and emails and are stricter than, for instance, those on mail marketing. This means that consent must be more specific, and will depend on the method of communication and the context of your app.

More information is available in the ICO's 'Guide to PECR' and guidance on direct marketing.

If your app is intended to use a premium rate service, you should adhere to the guidance provided by PhonepayPlus, the UK regulator for premium rate numbers and services. This will be relevant for example, if you want your app to send premium rate texts, make premium rate phone calls or provide application-based billing. The guidance covers areas including digital marketing, privacy and consent to charge.

Additionally, the Office of Fair Trading (OFT) enforces a range of consumer protection laws which are also relevant to app development.

The Consumer Protection from Unfair Trading Regulations (CPRs) prohibit unfair commercial practices relating to transactions between consumers and businesses. Broadly speaking, if your business misleads, behaves aggressively or otherwise acts unfairly towards consumers, then your business is likely to be in breach of the CPRs and may face enforcement action. See the OFT guidance on CPRs for more information.

The Unfair Terms in Consumer Contracts Regulations (UTCCRs) require standard contract terms to use plain and intelligible language. Important contract terms, particularly those which may disadvantage consumers, must be clear, prominent and actively brought to consumers' attention – not hidden in the small print of 'terms and conditions' or 'privacy policies'. This means, for instance, that if your app is distributed free of charge you should be particularly careful when asking for in-app payments once the app is installed and running. Refer to the OFT guidance on UTCCRs for more information.

If you do take payment from within your app, remember that you need to obtain proper authority, particularly for continuous payments. The OFT's Principles for Use of Continuous Payment Authority explain how this should be done.

The OFT has also proposed 8 principles for developing online and app-based games. These principles outline how an app-based game can better fulfil the requirements of the relevant consumer protection laws, but they will also have relevance to any app, whether or not it is a game.

Appendix 1

Further examples of good (and poor) practice

Example: An app allows users to record data about fitness activities, such as running or cycling, including location, altitude, speed and heartbeat. The data can be uploaded to a cloud service to share with other users of the app. The app also allows users to link with a range of popular social networking sites and automatically post updates of their most recent activities.

Good practice:

- There is a map on the home screen of the app with a clear marker showing the current location. This makes it clear that geo-location services are accessing the current location.
- An icon is visible indicating the geo-location services of the device are active.
- A clear, recognisable icon is used for the 'start' button, which must be pressed to start recording data.
- A clear indication is given of which external sites the user can upload the data to at the end of the activity. There is no obligation to upload anything.
- A simple means is given to access the settings to configure or to view current permissions.
- A simple interface is provided to remove or hide uploaded activities which the user no longer wants public.
- When uploading location data, the app allows the user to 'blur' the location by, for instance, only naming the nearest town.
- A simple means is provided to immediately and irretrievably delete activities the user no longer wishes to keep (eg a delete button next to each

Poor practice:

- Users are forced or not given an easy option to use the app without linking with a social networking site and automatically posting their recent activity.
- There is no clear explanation of which sites the user's data will be uploaded to.
- On first run, the app requests the user to enable public sharing of all fitness activity via a full screen notification, but the setting to disable the same feature is hidden and hard to find within the app.
- Shared activities always include precise GPS co-ordinates, with no option to disable this behaviour.
- Unique device identifiers (eg IMEI) are embedded within or otherwise linked to the fitness activities stored or uploaded to external sites.
- On install, the app states that it needs permission to send SMS messages, but there is no explanation as to why this is necessary.
- Users are forced or not given an easy option to use the app without granting access to stored contacts (either on the device or in social networking sites). The app automatically sends notifications to each contact as a form of viral marketing.

activity in a 'history' tab) • Before uploading of activities, a confirmation dialog is displayed and a progress bar is displayed with a 'cancel' option. • Where multiple reminders may cause an interruption to the user experience, an option to 'remember this option' is used with the option to disable found in the settings page.	• The app uses Bluetooth to communicate with the user's heart rate monitor. However, the app automatically tries to pair with any nearby device and does not give the user an option to restrict Bluetooth pairing.