Code of Practice for App Store Operators and App Developers

Background

This voluntary Code of Practice sets out practical steps for App Store Operators and App Developers to protect users. The eight principles within the Code refer to globally recognised security and privacy practices. They are not written in a priority order as they are each important in helping to protect users' security and privacy. The ICO has provided input for Annex A which highlights legal obligations from UK data protection law relevant to the Code of Practice. Some of the principles within the Code are mandated through existing legislation, including data protection law and other principles will help stakeholders demonstrate steps towards adherence. There are also obligations in existing legislation to notify particular regulators in specific circumstances. The ICO has also provided input for Annex B which provides an overview of how a stakeholder can make a referral to the ICO if they find details of security and/or privacy concerns in apps. Annex C includes details of an additional requirement on securing the mechanism for creating enterprise app stores which applies to particular types of app stores.

The responsibility to implement the principles falls on App Store Operators, App Developers and Platform Developers. However, given the role of App Store Operators in setting policies and processes for their app stores, reasonable steps should be taken by them to verify that App Developers and Platform Developers are adhering to the principles set out in this Code. This Code will be reviewed, and if necessary, updated no later than every two years in light of technological developments, further clarifications, modifications to regulations and changes to the threat landscape in this area. For example, we may in the future consider if the Code should be expanded to include practices for Software Development Kit providers.

Audience

An indication is given for each principle within this Code as to which stakeholder is primarily responsible for implementation. Stakeholders are defined as:

App Store Operators: The persons or organisations responsible for operating the app store. The App Store Operator will have capability to add and remove apps. They will also decide on the requirements that apps will need to meet to be included in the app store, taking into account any legal requirements.

App Developers: Persons or organisations which create or maintain apps on the app store. App Developers are responsible for ensuring their app meets the requirements of the app store, as well as any legal requirements.

Platform Developers: Persons or organisations responsible for producing the operating system, default functionality and the interface that enables third parties to implement additional functionality, such as through apps.

Business-to-Business application programming interface (API) providers are not required to comply with the Code because it is the Developers' responsibility to understand what API codes/services they use and then develop their apps.

Key terms

App Store: A digital marketplace that allows users to download apps created by developers, including developers other than the app store's developers. App stores do not only host apps, as they also serve as storefronts that allow users to browse for apps, such as via search functionality.

Malicious app: A malicious app is one which intentionally seeks to illegally take user data, money, or control of their device, outside of the understood purpose of the app. It also incorporates apps that make a user or device undertake illegal activity. Indications that an app is malicious include (but are not limited to) phishing for credentials or illicitly collecting multiple types of sensitive data (e.g. contacts, messages), coupled with indicators of detection evasion such as obfuscation, dynamic loading, or cloaking of malicious behaviour.

Vulnerabilities: A vulnerability is a weakness in an app that may be exploited by an attacker to deliver an attack. They can occur through flaws and features, and attackers will look to exploit any of them, often combining one or more, to achieve their end goal.

Assessing adherence to the voluntary Code

There will be a 9 month period for Operators and Developers to adhere to the Code. DCMS are only initially focusing on assessing adherence of the Code with App Store Operators. This is because the vast majority of users access apps from platforms offered by Operators. DCMS intends to commence meetings with Operators from early 2023 to determine if Operators have started to enact changes in their processes, including requirements for Developers based on the Code. Operators are welcome to organise additional meetings with DCMS to seek any clarifications and to highlight what actions they are taking. DCMS intends to also request written reports from Operators in Spring 2023 which will be treated as confidential. The reports should clearly state how they meet the provisions in the Code and/or the steps that are being taken to adhere to the Code.

Once these meetings and written reports have been reviewed, if DCMS determines that insufficient data has been provided and/or that many Operators are not taking steps towards adherence, then we intend to commission our own independent research. This is a voluntary Code, therefore Operators and Developers will also be able to differentiate themselves by affirming publicly that they comply with the Code. We will work with the Operators and Developers to check this is the case. We will also welcome any feedback from other stakeholders and will liaise closely with cyber security companies who have published research reports on areas that overlap with provisions in the Code.

1. **Ensure only apps that meet the Code's security and privacy baseline requirements are allowed on the app store[1] -** Primarily applies to: App Store Operators

1.1. App Store Operators shall clearly set out security and privacy requirements for apps on the app store, published in a location that does not require purchasing access by Developers. This shall include those provisions set out in principle 2.
1.2. App Store Operators shall have a vetting process which includes security checks in which the above requirements are reviewed prior to approving app submissions and updates. Operators shall notify the Developer if an app or update is rejected for security reasons (see principle 7 for more detail).
1.3. App Store Operators shall provide an overview of the security checks that are undertaken for apps and updates in a publicly accessible location.

Example of information provided by an Operator on their security checks

Apps undergo a security check which consists of both automated and manual activities. The following activities will be undertaken:

- Use of static analysis tools
- Confirmation of necessity of permissions
- Confirmation of Software Development Kit versions
- Scanning for default credentials
- Sharing of submission with a third party for further static analysis and vulnerability scanning.

1.4. App stores shall have an app reporting system (such as visible contact details or a contact form), so that users and security researchers can report malicious apps, and Developers can report fraudulent copies of their own apps to the app store.
1.5. Once an App Store Operator has verified that an app is clearly malicious, they shall make the app unavailable on the app store as soon as possible but no later than 48 hours. Operators shall notify the Developer that their app has been made unavailable.
1.6. Once an App Store Operator verifies that an app or an update is malicious, they should initiate a proportionate review of other apps that have been produced by the same Developer.
1.7. App Store Operators and Developers should consider working with independent parties to assess app security and privacy.

[1] Please note – Relevant authorities such as NHS England and Medicines and Healthcare products Regulatory Agency (MHRA) are exploring whether an enhanced regime focused on clinical safety for health apps are appropriate.

2. **Ensure apps adhere to baseline security and privacy requirements -** Primarily applies to: App Developers and Platform Developers

2.1. Developers shall use industry standard encryption within their apps, specifically in relation to data in transit and where an app needs to encrypt data locally.

Apps utilise, receive and transmit data that is often sensitive in nature. This may include data relating to users, an enterprise, functionality or other information necessary for the app to operate securely. This data needs to be encrypted at rest and in transit in order to ensure it cannot be compromised by an attacker.

This may be done by APIs native to the platform, which will often integrate with secure hardware on the device.

2.2. Developers shall ensure that the primary function of an app operates if a user chooses to disable its optional functionality and permissions.[2]

2.2.1. If the user isn't presented with any optional functionalities, developers shall ensure that their app only requires the enabled functions and permissions necessary to operate.

2.3. Developers should not request permissions and privileges which are not functionally required by the app.[3]

2.3.1. Developers shall share the permissions and privileges requested by the app in the app manifest with the App Store Operator, to allow for this to be cross-checked.

A functional requirement is defined as one that is necessary for the user-facing operation of the app. This does not include any background operation which does not offer the user any features or an improved experience.

2.4. Developers shall take steps to make their app adhere to security requirements, data protection by design, broader requirements set out in data protection law[4] and other appropriate laws to the app's purpose.[5]

2.5. Developers shall ensure there exists a simple uninstall process for their app.[6]

---

[2] Developers should be aware that the standards of the ICO's Children's Code require that certain functionality, in particular geolocation (under standard 10), is off by default unless the service provider can justify why it should be on by default, taking into account the best interests of the child. See: "Age appropriate design: a code of practice for online services". Guidance to support the implementation of the Children's Code can be found here: The Children's code design guidance

[3] Relevant stakeholders must adhere to requirements under UK GDPR Articles 13/14 to explain the purposes for processing personal data, which would include processing facilitated via permissions or optional functions.

[4] Mandated in data protection law; see UK GDPR Article 5(1)(f), 25 and 32 and Annex A. For further information on security requirements and data protection by design and default see: Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)" and "Data protection by design and default"

[5] With regard to regulatory requirements for health-related apps that qualify as medical devices, please refer to UK Medical Device Regulation and accompanying guidance Medical devices: software applications (apps) for Great Britain and to Regulation (EU) 2017/745 for Northern Ireland. The NHS Digital Technology Assessment Criteria (DTAC) sets out the standards that are required from health apps and digital health technologies.

[6] This may be by using the standard functionality of the operating system. However, when using a platform without that functionality, this may involve providing an uninstall script.

2.6. Developers should have a process to readily update and monitor their software dependencies for known vulnerabilities in all the published versions of their app.
2.7. Developers should provide users with a mechanism to delete locally held data, and request deletion of personal data gathered by an app.[7]

3. **Implement a vulnerability disclosure process -** Primarily applies to: App Developers and App Store Operators

3.1. Every app shall have a vulnerability disclosure process, such as through contact details or a contact form, which is created and maintained by the Developer.
3.2. Operators shall check that every app on their platform has a vulnerability disclosure process which is accessible and displayed on their app store. This process shall ensure that vulnerabilities can be reported without making them publicly known to malicious actors.
3.3. App Store Operators shall ensure that their app store has a vulnerability disclosure process, such as contact details or a contact form, which allows stakeholders to report to the Operator any vulnerabilities found in the app store platform.
    3.3.1. App Store Operators should accept vulnerability disclosure reports from stakeholders for apps on their platforms if the Developer has not issued acknowledgement specific to said report after 15 working days. App Store Operators should assess the merit of these reports, and contact the Developer if they are deemed credible.
    3.3.2. If App Store Operators don't receive an acknowledgement from the Developer, after a further 15 working days, then they should make the app unavailable on the store.

The NCSC's Vulnerability Disclosure Toolkit exists to help organisations implement an effective vulnerability disclosure process. Such a process should:

- Enable the reporting of found vulnerabilities
- Be clear, simple and secure
- Define how the organisation will respond

The Toolkit defines how to effectively communicate with finders of vulnerabilities, and how to make a sensible policy that will be clear to the necessary stakeholders. We recognise that vulnerability disclosure reports could be abused for various reasons, such as attempting to make an app unavailable.

App Store Operators and App Developers may also benefit from the following standards:
ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure
ISO/IEC 30111:2019 - Vulnerability handling processes

[7] Mandated in data protection law where the right to erasure applies under UK GDPR Article 17. See Annex A for more information.

4. **Keep apps updated to protect users -** Primarily applies to: App Store Operators, App Developers and Platform Developers

   4.1. Developers shall provide updates to fix security vulnerabilities within their app.[8]
   4.2. Developers shall update their app when a third-party library or software development kit (SDK) that they are using receives a security or privacy update.[9] See principle 6.4 for the proposed actions on App Store Operators.
   4.3. When a Developer submits a security update for an app, App Store Operators shall encourage users to update the app to the latest version.
   4.4. App Store Operators shall not reject standalone security updates without providing a strong and clear justification to the Developer as to why this has happened. In cases where an Operator is not approving the update due to concerns that they are engaging with a malicious Developer, an Operator shall have flexibility on the time period and detail of said feedback.

A standalone security update is one which affects only the security and privacy functionality of the app, with no changes to user functionality, or non-security background operation.

   4.5. App Store Operators shall contact a Developer if an app has not received an update for 2 years to check that the app is still being supported. If the Operator does not receive a response from this process within 30 days, then they shall make the app unavailable on the store.

[8] In line with data protection law requirements of UK GDPR Article 32. See Annex A for further information.
[9] In line with data protection law requirements of UK GDPR Article 32. See Annex A for further information.

5. **Provide important security and privacy information to users in an accessible way -** Primarily applies to: App Store Operators and App Developers

5.1. When an app is removed or made unavailable from an app store, the Operator shall notify users of said app and link to instructions on how a user would remove the app from their device within 30 days.[10]

> The term "unavailable" refers to when an app is hidden from new users so they can't download the app, but may still be on the app store so current users may be able to receive updates.
>
> The term "removed" includes when an app is completely removed from the app store; this could be by either the operator or developer. This may be for security or other reasons.

5.2. Developers shall provide the following information about an app's behaviour: where a user's data is stored, shared and processed within a privacy policy; when the app was last updated; and other relevant security information.[11]

5.3. App Store Operators shall display the below information (provided by Developers) for all apps on their app store, such as in a dedicated security and privacy section:[12]

- 5.3.1. The jurisdictions where a user's data is stored and processed for each app.[13]
- 5.3.2. The stakeholders that are given access to a user's data. The categories of stakeholders that are displayed to a user should include third party companies, the app's organisation, specific governments or not shared with anyone.
- 5.3.3. The purpose of accessing or using a user's data. Categories should include marketing, analytics, user services.
- 5.3.4. When the app was last updated and any other relevant security information, as well as the information linked to permissions noted in principle 2.
- 5.3.5. The above information shall be written in an accessible format for all users and be clearly available prior to purchase and download.

5.4. Developers shall provide information about the permissions which an app may request, such as access to contacts, location and the device's microphone, along with justifications for why each of these permissions are needed. This information shall be provided to app stores and any users who install the app without an app store. Operators shall display this information for all apps on their app store prior to purchase and download.

---

[10] This should not supersede principle 1.4 and 1.5 related to malicious apps.

[11] See UK GDPR Article 4(1) and (2) for definitions of personal data and details on processing: https://www.legislation.gov.uk/eur/2016/679/article/4

[12] There are services offered by industry to help operators with verifying this data so that factual information is signposted to users.

[13] NCSC Cloud Security guidance (see principle 2 on physical location and legal jurisdiction). Additionally, the guidance notes that the service provider should be able to tell you where your data is processed, where it will be stored, and in what country the company (and any of its providers that handle your data) is legally based. See: https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-2-asset-protection-and-resilience

6. **Provide security and privacy guidance to Developers -** Primarily applies to: App Store Operators

6.1. App Store Operators shall signpost this Code of Practice to Developers prior to an app's submission.
6.2. App Store Operators should publicise any upcoming changes to be introduced to their Developer guidelines / policies.
6.3. App Store Operators should provide information on what is considered best security and privacy practice where that goes beyond the Code's baseline requirements, such as information on other standards that have been produced.

See DCMS's mapping of the app security standards landscape for more information.[14]

6.4. App Store Operators should support App Developers in implementing effective supply chain management, such as by monitoring common third-party libraries and services and sharing relevant information, highlighting potential threat vectors across multiple apps.

NCSC has published Supply Chain Security Guidance which is designed to help organisations establish effective control and oversight of their supply chain. We encourage organisations that are part of the app ecosystem to adopt this guidance (where relevant).

7. **Provide clear feedback to Developers -** Primarily applies to: App Store Operators

7.1. When an app submission is rejected, the App Store Operator should provide consistent and actionable feedback, justifying the rejection of the app and making clear what elements would need to change in order for the app to be accepted.
7.2. When an App Store Operator removes or makes an app unavailable for security or privacy reasons, they shall notify the Developer of this step, and provide feedback explaining the reasoning behind the decision. Operators shall take into consideration that the feedback they provide does not help malicious actors.

8. **Ensure appropriate steps are taken when a personal data breach arises -** Primarily applies to: App Developers and App Store Operators

8.1. If a Developer or App Store Operator becomes aware of a security incident in an app which involves a personal data breach, they should inform other relevant stakeholders including App Developers, App Store Operators, and library/SDK Developers.
8.2. Developers shall assess the impact of said incident and follow appropriate steps set out under data protection law.[15]
8.3. When a personal data breach occurs through an app, the Developer shall inform affected users and signpost instructions for users to protect themselves.
8.4. When Operators are notified about a personal data breach in an app, Operators should consider whether the app should be made unavailable to users.

[14] DCMS commissioned mapping by Copper Horse Ltd, 'Application Security Mapping', November 2022. https://appsecuritymapping.com/
[15] ICO guidance on this can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Annex A: UK Data Protection Law

App Store Operators and App Developers shall comply with the broader requirements of data protection law, including the Data Protection Act 2018 and UK General Data Protection Regulation, but the sections below have been added to highlight requirements of particular relevance to the Code of Practice.[16]

Controllers and processors

- Understanding your role in relation to the personal data you are processing is crucial to ensuring compliance with the UK General Data Protection Regulations (GDPR) and the fair treatment of individuals.
- Your obligations under the UK GDPR will vary depending on whether you are a controller, joint controller or processor.
- The ICO has the power to take action against controllers and processors under the UK GDPR.
- Individuals can bring claims for compensation and damages against both controllers and processors.
- You should take the time to assess, and document, the status of each organisation you work with in respect of all the personal data and processing activities you carry out.
- Whether you are a controller or processor depends on a number of issues: The key questions are; 1.) who determines the purposes for which the data are processed (the "why") and 2.) the means (the "how") of processing?
- Organisations that determine the purposes and means of processing will be controllers regardless of how they are described in any contract about processing services.

Relevant UK GDPR articles: 4(7), 4(8), 5(1), 5(2), 26, 28-36
ICO guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

Security

- A key principle of the UK GDPR is that you must process personal data securely by means of 'appropriate technical and organisational measures'. This is the 'security principle'.
- Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.
- You also have to take into account additional requirements about the security of your processing and these also apply to data processors.
- You can consider the state of the art and costs of implementation when deciding what measures to take, but they must be appropriate both to your circumstances and the risk your processing poses.
- Where appropriate, you should look to use measures such as pseudonymisation and encryption.
- Your measures must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data you process within them.
- The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.

[16] ICO Glossary of Terms: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-fee/glossary/

- You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.

Relevant UK GDPR articles: 5(1)(f) and 32
ICO guidance:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/
https://ico.org.uk/for-organisations/security-outcomes/

Data protection by design and default

- The UK GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is 'data protection by design and by default'.
- In essence, this means you have to integrate or 'bake in' data protection into your processing activities and business practices, from the design stage right through the lifecycle.
- This concept is not new. Previously known as 'privacy by design', it has always been part of data protection law. The key change with the UK GDPR is that it is now a legal requirement.
- Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the UK GDPR's fundamental principles and requirements, and forms part of the focus on accountability.
- Data protection by design is particularly important in the context of mobile apps; for example, understanding the various software components involved, how these relate to the personal data the app processes and what steps you need to take to build in privacy from the design stage.

Relevant UK GDPR articles: 25
ICO guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

Personal data breaches

- The UK GDPR introduces a duty on all organisations to report certain personal data breaches to the ICO. You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority or the affected individuals, or both.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify the ICO.

Relevant UK GDPR articles: 33, 34, 58, 83
ICO guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Transparency

- You must be clear, open and honest with people from the start about how you will use their personal data.
- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.
- You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. The ICO calls this 'privacy information'.
- You must provide privacy information to individuals at the time you collect their personal data from them.
- If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.
- There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.
- The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- It is often most effective to provide privacy information to people using a combination of different techniques including layering, dashboards, and just-in-time notices.
- User testing is a good way to get feedback on how effective the delivery of your privacy information is.
- You must regularly review, and where necessary, update your privacy information. You must bring any new uses of an individual's personal data to their attention before you start the processing.
- Getting the right to be informed correct, can help you to comply with other aspects of the GDPR and build trust with people, but getting it wrong can leave you open to fines and lead to reputational damage.

Relevant UK GDPR articles: 5(a), 12-14
ICO guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/ and https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

Annex B: Making a referral to the ICO

The Information Commissioner's Office (ICO) has responsibility for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18), the Freedom of Information Act 2000 (FOIA), the Privacy and Electronic Regulations 2003 (PECR), the Network and Information Systems Regulations 2018 (NIS), and the Environmental Information Regulations 2004 (EIR).

Should you believe that you have information, or evidence that indicates an organisation or individual has poor app security and/or privacy practices in place, you can refer your concerns to the ICO. The ICO will consider your referral to establish if the matter should be developed further.

Potential outcomes include:
After assessment, your referral may be submitted to an ICO department for further consideration and action as deemed appropriate. The ICO will record your referral and log the matter for future reference.

The referral procedure outlined in this code does not apply to Data Protection, FOI and EIR complaints, nuisance calls and messages, and complaints about cookies. Information or how you can make a complaint in relation to these, and other information rights issues can be accessed via the ICO website.

It is also important to note that the above procedure does not apply to the following:
Personal data breaches under Freedom of Information and Data Protection GDPR or DPA 2018, which must be considered and where relevant reported to the ICO as outlined in the following guidance: Protected Disclosures to the ICO - A whistleblower may be making a qualified protected disclosure under the Public Interest Disclosure Act 1998 (PIDA) or the Public Interest Disclosure (Northern Ireland) Order 1998. The ICO has produced guidance on whether an individual may be afforded protection under these pieces of legislation. However, the ICO cannot advise whether a disclosure would be protected, and the individual must satisfy Voluntary Code of Practice for all app store operators and developers themselves that this would be the case through seeking their own independent legal advice.

If you believe you have identified a potential app related security or privacy concern, please forward your concern to the ICO using the following email address: IH@ico.org.uk We would encourage you to provide as much detail as possible and to include your contact details - if you are comfortable in doing so. Any evidence, which supports your concern, should be included in your referral.

As part of any assessment process, the ICO may need to contact you to seek further information but will not routinely enter into any correspondence with you regarding your referral. It is important that your referral to the ICO remains confidential, subject to any other reporting obligations. This is to ensure that any future potential investigation we may undertake is not compromised.

Annex C: Further information

Protecting the mechanism for allowing enterprise app stores

App stores can offer organisations mechanisms to set up private app stores, curated for their employees. Thus far, this has predominantly been offered by some operators for mobile and desktop devices. App Store Operators shall ensure that their platform is protected from malicious actors who may use the mechanism for creating enterprise app stores as a backdoor into their customer's organisation or as a mechanism to distribute malicious apps to consumers. If an organisation intends to create an app store that involves processing employee data, it shall be required to implement security measures which are required under data protection law to ensure that employee data is protected.[17]

[17] See for example, UK GDPR Articles 5(1)(f), 24, 25 and 32