COVID-19 Contact tracing: data protection expectations on app development

Purpose

This document sets expectations on how contact tracing solutions may be developed in line with the principles of data protection by design and default, and includes a series of best practice recommendations.

Audience

The expectations outlined below have been developed to support technical design teams (architects, product managers, designers, engineers) in understanding how to apply information rights and data protection by design and default approaches to the technical development lifecycle of COVID-19 contact tracing apps. Risk management professionals, including those working in privacy and data protection, information security, compliance and operational risk may also benefit from this document.

Scope

This is a discussion document that has been provided by the Information Commissioner's Office (ICO) to supplement ongoing conversations between the ICO and NHSX regarding its planned contact tracing app and associated activities.

The ICO recognises the importance of the app as one part of a package of measures in the UK's fight against the COVID-19 pandemic, while recognising that an app cannot be used to address all the challenges of supporting citizens appropriately, especially those who don't have smartphones, or members of society that may be vulnerable or disadvantaged.

Our role as an independent regulator is to act in the public interest, and our approach has always been to be a pragmatic and proportionate regulator. We appreciate the effort NHSX has made to maintain a dialogue with the ICO whilst having to move at speed in addressing complicated technological and epidemiological challenges.

This document provides further detail on our understanding of privacy and data protection considerations around contact tracing apps, and our articulation of best practice recommendations in this area.

For the purposes of this document, a contact tracing app is considered to be a mobile application which functions to notify users when they have been in recent proximity with another user who has confirmed symptoms of COVID-19 (whether via official or self-diagnosis). It uses 'proximity data' which consists of identifiers broadcast by pairs of devices that have been close to each other (possibly including how close they were, and for how long). One typical approach involves generating identifiers and the matching process taking place on-device, while another involves these processes being driven by the backend infrastructure. In popular parlance these have become known as 'decentralised' and 'centralised' approaches, although both may include a server.

Any additional functions or features, such as recording/communicating the location in which contact has taken place, or collection of additional data that may support other functions (such as epidemiological research) is considered beyond the core functionality needed for contact tracing via proximity detection, notwithstanding the value additional functionality may offer medical professionals in combatting COVID-19, and will need to be assessed on a case-by-case basis.

This document has been drafted to support our ongoing conversation with NHSX. We appreciate this is a fast moving project; we are happy to discuss any aspect of this document with NHSX and its stakeholders.

Compliance with data protection law

Any assessment of the data protection implications of a contact tracing app must be undertaken on a case-by-case basis and therefore the specific implementations may require additional measures and considerations beyond the scope of these recommendations.

The ICO considers that a Data Protection Impact Assessment (DPIA) is required for contact tracing solutions prior to implementation, given that the processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA may also need to iterate over time, particularly in accordance with any Product or Project roadmaps and functionality/scope updates and releases. The principles and expectations below therefore do not replace a DPIA, however they can be used to support its completion.

Principles

The following principles should guide the development of your contact tracing app. They are linked to the core principles and provisions of data protection law and are designed to support your design decisions and key considerations for documentation, accountability and auditability.

You should consider how to apply these principles throughout the lifecycle of the contact tracing app or service.

1. **Be transparent about the purpose**: Explain if the purpose is only proximity notification or if the purpose is broader, or is likely to expand in accordance with any development roadmap. Explain any additional purposes clearly and make sure you assess the necessity and proportionality of the processing the app undertakes. Ensure your considerations address all relevant parties - for example, build core requirements into your notices, user experience (UX) design and other appropriate in-app transparency mechanisms, but also provide more detailed information about your app's development outside of the app itself.

2. **Be transparent about your design choices:** Be clear about the system's architectural design decisions, how they were made and what risks the approach poses to individual rights. Use the least privacy intrusive approach possible to achieve your purpose and ensure you justify the design choices you make. Make the service requirements and objectives available to users and other parties.

3. **Be transparent about the benefits:** Be clear about the benefits and outcomes your app seeks to achieve, from both your perspective and that of the user. Where benefits for different parties may be the subject of tension, ensure that you are clear on how you have managed these in the data protection context. As part of assessing necessity and proportionality, clearly define these parties and clarify how your solution addresses each in line with data protection requirements.

4. **Collect the minimum amount of personal data necessary**: Minimise the data your solution processes to that which is necessary to achieve your purposes. Begin by considering whether you can generate and match identifiers on-device. Where this approach is available, feasible, and enables you to achieve your purposes, then you should use it. If you decide to use an alternative approach, you must be able to explain why it is necessary to do so, as well as the steps you will take to ensure you will not introduce unnecessary risks to the user. Contact tracing apps should only collect or otherwise process information that is required for the core purpose (e.g. excluding location data, other device identifiers beyond any that are strictly necessary for the purpose, and personal data such as user account information, etc.). As noted above the collection and processing of personal data for other purposes will need to be assessed on a case-by-case basis.

5. **Protect your users:** Ensure your app uses pseudonymous identifiers, which are renewed regularly as appropriate to your purposes, and are

generated in such a way that risks of reidentification and tracking are reduced.

6. **Give users control:** Ensure your users can exercise their rights via your app, where these rights apply. Provide controls while onboarding and during use, e.g. via a dedicated privacy control panel or dashboard.

7. **Keep data for the minimum amount of time, and, where appropriate, ensure the user has control over this:** Store data for the minimum amount of time necessary for your purposes. Explain what that period will be and why. Avoid gathering, augmenting or correlating user data without express permission.

8. **Securely process the data**: Apply appropriate cryptographic/security techniques to secure the data, both at rest (in servers and apps) and in transit (between apps and the server). Ensure confidentiality, integrity and availability has been engineered into the service.

9. **Ensure the user can opt in or opt out without any negative consequences:** App use, from installation to sharing of information, should be voluntary with no negative consequences for individuals if they do not take action. Functions should be de-coupled to allow the user to benefit from one function without being compelled to provide data for other functions..

10. **Strengthen privacy, don't weaken it:** Ensure the design of the app does not introduce additional privacy and security risks for the user (for example requiring the phone to be unlocked, or location to be identified).

Consider how to test functional and non-functional requirements or use cases and user journeys that are being developed against these principles on a continuous development basis – for example including testing against these principles to determine the impact on the user, as part of any sprint planning and retrospectives.

Best practice recommendations

The following best practice recommendations are grouped under a development lifecycle. While these (and any references to document types) may not align with the process your organisation uses, the key point to recognise is that there are data protection obligations during the ideation and design phase, when onboarding and operating any service, when iterating any service, and when decommissioning any service.

It may also be the case that different parties may be responsible for specific aspects of the processing. For example, developers of a contact tracing app may only be responsible for collecting information from the user, while a different party may be responsible for its analysis. However, even in these circumstances it is incumbent upon the developers of a contact tracing service, particularly where acting on behalf of a public health authority, to take steps to ensure that:

- data is not used for analysis or for other purposes in ways that may detrimentally affect information rights and privacy; and
- data use does not lead to other significant decisions about the user without the user's permission or understanding that this is the case.

This responsibility can be met in part through the design of privacy protections into the technical approach of the service, including clear privacy and security objectives and controls, and by ensuring that all involved parties are clear on their respective responsibilities.

While this document comprises good practice recommendations, from a design perspective the key words 'must', 'must not', 'required', 'shall', 'shall not', 'should', 'should not', 'recommended', 'may' and 'optional' are to be interpreted as described in RFC 2119. These are used to aid translation of the requirements of data protection law.

Scope, requirements and design

1. Contact tracing app initiatives must describe the objectives they seek to achieve. This must include articulating if the benefit is directly for the user and/or if the benefit is for a broader societal purpose. Being transparent on the objectives, requirements and future plans will help to build trust amongst all stakeholders, especially users.

    a. Within any product roadmap or description of objectives and requirements (epics, stories) articulate how the user will understand, e.g. through the experience and interface design, that their privacy has been engineered into the project. Make sure your design choices enable you to clearly tell your users about any uses of their data that may be unexpected or could

have significant effects on them, and if there are any residual privacy risks.

b. Publish the product roadmap and user needs/journeys, as well as any supporting documentation, code or collateral that explains the requirements, scope, approach and risk management controls.

2. Contact tracing apps must exclude further processing for purposes unrelated to the primary aim, as explained to the user. The purposes must be specific enough to exclude other unrelated purposes. Personal data beyond that necessary for contract tracing purposes must not be processed merely because it may become useful in the future.

    a. Describe how you have assessed what the minimum amount of data (and types of data) are that you have to collect and process to enable proximity detection.

    b. Detail the technical and design controls you will put in place to ensure data collection doesn't expand during any further development without user engagement.

3. Contact tracing apps may develop roadmaps for additional functionality involving personal data; in such cases, a documented re-assessment of the data protection implications is required.

    a. Describe the product roadmap in a way the user can understand, both in general and with specific reference to any implications for their privacy rights. Ensure any technical or policy decisions are explained to the user in an accessible way.

    b. Describe as part of the development of the roadmap how features could lead to privacy challenges and what control measures have been considered.

    c. Consider how to functionally decouple features. Ensure users are not compelled to share additional data to access existing features or new features, and to allow any features to be rolled back or deprecated.

4. Processing of personal data may be based on consent or an alternative lawful basis where this is more appropriate, such as performance of a task in the public interest (particularly where an app is developed by or on behalf of a public health authority). For the latter, the processing must be necessary; if you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply. The voluntary use of an app does not mean that processing has to be consent-based. However, where the processing is based on

consent, that consent must be collected in line with the requirements of data protection law.

5. The consent requirement of Regulation 6 of the Privacy and Electronic Communications Regulations 2003 ('PECR') does not apply in relation to storage of information, or access to information stored, on user devices where this is strictly necessary for the provision of a contact tracing service the user requests (e.g. exchange of proximity data and receipt of push notifications). Where storage and access is not strictly necessary, valid consent must be obtained. Consideration of this requirement must take place on a case-by-case basis.

    a. Consider how to separate out storage/access to user devices that is strictly necessary from that which is not, where this applies. Where strictly necessary, establish how you will obtain prior consent from the user.

6. App developers should break down the processing operations involved in their proposed contact tracing apps into their individual components and assess necessity and proportionality, the lawful basis and user impact, of each one. Design should incorporate the ability to functionally decouple each discrete process.

    a. Consider how to offer proximity notification to a user as a minimum product feature, with any other features layered on top with simple mechanisms for the user to opt in or out without feeling compelled.

    b. Consider architecting your data model and data pipelines to allow clear separation between processing that is taking place, and to clearly link the functional (experience) layer with the data and processing enabling it.

    c. Document and demonstrate how you have achieved this, and what technical and policy controls have been put in place to validate the separation of processing and experience.

7. Source code must be open to allow scrutiny and review.

    a. Consider how you will implement established code management and publication principles, such as those in the GDS Service Manual (or other relevant guidelines as appropriate).

8. The design stage must consider the most appropriate architectural design to achieve the purpose from the user's perspective. As a general rule, the decentralised approach allows most readily for best practice compliance with the data minimisation principle.

a. How might you separate out elements of the service that rely on personal data so that they are developed and deployed using a decentralised model, especially if this is sufficient to achieve the core purpose of proximity notification?

b. As the technology and modelling capability of end point devices evolves, how might you transition the product roadmap from a centralised approach to a decentralised approach - where the decentralised approach offers greater privacy protections?

9. A DPIA must be completed prior to the commencement of the processing, and updated at all relevant stages of your app's development. Where a DPIA identifies risks to users that you cannot mitigate, you must submit it to the ICO for prior consultation. The ICO will expedite the consultation process for any such DPIA we receive.

    a. Consider how to ensure the technical development lifecycle and product updates trigger the right thresholds for refreshing the DPIA, and what you can do to build this into the sprint cycle.

Development, deployment, onboarding and operation

10. Contact tracing apps should adopt a user centric design approach, even if the circumstances of the current pandemic mean the development lifecycle is compressed.

    a. Consider how to test for different user needs, taking special consideration for different societal groups that may be vulnerable, disadvantaged, or require accessibility support.

    b. Consider how to build technical and policy controls to ensure users, especially children, vulnerable adults, and other at risk members of society are treated fairly.

11. Contact tracing apps must not involve or require the processing of location data, or the tracking of the location of users either directly or by inference. Proximity data must be used; as contact tracing apps do not require location data to fulfil their purpose, any processing of this data is therefore not necessary and poses additional privacy risks. The app and backend infrastructure must not directly identify users or process other information from the device such as call logs, device identifiers (beyond any that are strictly necessary for the purpose), IP addresses and any other information (including personal data), as this is not required for contact tracing purposes.

12. An interoperability framework may be considered (e.g. for efficient notification of users travelling outside the UK). Data processed must be for the sole purpose of interoperability and must be limited to that

which is strictly necessary for the purpose and be undertaken in accordance with applicable law.

a. Consider how your technical and design controls will mitigate the risks of personal data being shared with other third party app controllers.

b. Ensure the app only collects data transmitted by interoperability equivalent applications.

13. Use of coding libraries, frameworks, APIs, SDKs and other software components, including those within the mobile operating system, must be understood and clarified. Collection of data by third parties for other purposes must be avoided.

14. In general, information should remain on the user's device as far as is reasonably practicable. Backend infrastructure should only collect that which is strictly necessary in the context of the functions it provides.

a. What data retention technical controls are in place to manage data stored locally on the device and centrally?

15. Proximity data must comprise pseudonymous identifiers that are refreshed at regular intervals as appropriate for the purpose of the processing, as a means of limiting the risk of reidentification and of tracking individuals.

a. These pseudonymous identifiers should be generated on the device if possible. If they are generated by the backend infrastructure, you must explain why you have decided this is necessary and how you have assessed the risks of this approach.

b. Ensure that any underlying smartphone operating system APIs, e.g. for processing data via Bluetooth, are used in accordance with relevant developer documentation, app store guidelines and terms of use.

16. Retention periods must relate to the purpose of the processing and must not be disproportionate. They should be based on scientific or epidemiological considerations (e.g. period of infection). Personal data must only be processed for the duration of the COVID-19 crisis. Afterwards, as a general rule, it should be erased or anonymised. The purposes for the use of anonymised data (e.g. future research value) must be documented. Appropriate measures must be in place to address the risk of re-identification.

a. Where a research purpose may deliver value in the public interest, any such use case should be assessed in the DPIA and discussed with the ICO.

17. Backend infrastructure must process the minimum amount of personal data necessary. As a general rule, backend infrastructure should only collect identifiers after the user has taken a voluntary action, and should only process identifiers for the time needed to inform other users. If the specifics of the solution mean that this is not possible, justification shall be documented along with the additional measures to ensure data minimisation is achieved. Data in server logs must be minimised in line with data protection law (i.e. no identifiers should be included).

18. Backend infrastructure must be secured with appropriately robust and state of the art cryptographic/security techniques. Data sent to the backend infrastructure must be transmitted over a secure communications channel. Appropriate security measures must be applied to secure any exchange of data between the backend and a user's device, and between user devices.

19. Apps and servers must authenticate with each other at the transport layer, and other security protections must be considered to ensure the exchange of data protects the privacy of the user.

20. If self diagnosis is necessary, appropriate measures should be in place to mitigate the risks of false positives and the impact on the rights of those notified. For reporting test results, a separate authentication must be made e.g. a one-time password linked to the medical professional that made the diagnosis.

21. Processes must be in place to test the effectiveness of the security measures as well as to respond to any security issues, with actions taken where necessary, to ensure the security of the processing is maintained. Appropriate consideration and action must be taken to ensure common security threats are assessed and mitigated, both in respect of the backend infrastructure and the mobile app environment.

22. App developers should break down the processing operations involved in their proposed contact tracing apps into their individual components and assess necessity and proportionality, the lawful basis, and the user impact of each one. Design should incorporate the ability to functionally decouple each discrete process.

    a. Consider how to offer proximity notification to a user as a minimum product feature, with any other features layered on top with simple mechanisms for the user to opt in or out without feeling compelled.

23. Processes involved in matching identifiers must be developed to mitigate risks of false positives and false negatives. Any algorithms or

models deployed must be auditable and subject to regular review (e.g., by independent experts) and any necessary changes.

24. The identities, roles, and responsibilities of all parties that process personal data as part of the contract tracing solution must be clarified, documented, and made clear to the user.

25. Users must be provided with clear and comprehensive information about the data your app processes before the processing takes place. Privacy information may be made available in different ways, as appropriate to the circumstances and the reasonable expectations of individuals - including app store information, information within the app itself, user interface design, just-in-time notifications, etc.

    a. How might you design simple and accessible engagement moments to explain to the user the purpose and outcome from the use of their data?

26. Collection of personal data relating to health shall be allowed only where the processing is either based on explicit consent, is necessary for reasons of public interest in the area of public health, is for health care purposes, or is necessary for scientific research or statistical purposes.

27. Apps must be designed in such a way as to enable users to access their rights as set out in the GDPR, including rights of access, erasure, restriction and rectification, as applicable.

28. Backend infrastructure must not attempt to identify infected or potentially infected users. Access to data on the central server must be restricted to authorised individuals.

    a. Develop technical, procedural and policy controls to avoid data sharing outside the operational boundary of the PHA.

    b. Limit APIs, database analytics or other data exchange mechanisms to parties that are directly supporting proximity notification delivery. Where access is required for epidemiological reasons for trend/pattern analysis then consider earlier points about purpose limitation and refreshing the DPIA.

Decommissioning

29. Assessment must be made about how the functionality of the app and the backend infrastructure, and any data processed, will be deprecated once the pandemic ends. This should be made at the design stage, or alternatively may take place as part of development roadmaps.

a. How will you incorporate decommissioning into your roadmap?
b. Consider whether your app/infrastructure should be designed to dismantle itself once the crisis ends and people cease using the app, or whether specific processes are necessary.
c. What steps will be taken to erase or anonymise the data once the contact tracing purposes are no longer relevant?
d. How will you ensure your decommissioning process is independently verifiable and auditable, including to the ICO?

30. Decommissioning considerations should cover not only the 'general' retirement of the service as described above, but instances where an individual ceases to use the application.

    a. Consider how you will make the decommissioning a matter of public record, and how you will inform your users (e.g. by providing messages to delete the app from their device).

31. The decommissioning process must consider the possible future use of personal data and/or any models derived for legitimate research purposes (e.g. developing responses to future outbreaks, development of models or inferences to understand epidemiological impact). Any consideration of use of data for research purposes is undertaken in accordance with data protection law, with appropriate safeguards in place.

32. Consideration should be taken after, or as part of, the decommissioning process to analyse the privacy issues raised, how risks were managed, and what lessons can be learned for the future. This can act as an overarching safeguard.

    a. Consider undertaking this analysis through relevant governance groups in order to fully understand the efficacy of the approach.

The ICO will keep these recommendations under review, taking into account how the COVID-19 pandemic develops and the particular proposals under development to respond to the crisis. The ICO is open to any conversation regarding these recommendations in order to help technical teams build data protection by design and default into their service, because this is the best way to promote trust and confidence in any solution.