An Coimisiún um Chosaint Sonraí
Data Protection Commission

COVID Tracker Ireland App

Data Protection Impact Assessment Review

June 2020

Contents

1. Introduction

This document reviews the Data Protection Impact Assessment (DPIA) submitted to the Data Protection Commission ("the DPC") by the HSE and Department of Health ("the Data Controllers") in relation to the processing of personal data by the proposed COVID Tracker mobile app ("the App"). The review is provided to the Data Controllers on an informal consultation basis and without prejudice to any further assessment or exercise of the DPC's functions and powers, including but not limited to the handling of complaints should such arise.

Article 35(7) GDPR sets out that the minimum requirements of a DPIA shall be:

(a) A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
(b) An assessment of the necessity and proportionality of the processing operations in relation to the processing
(c) An assessment of the risks to the right s and freedoms of data subjects referred to in paragraph 1; and
(d) The measures envisaged to address the risks, including safeguard, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

This review examines the DPIA in terms of each these four requirements as well as adherence of the proposed processing to the principles of data protection and wider compliance with the data protection legislative frameworks.

2. Processing operations

Sections 3 and 4 of the DPIA[1] respectively set out an overview of the processing operations, and the scope of the processing to be carried out using the App. The overview of processing details the App's functions and purposes, and the systems that process data, while the scope of the processing documents the data that will be processed in each case.

These sections set out the processing operations and the data necessary to achieve the purposes outlined in the Overview (Section 1)[2] in a systematic manner, as required under Article 35(7)(a) GDPR.

[1] DPIA pp 3-12
[2] DPIA p2

3. Necessity and Proportionality

In addition to the identification of an appropriate legal basis, the processing of personal data must be justified on the basis of necessity and proportionality. The DPIA provides an analysis of the application of these principles to the various functions and purposes of the App in Section 7.4[3], with reference to both the stakeholder engagement that has been undertaken and the research literature referred to in Section 6.4[4].

In relation to the contact-tracing purpose, the DPIA establishes a need for the use of an app-based contact tracing solution due to the over reliance of manual tracing upon memory, and the need to increase both the completeness and speed of tracing to a level that is not achievable via solely manual means. The DPIA states that "the App is being developed because using mobile technology can improve the speed and accuracy of manual contact tracing".[5] It should be noted that this assertion is somewhat speculative due to the novelty of the technology and the unproven nature of its effectiveness.

The DPIA states that measures to avoid the disproportionate processing of personal data in relation to contact tracing include its voluntary nature, the optional provision of phone numbers, and the controller's decision to not collect and process device generated location data.

The COVID Check-in function is stated as justifiably necessary on two grounds. Firstly, it adds "syndromic surveillance" to the tools available to the public health authorities in conducting modelling of the spread of the virus, which will improve the quality of information available in making policy decisions around virus management. Further information on the use of syndromic surveillance is provided in Appendix C of the DPIA.[6] Secondly, it is stated that the COVID Check-in function acts as an aide-memoire for users to monitor their own symptoms and take decisions around their own healthcare needs.

In terms of proportionality, the processing for the COVID Check-in function is determined to exert limited interference with individuals' rights as the information is obtained only in a pseudonymised form by the HSE and transferred anonymously to the CSO for statistical analysis.

The News and Information function is considered necessary as it provides a range of information on national measures to combat the virus in a convenient and reliable manner. In terms of proportionality, it is considered that this function has little impact on a user's rights as no personal data is processed.

[3] DPIA pp 17-20
[4] DPIA pp14-15
[5] DPIA p2
[6] DPIA p34

The collection of app metrics data is considered necessary to monitor the effectiveness of the App and to give public health authorities insights into its functioning. The data minimisation and anonymisation techniques applied to data relating to the COVID Check-in function are also applicable in this context.

Recommendation: As this application of technology is essentially untested it will be necessary to ensure that the App continues to process personal data in a manner that meets the requirements of necessity and proportionality. For example, if the population uptake of the App fails to reach a sufficient threshold, the necessity and proportionality of continuing to process the data of those who do use it should be reconsidered. It is noted that this is one of the specific tasks of the Governance Committee – "ensuring that effective monitoring is in place to assess the ongoing efficacy of the App in contributing to the HSE COVID-19 response"[7]. Similarly, the processing of COVID Check-in data should be discontinued if it is not proving to be effective in its stated aim of assisting public health authorities with virus modelling.

Both uptake and other metric factors should be clearly defined and understood so that effectiveness is measurable and reliable, and contributes to the decisions the Governance Committee is required to undertake.

4. Assessment of Risk and Risk Mitigation

Appendices E and F of the DPIA[8] respectively set out the identified and mitigated risks identified with the project.

The risks posed by the processing are set out clearly and highlight identified threats related to the fundamental fitness for purpose of the App, potentially unlawful processing, security issues, and potential technical flaws due to the generally untested nature of the technology. The mitigating factors in each case are also set out clearly and in a considered fashion, and no incidence of high risk is considered to remain following the implementation of mitigating factors. However, it is not clear in every case where responsibility will sit for ensuring the implementation of mitigation measures.

It is noted that in this section of the DPIA the DPOs of both data controller organisations have been consulted on the DPIA[9], as required by Article 35(2) GDPR, and have given their opinion that the identified risks are satisfactorily reduced subject to controls. One of the DPOs observes the need for control measures to be subject to ongoing review, with which the DPC agrees.

[7] DPIA p27
[8] DPIA pp37-53
[9] DPIA pp25-26

Recommendation: The novelty of this type of processing and the technology that is involved create a potential difficulty in verifying the effectiveness of certain mitigating measures. It is clear that close monitoring to understand effectiveness of the App and its processing of data will be required subsequent to its launch to achieve this. The general oversight role of the Governance Committee in this area is noted. However, it is recommended that specific delegation of responsibility be made for each risk and its mitigation to help ensure that issues are not overlooked.

The wider data protection risks that are presented in the process of developing apps should be clearly addressed, as well as the specific risks related to the specific processing operations of the COVID Tracker app. The necessity to develop this app over a short period of time, combined with the multiple actors operating on the project, would suggest a need for very thorough testing and validation processes. The Article 29 Data Protection Working Party's Opinion 02/2013 on apps on smart devices addresses many of these issues.

GDPR Article 25 also obliges data controllers to put in place effective and integrated measures and safeguards that are designed to implement data protection principles and to protect the rights of data subjects. This is to take place at the time of the determination of the means for processing and at the time of the processing itself, and needs to be demonstrable and maintained over time and appropriate to the nature, scope and context of processing.

5. Article 5 Principles

(a) Lawfulness, fairness and transparency

Lawfulness will be considered in the next section – Lawfulness of Processing, with reference to Articles 6, 7, and 9 GDPR.

Fairness

The principle of fairness in relation to the processing of personal data means that data should be processed in ways that data subjects can reasonably expect, and not processed in a manner that causes adverse effects to data subjects. The DPIA states that the use of the App is in accordance with the HSE's functions as prescribed by Section 7 of the Health Act 2004 and as a response to the COVID-19 pandemic to protect the public health.[10] The other data controller of the App, the Department of Health, provides the project with "strategic leadership" and ensures that, "government policies are translated into actions and

[10] DPIA p15

implemented effectively".[11] The stated purposes of the processing of data using the App are in line with the functions and legitimate aims of the two data controllers.

In the processing of medical and healthcare data, the principle of fairness can be considered as related to the role of medical ethics. The DPIA states that the App has also been subjected to an ethical review by Science Foundation Ireland and will be reviewed by the Pandemics Ethics Advisory Sub-Group of the National Public Health Emergency Team (NPHET). The HSE's National Patient Forum, comprising patients, family members, carers, and patient safety and disability advocates, has been consulted on the App for feedback. While this stakeholder engagement will be considered in greater detail later in this document, it assists in demonstrating that the processing of personal data can be considered to be fair.

Transparency

The principle of transparency means that any information or communication relating to the processing of personal data is easily accessible and easy to understand, using clear and plain language. Transparency around data protection will be key to the success of the App, as widespread usage by the population is required for digital contact tracing to be an effective tool in combatting COVID-19. The provision of clear and accurate information that leads to comprehension on the part of users is fundamental to building the public trust necessary to achieve the required buy-in.

The necessary information to be provided to data subjects, at the time when personal data are obtained, is set out in Article 13 GDPR. It is the responsibility of the controller to ensure that this information is provided in a concise, transparent, intelligible and easily accessible form. According to the DPIA, this information is provided via a Data Protection Information Notice within the App, accessible from each page that requests information from the user and in the app settings.[12] The release of the App will also be accompanied by the publication of a product brochure, "Introducing Ireland's Pandemic Response App" and a media campaign to promote awareness and understanding of the App and its purposes.

It is noted that it is the intention of the data controllers to publish the source code and the DPIA and related documents prior to the release of the App.[13] Putting this material into the public domain will enhance transparency, allowing civil society groups and other interested parties to examine and comment on any data protection implications.

As the HSE and Department of Health are joint controllers, it will be necessary for an arrangement or agreement to be put in place that transparently sets out their respective compliance responsibilities. This is of particular importance in the designation of

[11] DPIA p2
[12] DPIA p6
[13] DPIA p24

responsibility for facilitating the exercising of data protection rights. The need for such an arrangement is recognised in the DPIA[14] and this arrangement, or at least an essential summary thereof, should be published.

Section 5.5 of the DPIA on Accessibility[15] states that user experience of the App has been tested in behavioural studies and that further accessibility testing will be conducted following release to inform any app enhancements or updates. This section also refers to consideration of providing support materials in commonly used languages, as well as the Irish and English languages. The DPC recommends that this be done in the interests of making transparent information available to all users.

The foregoing suggests that the data controllers will make all necessary efforts to meet their transparency obligations.

Recommendation: In the interests of transparency, the App source code and the DPIA and related documents (including details of the respective responsibilities of the Joint Controllers) should be published as soon as possible and well in advance of the release of the App.

(b) Purpose Limitation

This principle requires that personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. (See also the "legal basis" section below)

The App is described in the DPIA as having two purposes designed to "support and augment the HSE's COVID-19 pandemic response efforts". [16] These purposes are set out in the following terms:

Purpose 1: To support the national public health response to COVID-19 by

a) Enhancing the existing HSE contact tracing operations
b) Monitoring and mapping the spread of COVID-19 symptoms

and

Purpose 2: To support members of the public during the COVID-19 crisis by

[14] DPIA p2
[15] DPIA p13
[16] DPIA p2

a) Providing COVID-19 related news, information, and national updates on the App
b) Storing a personal record of symptoms on the App

These are intended to align with the with broader pandemic response activities of the two data controllers so that the processing of personal data using the App can be considered to be in pursuit of their legitimate purposes.

The description of the processing of personal data in relation to the Contact Tracing function of the App, and the Symptom Checker make it clear that these purposes can also be considered sufficiently specific.

The terms of reference of the COVID Tracker App Governance Committee are set out under Appendix A of the DPIA and include oversight responsibilities that relate to ensuring adherence to the principle of purpose limitation[17]. In particular, the following apply:

- Overseeing that the functioning and the use of the app is within the purposes of the app as set out in the document.
- Overseeing any enhancements of the mobile app and ensuring that they are in line with the app design principles set out in this document (the DPIA).
- Overseeing that the app processes data in line with the DPIA and that the data controllers keep the DPIA up to date and public.

While the functioning of the Governance Committee is given further consideration later in this document, its role in relation to governing purpose limitation and the prevention of any "scope creep" is noted as an indication that this principle, and adherence to it, appears to have been given due consideration in the development of the CTI App.

(c) Data Minimisation

Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be met by other means. It is noted that efforts have been made at various stages of the App design process to ensure adherence to this principle.

As set out in the DPIA, the design of the App follows the so-called 'decentralised' model[18], which aims at keeping to a minimum the personal data that is transferred to public health authorities by contact-tracing apps. The processing of personal data is carried out by the app itself, on the user's device, to the greatest extent possible.

[17] DPIA p27
[18] DPIA p12

According to the DPIA, the data to be processed for each function of the app has been subjected to a data minimisation test[19] and determined to be strictly necessary to achieve the stated purposes.

It is understood that each of App's functions will operate independently and there will be no cross-pollination or linkage of personal data between the App's functions, even in circumstances where a user decides to activate all functions. This should be made clear to users at the point of installation of the App on their device and making choices on use of functions.

The processing of personal data using the app employs pseudonymisation to ensure that identifiable information is not processed unnecessarily. The user's IP address, which is the only direct identifier obtained by the HSE through the App's core functions, is only processed for essential networking reasons and cannot be used to in combination with other data to identify individual users.[20] This identifier is also removed from symptom check-in data prior to transfer to the CSO for statistical analysis. According to the DPIA, this means that the CSO receives anonymous data.[21]

The foregoing measures, in combination with the oversight responsibilities of the Governance Committee, suggest that due consideration has been given to ensuring adherence to the principle of data minimisation in the design of the App and subsequent to its release. It is emphasised, however, that data which is shown not to be effectively anonymised, remains personal data and subject to the requirements of the GDPR, including having a lawful basis for the processing.

Recommendation: The methodology used in the data minimisation test described in Section 4.6 should be carefully explained. Where data is determined to be anonymised by the data controllers, this determination should be subject to demonstrable and robust testing across its lifecycle, to ensure that no reasonable likelihood of re-identification, inference or singling-out remains.

In the interests of transparency, it should be made clear to users at the point of installing the App and making choices on the use of functions that the functions operate independently with no linkages or cross-pollination of personal data, on the device or at subsequent stages of processing such as if/when transferred to the contact tracing teams.

[19] DPIA p8
[20] DPIA p7
[21] DPIA p8

(d) Accuracy

Controllers must ensure that personal data are accurate and, where necessary, kept up to date. Controllers are to take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. In particular, controllers should accurately record information they collect or receive and the source of that information. In the case of obtaining personal data for the purposes of contact tracing to combat the spread of COVID-19, it is clear that data accuracy is of paramount importance if the measure is to prove effective and to ensure that inaccuracies do not have negative affects on individual's rights and freedoms.

The DPIA notes that the use of smart phone technology for contact-tracing purposes is a new development and references efforts that have been made to engage with teams in other countries to identify the best technical solutions. The choice to implement the Exposure Notification System (ENS), developed by Apple and Google, is referenced in relation to the robustness of the system and the expectation that it will be "heavily optimised and tested for efficient battery use and will not interfere with other Bluetooth peripherals".[22]

The DPIA also refers to testing that has been conducted and will continue to be conducted to ensure the robustness and reliability of the App[23]. Outside expertise has been provided by Science Foundation Ireland in the development of the App, in particular in the area of Bluetooth proximity analysis, which is of particular importance in ensuring data accuracy in this context.[24]

One of the functions of the App is to gather in-app metrics that will be used to measure its efficacy against its stated purposes.

Taken as a whole, the measures outlined in relation to ensuring the accuracy of data obtained by the App seem to indicate that due consideration has been given to compliance with this principle.

Recommendation: In the interests of accountability and transparency, it is recommended that the results of testing and any independent analysis of functionality should be published and open to timely peer scrutiny.

[22] DPIA p13
[23] DPIA p13
[24] DPIA p13

(e) Storage Limitation

Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

The DPIA sets out the various retention limits on the different types of data that will be processed in association with each function of the App.

It is noted that the Governance Committee is responsible for ensuring that all data is deleted following the eventual winding down of the App at the end of the COVID-19 crisis period. [25]

Recommendation: In order to ensure accountability, the justification for each of the retention periods should be clearly documented by the Data Controller and set out in a table or at a relevant point within the DPIA and Data Protection Information Notice. Measures to ensure retention policies are effectively implemented should also be set out and explained.

(f) Integrity and Confidentiality

Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful access to or use of personal data and the equipment used for the processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The DPIA outlines a range of technical and organisational measures to ensure the security of the data undergoing processing using the App, including the appointment of a specialist information security advisor at an early stage of the project.[26] The DPIA indicates that independent security testing will be conducted on the App itself and on the backend services. [27]

It is noted also that access to the backend databases of the App will be logged and that the logs will be retained for audit purposes. [28]

[25] DPIA p7
[26] DPIA p20
[27] DPIA p20
[28] DPIA p20

The DPIA refers to the engagement of a number of data processors by the data controllers in various stages of the processing of data by the App and it is noted that, in each case, this will be subject to a data processing agreement in compliance with Article 28 GDPR.[29] The DPC notes that, where processing is to be carried out by a data processor, the HSE and DOH will be responsible for ensuring that the processor can provide sufficient guarantees that it will implement appropriate technical and organisational measures to ensure the security and confidentiality of the data.

The foregoing suggests that the data controllers have given due consideration to the principle of data integrity and confidentiality from the outset of this project, and going forward under the oversight of the Governance Committee.

Recommendation: The publication of the results and analysis of security testing, the threat model it was based on, and of the relevant elements of the data processing agreements would provide further evidence of adherence to the principle of integrity and confidentiality, as well as a commitment to accountability.

6. Article 6 Lawfulness of Processing

The processing of personal data requires the identification of a lawful basis or bases. The lawful grounds for processing personal data are set out in Article 6 of the GDPR. Certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as "special categories" of personal data. Processing of these special categories is prohibited, except in the limited circumstances set out in Article 9 of the GDPR. It is also noted that ePrivacy Directive (as transposed by SI 336/2011) obligations are addressed in the DPIA[30], concluding that the exemption provided in section 5 of the SI is applicable as the on device data accessed by the app is deemed strictly necessary in order to provide a service explicitly requested by a user.

The DPIA identifies the legal basis for the processing of personal data using the App as being provided by Article 6(1)(a) GDPR:[31]

> "the data subject has given consent to the processing of his or her personal data for one or more specific purposes"

[29] DPIA p23
[30] DPIAp16
[31] DPIA p15

The DPIA further identifies Article 9(2)(a) as the enabling condition to permit the processing of special category data (data concerning the data subject's health in this case):[32]

> "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes"

The European Data Protection Board, in its "Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak", has noted that:

> "the mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that the processing of personal data will necessarily be based on consent. When public authorities provide a service based on a mandate assigned by and in line with requirement laid down by law, it appears that the most relevant legal basis for processing is the necessity for the performance of a task in the public interest i.e. Art. 6(1)(e) GDPR"[33]

However, the guidelines acknowledge that other legal bases, including consent (Article 6(1)(a)) may be applicable, noting that the controller will have to ensure that the strict requirements for such a legal basis are met.[34]

The DPC understands that the choice of the data controllers to base the processing of personal data on consent aims to align with their intention that use of the App be entirely voluntary and discretionary on the part of users. As the EDPB guidelines indicate however, reliance on this legal basis requires the controller to ensure that its strict requirements, as articulated in Articles 4(11) and 7 GDPR, are met.

The definition of consent is found in Article 4(11) GDPR, and sets out that consent must be freely given, specific, informed, and unambiguous, as well as that it must be made by way of a statement or 'clear affirmative action'. The consent relied upon for the processing of data using the App must meet each of these requirements.

<u>"Freely given"</u>

This aspect of consent means that individuals must have a genuine choice to allow the processing of their personal data or not. Recital 42 GDPR recalls that "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment ". The "freely given" nature of consent can also be called into question where there is a clear imbalance of power between the data subject and controller, giving rise to a situation where the data subject might feel under

[32] DPIA p15
[33] EDPB Guidelines 04/2020 p7
[34] EDPB Guidelines p8

pressure or coerced into providing consent. Recital 43 GDPR highlights the example of a public authority as a data controller where such an imbalance is likely to occur.

In order to rely on consent for the processing of data using the App, the data controllers will need to be able to demonstrate that no imbalance of power invalidates the freely given nature of the consent that is obtained. The DPIA states that, "having regard for the entirely voluntary and discretionary nature of the downloading the App, and noting that the HSE and Department of Health cannot determine whether a person has installed the App or not, it is not considered that an "imbalance of power" (GDPR recital 43) arises." While it is clear that it is the intention of the data controllers for use of the App to be entirely voluntary, it is not clear that an imbalance of power between an individual and a public authority arises only where the public authority has knowledge of whether the individual has consented or not – although this might exacerbate such an imbalance.

An imbalance of power might also be perceived where pressure is brought to bear upon the public at large to engage. It is also noted that when a user is contacted by the HSE contact tracing team on diagnosis they will be asked to consent to receive an SMS code in order to upload diagnosis keys. It must be made explicitly clear that this is based on consent and no efforts are made to coerce or pressurise the user during this conversation. Measures to help safeguard the conditions of consent in this context could, for example, include the provision of scripts to contact tracing teams.

The guidelines of the EDPB on Consent under the GDPR consider that, without prejudice to the general considerations of Recital 43, "the use of consent as a lawful basis for data processing by public authorities is not totally excluded under the legal framework of the GDPR.[35]" The guidelines provide examples of situations where consent may be relied upon by public authorities, indicating that it may be appropriate for opting in to receive information notices or agreeing to processing that allows for the sharing of personal data between public bodies for efficiency purposes. This second example may be relevant to the App, as it points to consent being valid for processing that is optional and where non-consent does not result in the denial of processing for a core service. The purpose of a exposure notification app should be to provide an optional supplementary system to augment the existing, manual contact-tracing procedures undertaken by health authorities. In this context consent may provide a valid legal basis. It should be noted in this regard, that the processing of personal data for the purposes of contact tracing in the existing, manual procedure is not based on consent but on a legislative basis.

It is clear that the HSE and Department of Health as data controllers must be in a position to satisfy themselves, and be able to demonstrate, that where processing is based on consent the data subject can exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he or she does

[35] EDPB Guidelines 05/2020 p8

not consent. "Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will".[36]

"Specific"

The requirement for consent to be specific means that where processing has multiple distinct purposes, an individual should give specific and informed consent to each of them. The DPIA indicates that consent to each processing function is obtained separately on a separate page, and that the App Settings page allows the user to view the data that is being processed and grant or revoke specific consents as they wish.[37]

Specific consent will also mean that *further processing* will not be possible. This may raise operational implications if a requirement for interoperability between different apps or any other further processing is subsequently identified. In such circumstances, a new consent will be needed to satisfy the conditions of the consent legal basis under Article 6 and as an exemption under Article 9 GDPR.

"Informed"

The informed nature of consent means that controllers should make particular efforts to present information and choices to data subjects, so that they can be certain that the individual has understood exactly what they are being asked to consent to. In relation to the DPIA[38], this aspect of consent is addressed in relation to the principle of transparency, to which it is closely linked.

"Unambiguous"

The indication of the data subject's wishes, by which they grant their consent, must be a clear affirmative action or statement leaving no room for misunderstanding or ambiguity as to what they have consented. In cases where consent is given by electronic means (as in the use of a mobile app), the mechanism for obtaining consent should be clear, concise and not unnecessarily disruptive to the use of the service.

While the specific purposes for which consent is sought are clearly separated, the data controllers must also ensure that the specific means by which the indication of consent is made are clear. Given that the processing of special category data is proposed, the consent of the data subject must also be explicit, in accordance with Article 9(2)(a) GDPR.

[36] EDPB Guidelines 05/2020 p. 7
[37] DPIA p6
[38] DPIA p15

7. Article 7 Conditions for Consent

Where processing is based on consent, the controller must also demonstrate compliance with the conditions set out in Article 7, GDPR.

Firstly, the controller must be able to demonstrate in an accountable manner that consent has been obtained for the processing of personal data in each relevant situation. For example, the app itself records the consent of the user to various processing operations, made accessible to the user through the App setting. However, where consent is sought to send the authorisation code via SMS to upload random IDs, this will take place in the context of a phone conversation with the HSE's contact tracing team. It will be necessary for the controllers to implement a measure to be able to demonstrate that this consent has been provided in a valid manner. It will also be important in the context of obtaining freely given consent that the user is not put under any pressure or coerced in any way to upload the random IDs.

Secondly, Article 7(3) provides that the data subject shall have the right to withdraw his or her consent at any time, and that the withdrawal of consent shall be as easy as to give it in the first place.

The DPIA indicates that the App has a 'leave' function to delete all data held by the App from the phone and cease any further processing. Using the App settings, the user can also revoke any of the specific consents that have been given. It should be made explicitly clear to users that these are the available methods for withdrawing consent. Presented in this manner, it would appear that the withdrawal of consent is no more difficult to do than to provide consent to each processing operation in the first place.

Where a user has consented to the use of their demographic, symptom, and app metric data, it would not appear that withdrawal of consent is required for the processing of this data by the CSO for statistical purposes as it is stated to be transferred in anonymous form by the HSE. The withdrawal of consent under Article 7 does not affect the lawfulness of processing based on consent prior to withdrawal and would not apply in the case of effectively anonymised data. However, the data controllers should be able to ensure that where consent has been withdrawn, all residual data (that may already be held by the HSE and collected prior to the withdrawal of consent) is anonymised and transferred to the CSO. See also below on anonymisation.

The DPC is in agreement with the view expressed by the EDPB that the consent of the data subject is not excluded as a legal basis for contact-tracing applications. However, basing processing upon consent places a clear onus on the data controllers to ensure that all such processing meets the requirements for valid consent outlined in the GDPR, and to be in a position to demonstrate this.

Recommendation: The Guidelines of the EDPB referenced in this section make it clear that where consent is identified as the legal basis for processing personal data for the purposes of contact-tracing, the public health authority must ensure that the strict requirements for this legal basis are met. It is recommended that a comprehensive analysis of this compliance position be published, in line with the principle of accountability.

8. Stakeholder Engagement

Section 6 of the DPIA outlines the stakeholder engagement undertaken by the data controllers to inform and support the development of the App[39]. This engagement has included the HSE National Patient Forum, in line with Article 35(9) GDPR which provides that, "where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations." It is noted that ongoing engagement with the Patient Forum is intended.[40] Such ongoing engagement could usefully feed into the work of the Governance Committee in assessing the efficacy of the App and the effectiveness of transparency and communications strategies.

It is noted that further stakeholder engagement has been undertaken with the scientific community through Science Foundation Ireland, and that an ethical review will be undertaken by NPHET. Again, this engagement should be maintained and used to support the work of the Governance Committee.

Recommendation: Stakeholder engagement should continue with the purpose of feeding into the work of the Governance Committee in assessing the efficacy of the App and effectiveness of transparency and communications strategies. In relation to the general conduct of stakeholder engagement, and the principle of transparency, the feedback generated in this process or a consolidation thereof should be published.

9. Collaboration with the CSO

The DPIA refers at several points to the transfer of data to the CSO for the purpose of "statistical analysis to assist the DOH and public health specialists in monitoring the progression of symptoms across the country".[41] This statistical purpose is predicated on the CSO receiving anonymous data from the HSE, derived from both the COVID Check-in function of the App and the collection of app metrics. As the data is determined in the DPIA

[39] DPIA pp13-15
[40] DPIA p14
[41] DPIA p3

to be anonymous, no legal basis for the processing of personal data is provided for this transfer as it takes place outside the scope of the data protection legislative frameworks.

The DPC understands that the basis for identifying the geographical data to be obtained as anonymous[42] is based on the CSO's census banding. Taking into account that the population size for the purposes of the App will be smaller due to smartphone ownership; age; app uptake etc, the impact these factors, if any, on the anonymity of data, directly and indirectly, should be assessed.

In order for this approach to be compliant, the data controllers must be satisfied and be able to demonstrate that the data is robustly anonymised by the HSE, prior to transfer. The Article 29 Data Protection Working Party has set out an anonymisation test in its Opinion 05/2014 on Anonymisation Techniques, and this has been reiterated by the European Data Protection Board in its Guidelines 04/2020[43] on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. This test considers the set of techniques used to remove the ability to link, infer or single-out an identified or identifiable natural person with the data using any "reasonable" effort, taking into account both objective and contextual elements. This has also been subject to ECJ scrutiny[44] and a high bar has been set against which controllers must satisfactorily demonstrate that personal data is anonymised.

Recommendation: The data controllers, and the CSO, must be clear, prior to the processing of any data that no identifiable information will be provided to the CSO by the HSE. Every effort must also be made to ensure that there is no reasonable likelihood that any information provided to the CSO is deliberately or inadvertently used to re-identify any individual app user. It is recommended that the assessment of anonymity be published and that app users be clearly informed that anonymised data is transferred by the controllers to the CSO.

10. Governance

As with any of the measures being implemented nationally to assist in the fight against COVID-19, it is important that the use of the App is appropriately limited in time and purpose and that personal data are not processed in an unnecessary or inappropriate manner. The terms of reference of the App Governance Committee[45] set out a number of responsibilities to ensure the operation of the App adheres to the design principles set out in the DPIA, that its purposes remains strictly limited, and that is continues to contribute to the national COVID-19 response plan in the manner intended.

[42] DPIA p9
[43] EDPB Guidelines 04/2020 p5
[44] http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN
[45] DPIA p27

The establishment of the Governance Committee and its oversight functions represent safeguards to protect the fundamental rights and freedoms of the individuals whose personal data will be processed through their use of the App. The Committee's oversight and diligence is required throughout the lifetime to the app and the processing of any related personal data that is collected.

Recommendation: For reasons of transparency and accountability, the decisions of the Governance Committee should be made public, along with information that is provided to the committee relating to the adherence of the App to the principles outlined in the DPIA and its efficacy in contributing to the COVID-19 response. Verification by an independent authority of the measures for ultimately winding down the App, and the conditions, criteria or events that lead to this determination, under the oversight of the Governance Committee, would also be beneficial in ensuring public accountability.

11. Data Subjects' Rights

The DPIA addresses, in Section 7.6, the exercise of data subject rights in relation to the COVID Tracker App.

It is noted elsewhere in the DPIA that the data controllers will enter into a joint controller arrangement, pursuant to Article 26 GDPR. This arrangement must determine, in particular, the respective responsibilities of the joint data controllers for compliance with their obligations as regards the exercising of the rights of data subjects. It is important that data subjects be provided with clear information and a point of contact to exercise their rights. It is equally important that the controllers are clearly aware of their responsibilities and are prepared to facilitate data subjects in the exercising of their rights. This can be addressed by the implementation of data protection policies in addition to the joint controller arrangement.

With regard to the matters set out in Section 7.6[46], some points are noted.

- The personal data within the scope of the right of access is not entirely clear. The DPIA refers to accessing data via the App itself (however, this may not include on-device ENS data) and making a subject access request to the HSE. Exactly what data may be included should be set out, and whether or not it will be possible to gain access to symptom check-in data, for example, following the removal of the IP address
- The DPIA refers to the right to object to processing with reference to the Leave function. It should be noted that the right to object does not apply where processing is based upon consent, and that the right to withdraw consent is separate to this –

[46] DPIA pp22-23

though the eventual effect may be similar. The rights of the data subject vis-à-vis the manual contact tracing procedure, where the right to object will be available, should be clearly explained at the appropriate time.

- In relation to the right not to be subject to a decision based solely on automated processing, the DPIA refers to the fact that this right does not apply in the context of personal data being processed on the basis of explicit consent. However, Article 22(3) GDPR requires that in this situation the data controller "implement suitable measures to safeguard the data subjects' rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller to express his or her point of view and to contest the decision."

Concerning the erasure of data by a user on activation of the App's Leave Function, it is understood that notwithstanding the Leave Function, Exposure Notification System data remains on the device and requires a separate process to delete. This will likely be difficult to understand and needs to be explained simply and clearly in the information provided to users.

Recommendation: The applicability of data subject rights in the limited, pseudonymised context of the data processing on and off the App should be clearly described to app users.

The relevant elements of the joint controller arrangement in relation to the exercise of data subject rights should be made explicitly clear to app users at the appropriate place in the Data Protection Information Notice.

An appropriate data protection policy should be implemented to ensure that the data controllers can facilitate any exercise of data subject rights in a timely and complete manner.

Information provided to users on the separate and additional steps to delete ENS data should be explained clearly and simply to minimise the risk of user confusion.

12. Safeguards and Security Measures

Data controllers are obliged to implement appropriate and effective technical and organisational measures to ensure the security and integrity of personal data undergoing processing. This is especially the case given the nature, scope and context of the proposed app and the associated data processing arrangements. Section 7.5 of the DPIA sets out how these obligations are to be addressed.

The DPIA details a number of technical security measures in relation to different processing operations. The organisational measures that are set out include reference to the

appointment of a specialist information security advisor at an early stage of the project, as well as controls around separation of roles and access to data.

Recommendation: Independent or secondary reviews of the testing of security measures should be undertaken where possible, and that the publication of the results of such testing would assist with the overall transparency and accountability of the App.

Consideration should be given to appropriate data protection training for staff members who may be working in data processing, and also to the risks that can be presented by inadequate knowledge or training in relation to their role.

The efficacy of the organisational and technical measures in securing the data should be subject to ongoing review and to the oversight of the Governance Committee.

13. Google/Apple Exposure Notification System

The DPIA refers to the choice of the data controllers to implement the Google/Apple Exposure Notification System (ENS) to facilitate processing of app data on-device. The DPC, in collaboration with EU data protection authorities, is engaged in ongoing dialogue with Google/Apple on the data protection implications of the ENS. At this time no matters giving rise to significant concern have been identified. However, it is incumbent upon the data controllers to implement the necessary organisational and technical measures to ensure the protection of the personal data they process. This should include an examination of the technical specification of any APIs to ensure the security and confidentiality of personal data undergoing processing.

Recommendation: The HSE and Department of Health should continue to review the appropriateness of the use of the ENS through their own testing and with reference to any independent review that may be published, in particular in light of the novelty of this technology and the importance of this processing in pursuit of a public health interest.