Data Protection Impact Assessment – COVID Alert Malta

Control Sheet

Title	COVID Alert Malta
Date Approved	
Version Number	0.4
Document Type	Data Protection Impact Assessment
Document Status	
Author	The Superintendence of Public Health External Legal Advisor: Dr Mireille M Caruana
Data Controller	The Superintendence of Public Health

Revision History

Version	Date	Summary of Changes
0.1	9 July 2020	
0.2	21 December 2020	DPIA updated to reflect the introduction of the EU Interoperability service.
0.2	23 December 2020	Feedback received from Mr Robert Spiteri Staines at MITA.
0.2	7 January 2021	Updated version finalised and recirculated.
0.3	18 January 2021	Updated version following feedback from the Joint Controllers Group.
0.4	12 February 2021	Inclusion of risk mitigation strategies in view of use of Azure Public Cloud.

Consultation History

Version	Date	Name	Designation
0.1			

Part 1 – Determining whether the proposed processing of personal data for contact tracing purposes is likely to result in a high risk to the rights and freedoms of the data subject		
Q1	Does this project involve the processing of personal data?	'Personal data' is defined in Article 4(1) of the European Union's General Data Protection Regulation (GDPR) as "any information relating to an identified or identifiable natural person". The 'data subject' is therefore an identifiable natural person that can be identified, directly or indirectly, by reference to an identifier like a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Recital 26 specifies that "to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly." In order to determine whether the information processed through the proximity tracing technology amounts to personal data, it must be determined whether the Temporary Exposure Keys ('TEKs') and the Rotating Proximity Identifiers ('RPIs') that are collected and stored with other meta data consisting of (Countries of Interest) country codes can be considered as relating to an identified or identifiable person, taking into account all lawful means reasonably likely to be used. In brief, the RPIs are ephemeral, pseudo-random IDs representing a user device (typically a smartphone) which are broadcast via Bluetooth; the app records pseudo-random identifiers of other user devices in close proximity, together with the duration and an approximate indication of time. The TEKs are used to generate the RPIs. The Maltese system being implemented is based on the secure and decentralised privacy-preserving proximity tracing software system called 'Decentralised Privacy-Preserving Proximity Tracing' (DP^3T) developed by 'an international

		consortium of technologists, legal experts, engineers and epidemiologists with a wide range of experience who are interested in ensuring that any proximity tracing technology does not result in governments obtaining surveillance capabilities which will endanger civil society'. The DP^3T consortium have also published a Data Protection Impact Assessment (DPIA)[1] which concluded that: "*the system is designed to avoid identification of individual users and uses technical solutions to ensure that all data is* ***pseudonymised.*** *Identification of individuals to which the data relates is in most cases impossible, but cannot be entirely excluded. For this purpose, taking the system as a whole,* ***the information that is shared between users through their use of the app must, at some points, be characterised as personal data.***" According to the GDPR, pseudonymised data is personal data falling within the scope of the Regulation. In the words of Recital 26, "*personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.*" However, "*as long as the system is adequately deployed,* ***the information that is stored by the backend will not be characterised as personal data from the point of view of the operator of the backend server***."[2] The code included in the solution which will be deployed and which is not part of the DP^3T follows the design of the DP^3T solution and does not involve further sharing, storage or other processing of personal data, pseudonymous or otherwise.[3] If it were to be determined that the app only processes anonymous data, then there would be no legal requirement to carry out a DPIA in terms of the GDPR. However, since this matter is subject to some doubt, and in view of the fact that a DPIA has been carried out for the DP^3T Proximity Tracing System itself, the Superintendence of Public Health, in collaboration with other involved entities, is undertaking this exercise which will consider the data protection implications

		in the event that the data being processed may under certain circumstances be considered to be personal data. When a user who has tested positive agrees to upload his or her TEKs, these TEKs are subsequently referred to as 'Diagnosis Keys' (DKs). Given the advice of the European Data Protection Board (EDPB) in relation to how DKs should be treated, the EU produced a specific and comprehensive DPIA for the European Federation Gateway Service (EFGS).[4] As documented by the EFGS DPIA and in accordance with Annex III of the Implementing Decision (EU) 2020/1023, personal data uploaded to the EFGS will be disposed of once either all participating back-end servers have downloaded the respective personal data or 14 days have passed since the upload of the data, whichever is earlier. The following data will be uploaded to the EFGS by the COVID Alert Malta backend: a. Infected citizens' Diagnosis Keys (TEKs). One Diagnosis Key per day from infectivity onset date (i.e. estimated date at which user was infectious) up to a maximum of 14 days will be uploaded to the EFGS. b. Countries of Interest. One or more country codes (MT and optionally other country codes) associated and uploaded with each Diagnosis Key to the EFGS. With the exception of MT (Malta) the country codes that are uploaded is dependent on the user's choices to exchange data with other European countries as follows: o Exchange exposure data with users of other European contact tracing and warning apps, or;

		○ Exchange exposure data with users of other contact tracing and warning apps of certain countries only (user selects from a list of countries, or; ○ Do not exchange exposure data with users of other European contact tracing and warning apps. Data exchange occurs when: a. The diagnosed citizen has entered the (COVID) code, provided by Public Health, in the app; b. The relevant TEKs on the diagnosed citizen's device are available; that is the app must have been installed and correctly functioning (e.g. Bluetooth enabled) on or prior to the infectivity onset date, and the TEKs were not deleted from the device by the citizen. In a separate process, and depending on the user's choices as described above, the COVID Alert Malta backend will periodically download, from the EFGS, the Diagnosis Keys originating from the backends of other participating European countries. All data exchange between Malta and the EFGS (upload or download) is via the COVID Alert Malta Backend only.
Q2	Who is the Lead/Manager/Senior Responsible Owner for the project? (Provide name, designation and contact details)	The Superintendence of Public Health Contact: Dr Hugo Agius Muscat, MD MSc Consultant Public Health Medicine

		COVID-19 Public Health Response – Data Management Lead Ministry for Health hugo.agius-muscat@gov.mt
Q3	Provide a summary of the project	**In general:** Use of the app will occur on a **voluntary** basis. Individuals who decide not to or cannot use the app will not suffer from any disadvantage at all (which includes not benefitting from advantages offered to users); this will be ensured through independent policies, **including through legislative safeguards**. Users will be able to withdraw their assent to use the system at any time (by deleting the app or simply stopping using it),[5] in which case no more data will be generated. The sole advantage of using the app is the direct benefits gained by its use, i.e. you may be notified of having been in contact with a positive person which may not have otherwise been possible. The system will be based on Bluetooth Low Energy proximity tracking, as proposed by the DP^3T consortium, and make use of new technical facilities provided by Apple and Google. The system tracks proximity events between user devices (without any other location information) in order to facilitate quick and efficient identification of possible contacts of infected persons. If one user is identified to be infected, and the user assents to the recording of the fact in his/her device, any users whose devices have been in significant proximity are alerted. The system does not track location, but devices "handshake" with each other when they are close to each other. The system does not determine *real* infection risk, but *presumed* risk. To make the difference clear, consider the following two situations: • A mobile carried by an infected person for an hour 1m away from a mobile carried by another person, where both persons are not wearing any personal protective equipment;

		• Same situation, but where both persons are wearing full personal protective equipment. The mobile will record exactly the same 'proximity', but in situation A there is significant infection risk, while in situation B there is negligible risk. The system will be used alongside conventional, manual methods in order to improve the Public Health (PH) Team's capability to trace COVID-19 contacts. The Public Health (PH) COVID-19 Response Team's intention is that this app captures and stores only anonymous/pseudonymous data that cannot be traced back to the user of the app. The app will be solely devoted to providing public information related to COVID-19 and exposure notification /contact tracing. It is completely independent from other COVID-related technical functionality. Location tracking functionality will **not** be built into the app. **Design principles** • Implementing 'privacy by design' / 'data protection by design' principles, the system uses a fully 'decentralised' and highly privacy-preserving approach. This means that pseudonymous contact information collected and stored by mobile phones is not automatically uploaded to a central server; it is only if an infected person registers the infection on his/her phone that contacts are anonymously informed via a central server. The data uploaded to the central server is also anonymous/pseudonymous TEKs, used to generate RPIs. Then, it is only if a contact consciously communicates with the PH team outside the app that the PH Team will learn of the identity of the contact; even in this case, the PH Team will not know the identity of the infected person; • The system is designed to support cross-border interoperability between contact tracing and warning apps of other participating countries[6] via the EFGS. **Business workflow**

		The following is the business workflow envisaged by the PH Team: 1) Phones that have the app installed exchange pseudonymous IDs when they are within Bluetooth range of each other. (PH is not involved in this.) 2) If an app user is informed by PH that he/she is positive, that user will be asked to voluntarily enter a code in the app. If the user accepts, and enters the code, the system will automatically alert the person's anonymous/pseudonymous Bluetooth contacts through their apps that they have been in contact with an infected person, without revealing his/her identity. The positive user's app will send its own ID to the central system to be sent to others whose phone app would thus be able to compute potential risk of exposure. The contacts will be invited to contact the PH Team by other means (e.g. phone, email). 3) If a contact voluntarily gets in touch with the PH Team, his/her identity will become known and conventional PH action will start (e.g. the contact will be invited to undergo testing for the COVID-19 virus). **In case of infection:** App users will have no obligation to notify the backend that s/he has tested positive for COVID-19, or to contact or give information to the backend when the app highlights that there was contact with a positive case. App users may therefore participate in the system "passively", i.e. solely to be informed if they encounter an infected person, without disclosing to other users if they themselves have tested positive for COVID-19. Use comes with no mandate whatsoever. Irrespective of whether a person is an app user or not, persons who are found to be positive or to be close contacts of persons who are positive are subject to applicable public health measures (such as mandatory quarantine) as mandated by existing public health legislation. **Continuous scanning and exposure notification:**

		Phones with Exposure Notification Services (ENS) active will continuously scan for other phones nearby with ENS active. This happens regardless of which national contact tracing app is deployed on the phone provided the phone is running the latest operating system from Apple and Google that incorporates the ENS service. Phones with national apps from different countries will continuously scan for other phones nearby with ENS active. When proximity is detected, the phones record this as described above. **The European Federation Gateway Service (EFGS):** In the effort to reduce the spread of COVID-19 within their communities, a number of EU Member States and EFTA countries have implemented proximity tracing apps. In the case of Malta this is COVID Alert Malta. While the proximity detection mechanisms of these apps are compatible, if the national backends behind the different national apps do not communicate with each other the individual countries' proximity tracing apps cannot trace potential infection between citizens from different countries using their country's app. This also applies to Maltese citizens when coming into contact with foreign EU and EFTA country citizens in Malta or whilst overseas in other EU and EFTA countries. To ensure contact tracing apps work seamlessly across EU borders, to avoid the need for EU citizens to have to download different contact tracing apps as they visit other member states, and to protect those who don't travel from visitors arriving from other countries, the EU initiated an interoperability project in the summer of 2020. In order to address this problem the EU eHealth Network endorsed an architecture blueprint for the implementation of a single European Federated Gateway Service to which each national backend would upload the keys ('Diagnosis Keys') of newly infected citizens on a frequent basis and from which the keys from the other countries participating in this initiative would be downloaded to the individual countries' proximity tracing apps.

		The EU Commission took on the role of developing the European Federated Gateway Server, to be hosted by the EU: "The purpose of the European Federation Gateway Service (EFGS) is to facilitate the interoperability of national contact tracing and warning mobile applications within the federation gateway and the continuity of contact tracing in a cross-border context."[7] The purpose of EFGS is to act as a relay server so that the backend servers in each participating country can communicate with each other to share DKs and so achieve cross border interoperability. Malta is participating in the EU interoperability project. Malta is actively pursuing this initiative through the Superintendence of Public Health with the collaboration of Government's IT agency MITA. Subsequently MITA engaged its approved contractor Seasus Ltd to analyse and compile a requirements specification that recommends options for the implementation of the COVID Alert Malta app for interoperability with the European Federated Gateway. Seasus Ltd is responsible for the software development and support and maintenance of the COVID Alert Malta app. In this way, diagnosis keys uploaded to the Maltese backend can be relayed to the backend server in other participating members states, so that their backend server can issue these keys to the app users in those countries. This ensures that Maltese app users who become Covid positive can alert app users in other countries. Conversely, the Maltese backend server will receive keys from other countries which can be used to alert Maltese app users that they have been in close contact with a user of another participating country's contact tracing and warning app who has subsequently tested Covid positive. Three main approaches for the adaptation of the Maltese contact tracing and warning app to be interoperable were carefully considered and documented:

		1. User Provided Travel History (exchange keys with apps of countries visited by the Maltese app user and related to visit dates) 2. User Provided Countries of Interest (the app user specifies a list of countries he or she may have an interest in, for example countries visited in the previous 14 days) 3. 'One World' (exchange data with apps of all participating countries). From a functional point of view 'One World' is the most effective approach to interoperability. However when taking into consideration current daily rates of infection in participating countries as well as uncertainty surrounding the technical impact on citizens' smart phones, it is believed that basing interoperability on One World, without an alternative mitigating approach, would present an intolerable risk to the COVID Alert Malta initiative. The Ministry for Health and MITA considered a 'hybrid' implementation, consisting of One World and Countries of Interest, and that allows users to choose the method that meets their individual needs, to be the way forward. In more detail: 1. A hybrid implementation will allow users to choose whether and how they wish to exchange data with participating countries. Users experiencing issues with One World may switch to the more (resource) economical Countries of Interest method. 2. Users will be requested to select from one of the following options[8]: a. Exchange exposure data with users of other European contact tracing and warning apps, or; b. Exchange exposure data with users of other contact tracing and warning apps of certain countries only, or; c. Do not exchange exposure data with users of other European contact tracing and warning apps.

		3. Selecting option 2(a) will signify 'One World' whilst selecting option 2(b) will signify 'Countries of Interest'. In this case the user will be given the option to select countries from a list of participating countries. 4. The COVID Alert Malta app will continue to share/exchange pseudonymous data with other users of COVID Alert Malta regardless of the option selected. 5. Selecting the option on how to exchange data provides users with the facility to mitigate any issues experienced with data usage and, or mobile phone performance, should these be experienced. All apps download the new diagnosis keys and compare against the recorded IDs on their phone. The download consists of diagnosis keys from the COVID Alert Malta app plus diagnosis keys for confirmed COVID-19 patients from other countries and jurisdictions (as per (2.) above), provided those countries use a national app based on the Apple Google ENS software and there are appropriate agreements in place between the participating national public health authorities. ***Options for the exchange (sharing) of data via the EFGS*** A user's choice to exchange, via the EFGS, pseudonymous data with users of other contact tracing and warning apps should be separated from a user's choice to use the app and share data with other COVID Alert Malta app users. Considerations for the implementation should include: a. The three options will by default be 'not selected' (no data will be exchanged); b. Options will be gathered on installation and set-up of the app, and thereafter may be modified by the user at any time; c. In the case of an infected user the app will request a user to confirm his or her chosen options to share (upload to the EFGS) his or her keys with users of other countries' apps on the basis of the selected options.

		Whilst encouraging users to exchange their pseudonymous data keys with users of other contact tracing and warning apps, it is important that particular attention is given to how this is presented and that the principle of voluntary participation is upheld.
Q4	Detail the benefits of the project to the Superintendence of Public Health	The system facilitates the identification of close contacts of COVID-19 cases, through technical methods not previously available to contact tracers. The benefit is that of aiding the Superintendence of Public Health to achieve the primary objective of preventing the spread of COVID-19. The system is an addition to the manual contact tracing process currently in use. It provides an efficient way to detect all proximity events, including in scenarios where the users do not know each other, e.g. public transport or public space. Therefore, it enables the very quick alerting of people who are at risk. If these individuals get tested as advised by PH, the app is a means to quickly stop infection chains. In the current manual process, an individual often experiences symptoms before getting tested; therefore, possibly already being infectious and passing on COVID-19 to other individuals. Manual contact tracing is also based on memory and is therefore error prone. **Benefits resulting from exchanging personal data via the EFGS:** Participating in the EU interoperability project has the significant advantage of contributing to the continuity of contact tracing in a cross-border context. The pursuit of this purpose permits enabling the cross-border interoperability of the national contract tracing and warning mobile applications for the COVID-19 pandemic within the territory of the European Union. Participating in the EU interoperability project could ensure that proximity events occurring between two or more users of apps of different participating counties, in Malta or overseas, will be assessed by the COVID Alert Malta app for risk of COVID-19 exposure. It will therefore extend the app's geographic scope beyond Maltese borders as well as potentially increase the population of interest to include any user of an app of another participating country.

		The project therefore has the potential to significantly increase the app's effectiveness as a proactive instrument that complements the efforts of public health authorities in Malta and other participating countries to control and curb the spread of the COVID-19 virus in Malta and other participating countries.
Q5	Detail the benefits of the project to any other relevant parties	The other relevant parties are a) the public-at-large, which clearly benefits from the prevention of the spread of COVID-19, e.g. not unwittingly spreading the virus and/or the possible indirect consequences flowing from any potential overwhelming of the public health system, and b) moreover, since the effects of the deadly virus are not well understood, other important countervailing public interests come into play, in particular 'the right to life'.
Q6	Define who has responsibilities for the data (Provide name, designation and contact details)	Within Government, data controllership is defined by function. The data controller is the Superintendence of Public Health. The Superintendent of Public Health: Professor Charmaine Gauci charmaine.gauci@gov.mt The Data Protection Officer in the SPH: Ms Pauline Schembri pauline.schembri@gov.mt
Q7	What personal data is to be processed?	The app is designed to process as little personal data as possible. It is the user's device that may process or store identifiable personal data about the user, while the system is designed to prevent the backend server from accessing any personal data. As long as the data that is stored on, or accessed

		by, the backend server cannot be characterised as personal data, the requirements laid down in the GDPR do not apply to it. The European Federated Gateway Server will act as a relay server for national backend servers to upload and download DKs and meta data from.
Q8	What sensitive data if any, is to be processed? State the categories.	Health data is any data containing information about the health of a particular individual. This includes not only information about past and current illnesses, but also about a person's risk of illness (such as the risk that the person has been infected with the coronavirus). As regards the information stored on app users' devices, if the app identifies a potential risk of infection for you, then your data also includes health data. Furthermore, the DP^3T DPIA Report concluded that: "[I]t cannot be excluded that a User notified that she or he has been in close proximity with an individual tested positive to COVID-19 may identify that individual. For this reason, the information stored on other Users' devices must be characterised as personal data. More specifically, this information will relate to the individuals' health, and must therefore be considered as sensitive data within the meaning of Art. 9 GDPR."[9] Since the app and the central system store and broadcast past TEKs and RPIs initially stored on the phones of those who tested positive, in line with the DP^3T DPIA Report and to err on the side of caution, for the purposes of this DPIA the data stored on Users' devices will be treated as pseudonymous data which could (although this is highly unlikely) reveal special categories of data (in particular, health data). However, the backend server does not process any data that can be linked to an identifiable person. Moreover, health data related to the COVID tests is not part of the system.

		As the DKs are only processed when a person is diagnosed positive for COVID-19 they are being considered as pseudonymised personal health data. In the DPIA-Draft European Federation Gateway Service Version 1.4 ('EFGS DPIA-Draft') [10] it is stated that "The processing in the EFGS and the subsequent processing concern health data."
Q9	What is the nature of the processing?	Processing involves using a secure and decentralised privacy-preserving proximity tracing software system and secure processing with the EFGS. This process is additional to other initiatives already being undertaken by the PH authorities, including traditional, manual contact tracing.
Q10	Define the scope of the processing	Processing for the sole purpose of contact tracing /exposure notification of RPIs of app users who voluntarily download and use the app; the processing is in practice not likely to reveal personal data (including health data), but theoretically it may do so.
Q11	Explain the context in which the processing will take place	The app is aimed at people who are resident in Malta and Gozo, who will be encouraged to download and use it, as part of a larger effort by the PH authorities to prevent the spread of the COVID-19 virus. The additional processing via the EFGS allows for interoperability, that is that the app will work when travelling abroad and that apps used by visitors from those countries will work here, noting importantly that neither public health authorities in Malta, nor in other jurisdictions can identify anyone from the DKs at any point in the process.
Q12	Describe the purpose of the processing	The purpose of the processing is limited to contact tracing / exposure notification.
Q13	How many individuals will be affected by the processing, or what is the proportion of the relevant population affected?	All those present and/or residing in Malta will be encouraged to download and use the app. It is hoped that a significant proportion of persons present in Malta will download and use the app.

		With the addition of interoperability, all app users of other participating countries may potentially also be affected by the processing.
Q14	Is the personal/sensitive data already held by the Superintendence of Public Health but it is now the intention to use it for another purpose? If so, provide full details of current purpose and new purpose.	No.
Q15	Taking account of the types of personal/sensitive data to be processed, and the • nature, • scope, • context and • purpose of the proposed processing, is the processing likely to result in a high risk to the rights and freedoms of the data subjects concerned? Provide the reason for your conclusion.	Article 35 GDPR states that "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data." In its Guidelines 04/2020, the EDPB concluded that a DPIA must be carried out prior to deployment of a contact tracing system, "as the processing is considered likely high risk (health data, anticipated large-scale adoption, systematic monitoring, use of new technological solution)" (EDPB Guidelines 04/2020, § 39). It has therefore been decided to carry out a DPIA, to err on the side of caution and to explicitly demonstrate that all efforts have been made to ensure that the app is indeed privacy-preserving insofar as it only processes data which are strictly necessary in view of the purposes for which they are processed, which data is considered to be pseudonymous despite the fact that in a practical sense the data is actually more likely to be anonymous in terms of the GDPR. Moreover, the EFGS DPIA-Draft concludes that "the planned processing in the EFGS is likely to result in a high risk to the rights and freedoms of natural persons and a DPIA is required."

Part 2 – Systematic Description of Processing		
In this section, describe the processing in detail.		
Q16	What will be the classification of the personal/sensitive data under the Government Classification Scheme?	Not applicable.
Q17	Exactly what personal data will be processed as part of the project?	The data stored locally on a user's device consists of the following. Data is deleted after 14 days. a) Rotating Proximity Identifiers (RPIs) that it broadcasts (pseudonymous); b) Coarse timestamps; and c) The Temporary Exposure Keys (TEKs) used to generate the RPIs. Other data stored locally on a user's device consists of the following: d) User's choice with respect to exchange of data; and e) Dependent on (d) list of user's Countries of Interest country codes. Data (d) and (e) will be stored indefinitely or until: i) User deletes or modifies the data; ii) User uninstalls the app in which case the data will be automatically removed from the device. In the event of an infection being confirmed in a user, the following data is recorded in the authorisation code management system: a) The authorisation code; b) The date on which the first symptoms appeared, or – if the infected individual is asymptomatic – the date of testing (onset date); c) The time at which this data is to be destroyed; and d) The transmission risk level assigned by Health Authority to the case. The backend server contains a list with the following data. Data is deleted after 14 days + 7 days backup. There is no link to the health records of infected users.

		a) The secret keys (TEKs) of infected users which were current in the period during which infection of other persons is likely to have occurred (i.e., from onset date onwards up to max 14 days); and b) The date of each key; and c) The countries of interest of infected users. After coming into proximity (2 metres or less) with another mobile phone on which the app is running, the app stores the following data. Data is deleted after 14 days. a) The Rotating Proximity Identifiers (RPIs) broadcast by the other device. There is no direct link that identifies the users of the other devices; b) Proximity (the Bluetooth low energy signal strength); c) Approximate time window; and d) The estimated duration of proximity. The European Federated Gateway Service will store the following data uploaded by participating country apps. A Maltese app user's data will only be uploaded to the EFGS with the assent of the individual users. Data is deleted after 7 days + 7 days backup. There is no link to the health records of infected users. a) The secret keys (TEKs) of infected users which were current in the period during which infection of other persons is likely to have occurred (i.e., from onset date onwards up to max 14 days); b) The date of each key; and c) The countries of interest of infected users.
Q18	What, if any, processing of sensitive data will be carried out and why?	Although the data processed is in a practical sense anonymous and there is no envisaged processing of personal or special categories of data, the system may reveal pseudonymous data. In the unlikely event that personal information is revealed, the system may reveal health data, through 'singling out' methods.

Q19	What is the source of the personal/sensitive data?	The source is the temporary exposure keys (TEKs) and random identification numbers (RPIs) that are generated by a user's smartphone and broadcast via Bluetooth Low Energy, and which other users' smartphones in the user's vicinity can receive if exposure logging is also enabled on them. This functionality serves to record encounters with other users. Users may also enter their countries of interest for use in the exchange of data with the EFGS. Users may also enter codes that indicate positive test results (DKs). In some instances, this may reveal personal information i.e. close proximity to another identifiable person. However, this identifiability does not result from app behaviour as such, but rather through inference/deduction etc.
Q20	Will the personal/sensitive data be fully identifiable, pseudonymised or anonymised?	Pseudonymised device identifiers.
Q21	Will another organisation be processing any of the personal/sensitive data either on behalf of the Health authorities or in conjunction with the Health authorities? e.g. contractors, external ICT support, partners? If so, provide details of: • the organisation • its Data Protection Officer and • the exact role of the other organisation in the processing of the data?	No organisation will be processing personal or personal, sensitive data by means of this app, not even the SPH itself. The data will be processed in an entirely anonymous /pseudonymous way and the data will not be traceable by MFH, MITA or MDIA to identifiable natural persons. PH will only learn of the identity of contacts if these voluntarily come forward, and even if/when they do, PH won't know the identity of the infected person/s they were in contact with.
Q22	In relation to the proposed processing, what is the status of: a) the Superintendence of Public Health b) the Department of Health Regulation c) MITA d) 18 Squared Consortium	a) Controller b) Joint Controller (with respect to the backend server data) c) Processor of the backend server (application) data and Data Controller of the Cloud Services platform d) Processor of the Cloud Services platform on behalf of MITA e) Sub-Processor engaged by and on behalf of the 18 Square Consortium

	e) Microsoft f) Google and Apple	f) Neither a controller, nor a processor
Q23	What policies / guidance etc will be in place prior to the commencement of processing?	The Conditions of Use and the User App Privacy Policy. These will be updated to reflect the exchange of personal data via the EFGS.
Q24	Data Flow analysis	Updated document attached.

Part 3 – Assessment of Necessity and Proportionality			
In this section, you are required to assess whether the processing is necessary and is not excessive.			
	Requirement – The Data Protection Principles		Comments
Q25	**GDPR /DPA 2018** **1st Principle**	**Lawful /Fair /Transparent:** • Is the processing based on consent and if so, why? • Is the processing necessary for the performance of a task? If so, provide details of the task.	The fact that a contact tracing application is used on a voluntary basis does not mean that the most appropriate legal basis for processing under EU Data Protection law is consent. While use of the contact-tracing app will occur on a **voluntary basis**, the most appropriate legal basis for processing the information is not consent. When EU public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, the most relevant legal basis for the processing, with regard to personal data, is the necessity for the performance of a task in the public interest, i.e. Art. 6(1)(e) GDPR. The GDPR lays down rules regarding lawfulness, proportionality and necessity. These provisions stipulate that the processing of personal data without the data subject's consent is prohibited unless 'necessary' for certain specified purposes:
		Sensitive Processing: • Does the processing involve processing of sensitive data? • If so, state which categories are being processed? • Is the processing being based on consent? If so, why is consent appropriate in the circumstances?	

		• If it is necessary for public health purposes, state why and which condition in Article 9 is satisfied.	• Article 6(1)(d): "Processing shall be lawful only if and to the extent that…: processing is **necessary** in order to protect the vital interests of the data subject or of another natural person". • Article 6(1)(e): "Processing shall be lawful only if and to the extent that…: processing is **necessary** for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"; the basis for the processing must be **laid down by law** and the purpose of the processing must be **necessary** for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.....[that] law shall meet an objective of public interest and be **proportionate** to the legitimate aim pursued (Article 6(3) GDPR). • The contact-tracing app will be processing health data of data subjects. Under Article 9(1), the "processing of personal data ... concerning health ... shall be prohibited". However, this general prohibition on the processing of 'special categories of personal data' is subject to certain exemptions: for example, the processing is **necessary** for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health....**on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject** (Article 9(2)(i) GDPR); or the processing is **necessary** for....the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law….and subject to

			the conditions and safeguards referred to in paragraph 3 (Article 9(2)(h) GDPR). ● Article 9(2)(j) GDPR also allows for health data to be processed when **necessary** for scientific research purposes or statistical purposes "in accordance with Article 89(1) **based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject**." Meanwhile the GDPR's Recitals provide further guidance about the changing role of the data protection framework during emergencies: ● Any processing of personal data necessary to protect lives is put on a lawful basis; more importantly, surveillance is *expressly permitted*: ○ **Recital 46: "**The processing of personal data **should also be regarded to be lawful** where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. **Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, <u>including for monitoring epidemics and their spread or in situations of humanitarian</u>**

			<u>emergencies</u>, in particular in situations of natural and man-made disasters." ● User consent is not needed during public health emergencies: ○ **Recital 54:** "The processing of special categories of personal data may be necessary **for reasons of public interest in the areas of public health <u>without consent</u> of the data subject**. **Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons.** In that context, "public health" should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council, namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest **should not result in personal data being processed for other purposes by third parties** such as employers or insurance and banking companies." **In the present case, Articles 6(1)(e) and 9(2)(i) are the most appropriate and protective legal bases for processing the (personal, sensitive) data.** The basis for the processing under Article 9(2)(i) indicates that the processing of 'special categories of personal data' like health data may take place without the consent of the data subject, provided such processing is necessary for the reasons stated therein

			and on the basis of a law which 'provides for suitable and specific measures to safeguard the rights and freedoms of the data subject'. Therefore, before rolling out any contact tracing app, **member states have a legal obligation to introduce a law providing for suitable and specific measures to safeguard the rights and freedoms of the data subject.** Any law to safeguard the rights and freedoms of the data subject should *inter alia* define who the controller/s is/are, specify the purpose of processing and lay down explicit limitations regarding further use, identify the categories of data as well as the entities to, and purposes for which the personal data may be disclosed, and enact additional meaningful safeguards as appropriate, including a specific reference to the voluntary nature of the application, provide specific rules for non-discriminatory protection,[11] and an exit strategy (the measures must be temporary – not here to stay after the crisis).[12] There should be strong measures and penalties for any data controllers/processors integrated into the law, with provisions guaranteeing deletion of any user data when the user no longer wishes to participate and/or the public health emergency is declared over. **It is not currently envisaged that processing for purposes of scientific research will be carried out on the data. The DPIA will be revisited and updated should a change of policy occur.** Regarding the lawfulness of the processing, the system involves storage and/or access to Bluetooth information (in the form of TEKs and RPIs) from the users' devices, which (independently from any processing of personal data) requires a lawful basis. The ePrivacy Directive[13] provides that 'the storing of information, or the gaining of access to information already stored, in the terminal equipment of a user is only allowed on condition that the subscriber or user concerned has given his or her

			consent ... This shall not prevent any technical storage or access ... as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service' (Article 5(3)). **In this instance, the storing of information in the smart phone of a user will happen with the user's consent, which is obtained when the user agrees to the privacy policy prior to downloading and using the app; moreover, this is also an instance of technical storage strictly necessary in order to provide the service explicitly requested by the user.** Additionally, depending on the nature of the prescribed intervention when a risk notification is provided, in particular whether it produces legal effects or similarly significantly affects the data subject, the system may be considered a decision within the meaning of Article 22 GDPR. This would require a lawful basis under that Article to be established for such a decision, and the implementation of safeguards in line with Article 22 and national law. However, in the present instance, the system is **not** considered to produce legal or similarly significant effects as it only informs the user of a presumed risk, suggests the user takes a specific action, but does not make any decision in relation thereto. The legal basis for the interoperability processing of personal data via the EFGS may consist of the data subject's (qualified) consent or statutory law. This DPIA has concluded that in the present case basing legal safeguards on statutory law provides superior protection to data subjects. Nevertheless, the data subject's assent will be obtained; this assent is viewed as a safeguard to uphold individual autonomy (so those who agree to further processing outside Malta or restrict it solely to Malta will be entitled to do so) rather than the legal basis in terms of Articles 6 and 9 of the GDPR.

			The European Data Protection Board (EDPB) states concerning its view of these requirements : "**When relying on public interest, national law may need to be adjusted to provide for the sharing of the data with other services. In case of consent as the legal basis, an additional consent will need to be collected for the interoperability processing fulfilling all of its requirements**. In particular, it needs to be specific and therefore sufficiently granular. When different legal bases are used by the different data controllers of the contact tracing applications, additional measures may be required to implement data subject rights related to the legal basis. Where it concerns health data, Art. 9 GDPR is applicable and the controllers will need to be able to rely on one of the exceptions mentioned there."[14] The legal basis for processing[15] will be amended/ updated to exchange the necessary information with participating countries having a similar proximity tracing and notification application for the purpose of notifying users of their close proximity of an infected person. Link to the Law: https://legislation.mt/eli/sl/465.52/eng/pdf
Q26	**GDPR /DPA2018** **2nd Principle**	**Specified/Explicit/Legitimate:** • State the specific purpose for which the personal/sensitive data will be processed. • Is the data to be used for any other purpose? If so what other purpose? Is the data to be used for any non-public health purpose?	The data is used solely for the purpose of exposure notification /contact tracing. The data collected by or from the app is not to be used for any other purpose.

		If so: • What is that purpose? • Why do you believe that this purpose is not incompatible with the specific reason for which you gathered it?	
Q27	**GDPR /DPA2018** **3rd Principle**	**Adequate/Relevant/Not excessive:** • What assessment has been made to ensure that the data being processed is adequate, relevant and not excessive in relation to what is necessary for the purpose for which they are processed?	The processing activities are adequate to achieve the purpose of exposure notification /contact tracing. The usefulness of exposure notification /contact tracing systems to limit the spread of COVID-19 will depend on the adoption of the system within a population and is contested. The following factors could limit the adoption of the system: - participation is on a voluntary basis only; - not everyone has a smartphone or knows how to download or set up an application. Any form of exposure notification /contact tracing is by itself not sufficient to tackle the spread of COVID-19. Accordingly, the system is designed as a complementary tool to traditional contact tracing techniques and other public health measures. Therefore, the use of the app may only be adequate to achieve that purpose if it is used in combination with other measures. If a user tests positive (confirmed by a health authority) and agrees to authorise use of their exposure notification/contact tracing app TEKs and RPIs, the user is given an authorisation code. This code needs to be inputted on the user device in order to allow the user to upload user pseudonyms. The test result itself is not uploaded on the backend server of the COVID contact tracing system, but is retained within another Health IT system. There is no way to link the user pseudonyms on the

			backend server with the identity of the user (including his or her health information). If a user is identified to be positive, the information whether to self-quarantine or self-isolate is provided by the health authority, and is distinct from the COVID exposure notification / contact tracing system. The same applies if a user tests negative; the health authority will provide the recommendations based on the case itself. The only health-related information provided is an alert to the user that, through proximity with an infected individual, they may be at risk and should contact the health authorities for a test. Personal data exchanged via the EFGS is strictly necessary to enable interoperability as detailed above.
Q28	**GDPR /DPA2018 4th Principle**	**Accurate/Kept up to date where necessary:** • How will the accuracy of the data be checked? • What process will be in place to rectify/erase inaccurate data?	The system ensures that only data about COVID-19 positive persons are uploaded to the backend server by requiring an authorisation code that needs to be provided by accredited healthcare providers.
Q29	**GDPR /DPA2018 5th Principle**	**Not kept longer than necessary:** • How long will the personal data be retained? • Will the system require manual intervention or will deletion be automatic? • If the data is required to be retained after the retention period, (e.g. for statistical	Data which is stored on the backend server is automatically erased after 14 days + 7 days backup; data which is stored on each user's device is automatically erased after 14 days. There are no exceptional circumstances for retaining data for longer than these normal periods. The 14 day retention period for the data on the user device is set by Google/Apple and cannot be extended. Retention by the Public Health authority of aggregated anonymous data for statistical purposes is lawful and should not be unnecessarily prevented. Nevertheless it is noted that the current system does not

		purposes) how will it be anonymised? • What processes will be in place to ensure the data is securely destroyed/deleted?	have the stated functionality (and relevant statistical data is not being collected or aggregated). It might be provided in the future, at which point in time the DPIA will be revised and updated. Data is deleted from the EFGS after 7 days and retained for a further 7 days for backup purposes after which it is also permanently deleted.
Q30	**GDPR /DPA2018 6th Principle**	**Secure:** • How will the personal data be secured and kept safe? • What technical/operational security features and/or policies will be in place to protect the personal data?	The system is designed to comply with state-of-the-art cryptographic techniques and security measures; See also response to Q36 below.

Part 4 – Measures Contributing to the Rights of the Data Subjects			
In this section, assess how data subjects' rights will be protected.			
Q31	**GDPR Articles 12 – 14**	**Information – Controller's general duties:** • How will data subjects be made aware of what is happening to their data? • Is it the intention to withhold any of the information listed under the exemptions? • If so, how do you propose to record your decisions?	The processing will be carried out in a way that is comprehensible to the data subject. The SPH plans to publish a Notice regarding this for information purposes. Users will be given relevant information when installing the application on their device. Information will also be provided through other media, including TV and radio. The app to be deployed is essentially the same code as DP^3T, with the addition of modules required for the system to work, e.g. the authentication server which generates and verifies authentication

			codes, and other minor changes to tailor it to the local context. **The software code will be made publicly available.** The code of the DP^3T and its documentation is public and can be freely accessed and audited by anyone. The Consortium further published an explanatory comic in many languages in order to help individuals understand how the system works and which data will be processed. Nevertheless, the onus of providing sufficient and adequate information to individuals mainly rest on the controller, i.e. the Superintendence of Public Health. This information will be provided in a concise, transparent, comprehensible and easily accessible form in clear and plain language (The first sentence of Article 12(1) GDPR). This information will be provided in the **User App Privacy Policy**, but also through any other appropriate way. In order to ensure their fairness, accountability and, more broadly, their compliance with the law, algorithms will be audited and also made openly available for review by independent experts.
Q32	**GDPR Article 15**	**Subject Access Requests:** • How will you ensure that the information will be available to Information Management for the processing of subject access requests?	The system has been designed so that only a user's device processes or stores any identifiable personal data about that user. No entities are involved in the processing of any identifiable user personal data. Accordingly, the system is neutral from the point of view of individuals: in the absence of personal data being stored on the backend server or the device of other users, individuals' rights pursuant to data protection laws are not restricted (nor are they enabled). Users who want to stop participating in the system may at any time stop using their user app or delete it. All data already uploaded to the backend server are erased at the end of the retention period (14 days + 7 days backup). Due to the decentralised design, the backend server

			only has a limited control on the data. In particular, it cannot (i) identify the individuals to which the data stored on the backend server relates (thus cannot carry out requests for deletion) or (ii) access (nor delete) the data that is stored on the users' devices. Providing the backend server with additional control over the data processed via the system would ultimately be detrimental to the individuals. Article 11(2) GDPR provides that 'where ... the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 (right of access by the data subject, right to rectification etc) shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.'
Q33	**GDPR Article 16**	**Right to Rectification:** • What processes will be in place to manage requests for rectification? • What process will be in place to notify any recipients of the personal data that is/was inaccurate data?	Not applicable. There is no manual entry and therefore updates. Information about infected secret keys (SK) are removed at the end of the infectious window. Data on the user's device is deleted after 14 days. Data on the backend is deleted after 14 days + 7 days backup. Data on the EFGS is deleted after 7 days + 7 days backup. Implementing a manual way to amend data is not necessary and could have detrimental effects (loss of integrity). See also response to Q33 above.
Q34	**GDPR Article 17**	**Right to erasure or restriction of processing** • The system being designed must be able to allow erasure of data. What processes will be in place to	Users who want to stop participating in the system may at any time stop using their user app or delete it. All data already uploaded to the backend server will be erased at the end of the retention period (14 days + 7 days backup) whilst data already uploaded to the EFGS will be erased at the end of the retention period (7 days + 7 days backup). Due to the decentralised design, the backend server and the EFGS only have a

		manage requests for erasure? • What process will be in place to notify any recipients of the personal data that it has now been erased?	limited control on the data. In particular, (i) individuals to which data stored relates cannot be identified. Therefore requests for deletion cannot be carried out and (ii) access (or deletion) of data that is stored on the users' devices cannot be performed. Providing the backend server with additional control over the data processed via the system would ultimately be detrimental to the individuals.
Q35	**GDPR Article 32**	**Security of processing:**	
		• Will the data be encrypted?	Yes, the data will be encrypted. All transmissions are TLS/SLL encrypted. The data at rest is only a series of cryptographic codes.
		• Will the data be pseudonymised? If so how?	Yes, the data will be pseudonymised. Full details in link.[16]
		• How will the data be protected against risk of loss, confidentiality, availability and integrity?	Data at rest will be regularly backed up using zone redundant storage ○ Data replication to secondary region possible ○ Fine grained access control to the database ○ Data in transit will be encrypted through TLS ○ Transmitted data will be digitally signed to ensure integrity
		• Will back-ups be taken? If so, when/how often?	The data on the backend server will be backed-up at frequent intervals, with a retention period of seven (7) days. Therefore, the total data retention period will be fourteen (14) days + seven (7) days for the back-up. This duration is enforced as the minimum back-up by the service provider.
		• Will the security of the system be required to have any formal accreditation or independent certification (e.g. ISO27001)?	The security aspects of the system were covered by an external audit conducted by an independent systems auditor licensed by the MDIA.

		• What processes will be in place to determine who will have access to the data/system?	Access control will be provided to selected individuals for maintenance and error handling purposes.
		• What data protection /security training will users of the data/system be required to have?	Strictly speaking no training is provided specifically for the system. Nevertheless, MITA has the policies in place to both engage individuals with the required skill set, as well as to implement the relevant procedures. See attached GMICT Policy document.
		• How will access to the system be granted?	Access to the data is governed by MITA's Request for Service (RFS) procedure. The data owner must approve such access. Following approval, the administrator will grant access either by creating a new account through the database's built-in security mechanism or granting access to the user's corporate identity.
Q36	Consultation	Consultation Requirements	The Office of the Information and Data Protection Commissioner (IDPC) will be consulted.
Q37	**GDPR Articles 44 – 50**	Data Transfers Outside the EU: • Will the data be held or transferred to a third country (i.e. outside the EU)? • If yes, for what purpose, and to where will it be held or transferred? • If yes, what processes will be place to ensure it is adequately protected?	The app is designed to support interoperability with other privacy-preserving contact tracing apps, also based on the DP^3T protocol, being designed by other EU Member States. In this case, the app may exchange pseudonymous TEKs, RPIs and country codes with such apps. Once borders between countries are open and the relevant agreements are in place, data can be shared with other EU Member States and third countries. The data shared is limited to pseudonyms (TEKs/RPIs) of infected individuals, and do not include any identification means linking to identifiable individuals.

		• Will the data be held or transferred to another country inside the EU? • If yes – for what purpose and to where will it be held or transferred?	

Part 5 – Other privacy legislation and policies		
In this section, assess the other rights that data subjects have. This helps balance the final risk assessment.		
Q38	**Human Rights** European Convention on Human Rights • Article 8 – Right to respect for private and family life Charter of Fundamental Rights of the European Union • Article 7 Respect for private and family life • Article 8 Protection of personal data	• According to Article 8 of the EU Charter of Fundamental Rights ('EU Charter'): o "Everyone has the right to the protection of personal data concerning him or her." o "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified." o "Compliance with these rules shall be subject to control by an independent authority." • Furthermore, according to Article 52(1) of the EU Charter: o "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

		• Similarly, Article 8(2) of the European Convention on Human Rights ('ECHR'): ○ "There shall be no interference by a public authority with the exercise of [the right to respect for private and family life] except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." Taken together, the qualifications in the provisions above require that any interference with fundamental, human rights are: (i) provided for by law / in accordance with the law (ii) necessary (iii) proportionate A key operational issue remains regarding the precise meaning of the '**necessity**' criterion in the provisions above (as well as those discussed above at Q.26 with regard to lawful basis.) It should be noted that 'necessary' is **not** the same as 'indispensable'. In *Huber,*[17] the CJEU assessed whether a centralized database was necessary in terms of *effectiveness*: "...the centralisation of those data ***could be necessary***, within the meaning of Article 7(e) of Directive 95/46, if it contributes to the ***more effective*** application of that legislation as regards the right of residence of Union citizens who wish to reside in a Member State of which they are not nationals." [**Emphasis added**] Although this judgment interprets Article 7(e) of Directive 95/46 (its equivalent is now found in Article 6(1)(e) GDPR), the terminology of 'processing is

		necessary….' is reproduced verbatim; accordingly, the same interpretation ought to be applied if a new case were to arise that requires a similar assessment. Moreover, this interpretation is in line with the jurisprudence of the European Court of Human Rights ('ECtHR'). The ECtHR has stated that 'the adjective "necessary" is **not synonymous** with "indispensable"'.[18] In Judge Mosler's separate opinion he stated: > Such a definition would be too narrow and would not correspond to the usage of this word in domestic law. On the other hand, it is beyond question that the measure must be appropriate for achieving the aim. However, **a measure cannot be regarded as inappropriate, and hence not "necessary", just because it proves ineffectual by not achieving its aim**.[19] In the words of the ECtHR in *Silver and Others v the United Kingdom*[20]: > On a number of occasions, the Court has stated its understanding of the phrase "necessary in a democratic society", the nature of its functions in the examination of issues turning on that phrase and the manner in which it will perform those functions. It suffices here to summarise certain principles: (a) the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" (see the Handyside judgment of 7 December 1976, Series A no. 24, p. 22, § 48); The judgments of the ECtHR also clarify the 'margin of appreciation' available to national authorities 'the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved'.[21] In the context of **covert, non-consensual surveillance** by state security agencies, the ECtHR has held that 'the margin of appreciation available to the respondent State in assessing the pressing social need in the present case, and in particular in choosing the means for achieving the legitimate aim of protecting national security, was a wide one'.[22] In the extraordinary situation of

		a pandemic, the margin of appreciation available to State parties in assessing what is necessary for fulfilling that aim should also be wide. It should also be noted that, in the present analysis, we are not faced with an instance of covert or otherwise non-consensual processing of personal data (as were the circumstances in the case-law discussed above), but rather with the consensual uptake of an app that users voluntarily sign up to for the purposes of assisting the State during a public health crisis. While there is as yet no case-law on this point, the voluntary nature of the processing throws into doubt the very existence of an interference with the rights laid down in Article 8(1) ECHR.[23] Beyond data privacy law, the principle of proportionality is a general principle of EU law, generally recognised as having three prongs: (i) suitability - is the measure concerned suitable or relevant to realizing the goals it is aimed at meeting? (ii) necessity - is the measure concerned required for realizing the goals it is aimed at meeting? and (iii) non-excessiveness (proportionality *stricto sensu*) - does the measure go further than is necessary to realize the goals it is aimed at meeting?[24] The requirement of proportionality has emerged as a data protection principle in its own right. This is reflected in the addition of the principle of proportionality to the core principles of the Modernised Convention 108,[25] as well as in elements of the GDPR and CJEU case-law.[26] The controller still has to observe, for instance, the basic principles of Article 5 GDPR -- and these principles bring with them tests of necessity and proportionality.
Q39	**Children** GDPR, Article 8 – conditions applicable to child's consent in relation to information society services	The Conditions of Use of the app will include the stipulation that the app user is at least 13 years of age. Children of at least 13 years of age will also voluntarily download and use the app.

	(In Malta you are no longer a minor at age 18. However, for the purposes of the GDPR, the processing of the personal data of a child in relation to the offer of information society services directly to a child is lawful where the child is at least 13 years old (S.L. 586.11))	In general, young children are assumed to be in proximity of an adult (parent /legal guardian) who has the application on their device. In case their parent /guardian are found to be in proximity of someone who tested positive for the virus, and subsequently test positive themselves, then manual tracing would help identify the children. The conditions of use of the app detail a minimum age. This is the age of thirteen (13), which is the age at which a child may give consent in relation to the offer of information society services in Malta. If a child under the age of eighteen (18) is tested to be COVID-19-positive by the health authorities, the verification code is not given directly to the child but to the holder of parental responsibility over the child, i.e. to the parent or the legal guardian of the child. Therefore the data stored by the app on the child's device is only uploaded if the verification code is given by the parent/guardian of the child.

Part 6 – Risks to the rights and freedoms of data subjects of the proposed processing				
In this section, using the information you have gathered so far in the DPIA, complete a final risk assessment				
Risk(s) identified to the rights and freedoms of data subjects	**Likelihood and severity of harm**	**Mitigation(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Curtailing of information rights provided for in the GDPR	Possible /Significant	GDPR Article 13 information will be provided in the **Privacy Policy**.	Eliminated.	Acceptable.

Curtailing of data protection rights and rights against discriminatory treatment	Possible /Significant	Malta has enacted an appropriate **statutory basis** that provides the lawful basis for the use of the contact-tracing app in terms of Articles 6(1)(e) and 9(2)(i) GDPR, incorporating meaningful safeguards, including a reference to the voluntary nature of the app. A clear specification of purpose and explicit limitations concerning the future use of personal data are included, as well as a clear identification of the controller involved. The criteria to determine when the application will be dismantled and which entity will be responsible and accountable for making that determination should be established as soon as practicable. It must be ensured in law and in fact that users have to disclose neither the status of the app nor the mere existence on a device to third parties. The controller is responsible for providing all required information to individuals in the **User App privacy policy**, and also through any other appropriate way.	Reduced.	Acceptable.
Notifications could, for example, cause panic, social stigmatisation, or adverse health outcomes	Possible /Significant	During installation of the app, informative screens are displayed to the user that in effect counsel the user on the purpose of the app and the possibility of being notified of	Reduced.	Acceptable.

		potential exposure to the COVID-19 virus. The language used has been carefully chosen to avoid causing unnecessary anxiety or alarm in the user. The user is provided with links to informative pages on a Health website, and is provided with the number of the Public Health Helpline (111) in order to be able to obtain help when needed.		
The system notifications that recommend you call the health authorities and get tested may result in a restriction of movement, or of private and family life (you may for example decide to self-isolate before the test)	Probable /Significant	Given the context of the project, precautionary behaviour is to be preferred to the possibility of the exponential spread of COVID-19.	Accepted.	Acceptable.
Compliance of Processors	Remote /Significant	The main controller of the system will assess the need to obtain a standard data processor agreement (DPA) with the mobile phone operating system providers (Apple and Google). However, a DPA is not strictly required as Google and Apple are not processing data. Signed documents for using the API will be made publicly available.[27] The system contemplated here is unlikely to pose additional risks to the rights and freedoms of data subjects, as data subjects with smartphones will already be using these systems every day.	Reduced.	Acceptable.

Right to respect for private and family life and to protection of personal data	Possible /Significant	This DPIA has been undertaken with the specific intention to consider in depth any interference with the rights to private and family life, and to the protection of personal data. It has been concluded that any such interference is minimal, lawful and justified.	Reduced.	Acceptable.
Expectations and Concerns of the General Public	Probable /Significant	These will be managed through a very clear and transparent information campaign, including through a privacy policy for the app and through the passing of specific legislation.	Reduced.	Acceptable.
The individual will contact the Public Health Authorities voluntarily, but may thereafter be subject to traditional contact tracing, imposition of self-quarantine etc. The resulting risk is that individuals may choose not to respond to notifications.	Possible /Severe	The transparency and openness surrounding the deployment of the app, coupled with a public information campaign emphasizing the importance of individual behaviour that supports the efforts of the Health Authorities, will hopefully encourage individuals to trust the system and participate therein, also out of a general sense of civic responsibility.	Reduced.	Acceptable.
The system not working as promised due to incorrect code	Possible /Severe	A systems audit was carried out ensuring that the code was reviewed by independent experts against well-defined control objectives; also, the DP^3T is an open source software and thus any bugs discovered can be fixed more effectively.	Reduced.	Acceptable.
Impact on effectiveness of app for those on holidays or working or visiting other countries regularly, or visitors from other countries to Malta	Probable/ Significant	Ensure that the app is to augment the existing contact tracing and testing operations in Malta;	Reduced.	Acceptable.

		Engage at an EU level with regard to cross border interoperability.		
Re-identification of individual users	Remote /Significant	Reidentification of individual users cannot be entirely excluded and is inherent to any proximity tracing system. The simplest example[28] is the user that never leaves her home, except once in a month to buy groceries in a shop which is empty except for the owner. If this user meets no other person on her way to and from the shop, and is notified by the system that she was in close proximity to an infected person, she will know that this person was the shop owner. There is no obvious way in which TEKs/RPIs can be associated with an identifiable natural person except perhaps by hacking in to the app/Bluetooth to allow the user to know when a particular ID appears so that s/he can associate it with a person (if only one is present at the time).[29] The EFGS DPIA-Draft noted that "The information conveyed by the EFGS must not allow users to identify users carrying the virus, nor their movements. The system must be designed in such a way that neither intentional nor unintentional movement profiles (location tracking) or contact profiles (patterns of frequent contacts	Accepted.	Acceptable.

		traceable to specific people) can be established." However, "No protocols exist on the server side that allow the re-identification of users. Since there's only a connection between the national back-end and the EFGS, no personal IP addresses are processed. The diagnosis keys themselves are pseudonymised data. So, re-identification of users is not an immediate outcome of the operation of the EFGS."[30]		
Users (patients) may be less likely to upload their DKs when advised they will be shared with other countries as a result of interop capabilities going live	Possible/ significant	Users (patients) will be requested to select from one of the following options: a. Exchange exposure data with users of other European contact tracing and warning apps, or; b. Exchange exposure data with users of other contact tracing and warning apps of the 'countries of interest' only, or; c. Do not exchange exposure data with users of other European contact tracing and warning apps. Considerations for the implementation should include: a. Assent is to be based on opt-in and by default 'not provided'. b. Assent should be gathered on installation and set-up of the app,	Accepted.	Acceptable.

		and thereafter may be modified by the user at any time. c. In the case of an infected user the app will request a user to confirm his or her assent to share (upload to the EFGS) his or her keys with users of other countries' apps; Whilst encouraging users to provide their assent to share their keys, it is important that particular attention is given to how this is presented and that the principle of voluntary participation is upheld. The script (and backup information) used by clinicians when they advise patients they are Covid-19 positive and invite patients to upload their keys will be updated to provide reassurance to patients that uploading the keys will not be used to identify them as an individual and adds value even if they are not travelling overseas themselves.		
Unlawful interoperability processing	Possible/ significant	The EFGS DPIA-Draft states that each controller is responsible for a sufficient legal basis. This risk is catered for in the EFGS DPIA-Draft: "The lawful legal basis is a requirement for the access of the EFGS...the certificate necessary for the communication of the national backend server and the EFGS server will only be issued if the eHealth network approves the legal basis... As long as	Accepted.	Acceptable.

		a member state cannot ensure a compliant legal basis for its processing activities, no certificate should be issued by the eHealth network that would enable the communication of the backend server of the member state with the server of the EFGS and therefore to participate in the interoperability of the EFGS."		
Non-transparent processing of personal data via the EFGS	Possible/ significant	The (updated) DPIA will be provided to the IDPC as part of the consultation process. No later than the time when personal data is obtained by the controller, the data subject will be given clear information about the additional processing related to the use of interoperability. At this point, the user will be informed of the conditions and extent of the data processing. The **Privacy Policy** will be updated to reflect the exchange of personal data via the EFGS.	Eliminated.	Acceptable.
Processing of inaccurate personal data	Possible/ Significant	The EFGS DPIA-Draft states that "A secure and trusted onboarding process for participants of the European Federation Gateway Service must be established. "Rules" for data sharing and minimum requirements of data quality should be required. One scenario to avoid is that one country does not trust the data of another country and must exclude the data from its	Accepted.	Acceptable.

		system. This would be particularly damaging if the countries in question are neighbouring countries, because then, the border crossers could not be warned accordingly. Therefore, an obligation for all participating countries should be established that regulates the need of a verification of the positive test result by a governmental body and according policies should be established."		
Processing of redundant/unlimited stored personal data	Possible/ Significant	The EFGS DPIA-Draft states that "To ensure the minimum exchange and processing of data, as is required by the GDPR, developers will need to agree on a common protocol and compatible data structures. Otherwise there is the risk of an increased collection of personal data for interoperability due to a lack of a coordinated approach." Counter-measures are proposed in the EFGS DPIA-Draft (at 14.2.4.7.)	Reduced	Accepted.

Part 7 – Use of public cloud services		
Q.	Does the national contact tracing and warning mobile application backend use public cloud services (eg. Amazon Web Services, Microsoft Azure, Google Cloud Platform)?	Yes. The data generated when the App is used (data generated when an infected person registers the infection on his/her phone) is uploaded and processed on the COVID Alert Malta backend server. The backend server is hosted within the Microsoft Amsterdam Azure Cloud data centre located in the Netherlands referred to as the Azure West Europe Region.

	(i) In what capacity are public cloud services used and to what extent?	Azure Cloud services are used to: a. Host the backend server including storing and processing of TEKs uploaded by infected users of the COVID Alert Malta app and TEKs downloaded from the EFGS for onward distribution of the COVID Alert Malta app running on users' devices for decentralized contact tracing. b. Provide communications between backend server and the EFGS (European Federation Gateways Services) via secure web services. Web service calls are authenticated via mTLS. c. Provide communications between backend and the COVID Alert Malta app running on end-user's devices (iOS and Android) via web services. Web service calls are secured using TLS. The following are the Azure Cloud services used by the backend server: a. Azure App Service (application server) b. Azure Database for PostgreSQL server c. Azure Container Registry d. Azure Key Vault All Azure services used by the solution have been configured to be confined to the West Europe (WE) region which means that processing and data, including back up, stored on the backend server will not be transferred out of the European Union. Further to this all data stored on the backend server is encrypted using a strong (RSA 2048 bit) encryption key thus ensuring that the data cannot be read without this encryption key.

	(ii) How the risks of using public cloud were assessed and managed?	
Identified risk	**Assessment of the risk**	**How the risk has been managed/mitigated**
Data transferred to a third country		Additional safeguards and technical configurations have been implemented to assure that application data including back-ups will not be transferred outside the EU. These additional safeguards and technical configurations are detailed in section (iii) below. The service provider is contractually bound to adhere the General Data Protection Regulation (2016/679). The service provider must also contractually adhere to the requirement that the Public Cloud services are offered from at least two (2) Data Centres that are at a minimum distance of 100 KM from each other, of which one Data Centre must be inside the European Union, while the other must be inside the European Union or a country on the EU data protection adequacy list as per article 45 of Regulation (EU) 2016/679. The DPA endorsed by the service provider requires that the data processor must not transfer personal data outside the EU unless the prior written consent of the data controller is provided.
Data is inappropriately accessed from a third country	Appropriate access to pseudonymized data stored on the COVID Alert Malta backend is through the application's data interfaces (web services) which are inherently global and which is a prerequisite of a decentralized system, such as DP3T on which COVID Alert Malta is based and where users do not identify themselves when using the application or the service.	Risks of inappropriate access to COVID Alert Malta data have been mitigated through the implementation of technical measures on both the application and the hosting platform detailed in section (iii) below.

	Further to this a user may travel anywhere in and outside the EU with the app installed on their mobile phone. Access to the pseudonymized data through methods other than through the application's data interfaces is inappropriate whether access occurs from within the EU or from a third country. The risk of inappropriate access to the data whether occurring from within the EU or from a third country must be mitigated.	
Data communications is routed via a third country	Data communications between the COVID Alert app and Malta backend and vice, and the Malta backend and the EFGS is performed over the (global) internet. This poses a risk to data privacy and integrity should data communications be intercepted.	Data in transit is secured using the accepted industry cryptographic standard protocol which renders data communications to and from the COVID Alert Malta backend unintelligible and tamper proof such data communications be intercepted from within the EU or a third country.
	(iii) What additional safeguards or configurations were applied in order to limit the risks of processing the data using public cloud services?	The following additional technical safeguards and configurations have been implemented to mitigate the risks identified above. a. The Azure subscription used to provision the services enforces a West Europe (WE) and North Europe (NE) regional policy. This means that services cannot be deployed or moved outside the region where the service, including the database,

		was provisioned and deployed. The WE region Azure Cloud data centers are located in the Netherlands. The NE region Azure Cloud data centers are located in the Republic of Ireland. b. All Azure Cloud services used by the COVID Alert Malta solution are configured to Regional (WE) and therefore processed and stored within the West Europe region (Amsterdam data center). c. The COVID Alert Malta backend stores application data in an Azure Database for PostgreSQL. This service does not move or store customer data out of the region the database was deployed in unless the customer has enabled geo-redundant backups or has created cross-region read replica(s) for storing data in another region.[31] In the case of COVID Alert Malta configuration: i. Geo-redundant backups have **not** been enabled. Data backups have been configured to use locally redundant storage (LRS) and therefore data backups will not be moved out of the WE region; ii. Cross-region replica(s) of the database have **not** been created or enabled. d. COVID Alert Malta application data is not stored in the Clear. Application data is encrypted at rest using a customer provided digital certificate (RSA 2048 bit) encryption and which is stored in a Key Vault. This ensures that data cannot be read by the public cloud provider or any other party whether in the EU or a third country.

		e. In relation to the data protection requirements included in the contract, a written statement has been requested from the service provider warranting that, when providing the Public Cloud Service, no Personal Data is transferred to a country outside the European Union or to a country not on the EU data protection adequacy list as per Regulation 45 of Regulation (EU)2016/679 in line with the statements provided by the Austria.
Q.	Is there a risk of personal data transfer to third countries or international organisations due to the use of public cloud as infrastructure of your national contact tracing and warning mobile application which may be incompliant with Court of Justice of the European Union judgment in Case C-311/18?	The service provider is contractually bound not transfer any data outside of the EU/EEA. Therefore although there is no such thing as absolute certainty that data can never be transferred out of the EU/EAA, such transfer could only happen in breach of the contractual obligations. All efforts have thus been made to ensure that data is not transferred outside of the EU/EEA including the technical and contractual measures described above.

Article 36 of the GDPR states that in cases where high risks cannot be mitigated in full, before proceeding with processing, the Information and Data Protection Commissioner must be consulted. This DPIA concludes that any risks have been reduced or even eliminated. Nevertheless, as good practice, the IDPC will be consulted.

Part 8 – Approval

Data Protection Officer
Signature:
Date:

The Superintendent of Public Health
Signature:
Date:

Endnotes:

[1] Data Protection Impact Assessment Report, Version: V.01 | 01.05.2020, visited at <https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf> on 30 June 2020.
[2] *Ibid.*
[3] The part of the code being referred to is the authentication server; its functionality is to generate random codes to be used as a verification method when an individual is tested to be COVID-19-positive and assents to upload his/her pseudonyms on the data server. The rest of the code is based on DP-3T but includes minor modifications to localise to the Maltese context, e.g. changing the text on the app, and data server sends a notification to authentication server when a code is received.
[4] European Commission, External Draft Data Protection Impact Assessment (DPIA-Draft) European Federation Gateway Service, Version 1.4. Accessed on 30 December 2020 at < https://ec.europa.eu/health/sites/health/files/ehealth/docs/efgs_dpia_en.pdf>
[5] Users can withdraw their assent temporarily by stopping the tracing function of the app, or more permanently by uninstalling the app. When contact tracing is deemed by the health authorities to no longer be necessary, the users can be made to update the app (forced update) to a version which has no functionality, as users cannot be forced to uninstall the app, and the app cannot be made to automatically uninstall itself.
[6] Information on the participating countries can be accessed here: https://ec.europa.eu/health/sites/health/files/ehealth/docs/gateway_jointcontrollers_en.pdf
[7] European Commission, External Draft Data Protection Impact Assessment (DPIA-Draft) European Federation Gateway Service, Version 1.3.
[8] Presentation and description of options are examples for demonstration purposes only and will be revised accordingly. COVID Alert Malta app FAQs to include detailed information on each option.
[9] DP^3T Data Protection Impact Assessment Report (n 1) 17.
[10] The document is a 'final draft' intended "to provide certain components of a Data Protection Impact Assessment (DPIA) for the Member States as a basis (as stipulated in Annex II paragraph 12 of the Commission Implementing Decision (EU) 2020/1023) for their respective own DPIA as joint controllers for the exchange of personal data via the European Federation Gateway Service (EFGS)."
[11] For example, any discrimination (e.g. denying the use of public transport) will be disallowed. "This would imply, in particular, that individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all." European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, Adopted on 21 April 2020 ('EDPB Guidelines 04/2020').
[12] "The EDPB recommends including, as soon as practicable, the criteria to determine when the application will be dismantled and which entity shall be responsible and accountable for making that determination." EDPB Guidelines 04/2020.
[13] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p.37, as amended by Directive 2009/136/EC) OJ L 337, 18.12.2009, p.11.

[14] EDPB Statement on the data protection impact of the interoperability of contact tracing apps. Adopted on 16 June 2020 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en_0.pdf>
[15] Subsidiary Legislation 465.62 Contact Tracing and Alerting Mobile Application Order, Legal Notice 379 of 2020 Public Health Act (Cap. 465) < https://legislation.mt/eli/sl/465.52/eng/pdf>
[16] https://www.blog.google/documents/60/Exposure_Notification_-_Cryptography_Specification_v1.1.pdf
[17] Case C-524/06; ECLI:EU:C:2008:724.
[18] *Handyside v UK* (1976) 1 EHRR 737 at 48.
[19] Ibid. Separate opinion of Judge Mosler.
[20] (1983) 5 EHRR 347 [97].
[21] Leander (1987) 9 EHRR 433 [59].
[22] *Ibid.*
[23] cf. Lee A. Bygrave, *Data Privacy Law: An International Perspective*, (OUP 2014) 91.
[24] See further P Craig and G de Búrca, *EU Law* (6th edn, OUP 2015) 380-428.
[25] Council of Europe Convention 108 + Convention for the protection of individuals with regard to the processing of personal data 2018, CETS No.223, Article 5(1). Malta has not yet signed or ratified this Convention.
[26] Bygrave (n 15) 147-150.
[27] Google's terms of service may be accessed at https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdf
[28] Provided by the DP^3T Data Protection Impact Assessment Report (n 1) 13.
[29] As noted in the analysis of DP^3T, this is highly improbable: see Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems: the DP-3T Project 21 April 2020, visited at https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf on 6 July 2020.
[30] EFGS Draft-DPIA at 14.2.5.7.
[31] https://docs.microsoft.com/en-us/azure/postgresql/concepts-backup#backup-redundancy-options