centralised model and GPS/location tracking, and while certain benefits prevail over the proposed approach for NI (namely assistance in cluster identification), significant privacy concerns exist with these approaches and they are not being pursued. The StopCOVID NI app will be launched with interoperability between it and the ROI app. This is a significant development, supporting cross-border travel, and helping reduce chains of transmission traversing the border. The MOU governing this arrangement is appended ('Appendix D').

Governance safeguards to limit the scope and extent of interference with data protection and privacy rights are in place through the terms of reference of the Expert Advisory Group (see 'Appendix A'), ensuring data is processed in line with its purpose and principles, including the full wind-down of data processing when the COVID-19 crisis is over, and the ongoing monitoring of the effectiveness of the app and appropriate wind-down if it is not. Through the design and implementation of the Contact Tracing function these rights are further protected by ensuring it is, and continues to be, entirely voluntary in nature; and that users are asked for their clear and explicit consent if they wish to turn on ENS, and upload their diagnosis keys.

Location services are never used to track the location of users, where instead Bluetooth is used to detect proximity without any location data, meeting its purpose in a data minimised way. Consent can be withdrawn at any time for the processing of all Contact Tracing data and can be deleted under the control of the data subject, independently and without the knowledge of the DoH. There is no consequence to not using the app as the DoH cannot tell who has and who hasn't installed the app. Having taken into account the necessity set out above and the limited interference with data subject rights, the processing proposed under the Contact Tracing function of the app is seen as necessary and proportionate.

Necessity and proportionality of App metrics – the processing of app metric data is a supporting form of processing for the performance of the above functions and to monitor their effectiveness. It is also intended to give the public health teams insights into the functioning of the app, such as the number of exposure notifications per day, for use in health policy formulation and measurement. It does not collect, nor share personally identifiable information. Users receive information in relation to the collection of the data during the 'on-boarding' process, and can decide to remove the app from their pone at any time. It is considered to have little interference with individuals' rights, and is seen as necessary and proportionate. The data collected is essential in proving efficacy, essential for regulatory approval and the continued availability of the app.

7.5 Technical and Organisational Measures

Technical and organisational measures will be put in place prior to the launch of the app to ensure the information processed in relation to the COVID Proximity app is carried out only as detailed in this DPIA and ultimately only for the purposes intended. The DOH is designing, developing and putting in place the required organisational measures to ensure the privacy preserving approach to the app and the protection of the fundamental rights of individuals to privacy and data protection are established and maintained.

The organisational security measures implemented include the following.

- The DoH has engaged a specialist information security advisory at an early stage in the design, development, testing and operational planning of the app. The company providing this service is a National Cyber Security Centre (NCSC) approved service provider. Support has been provided directly by the NCSC, in oversight of penetration testing process, and advising on likely threats and mitigations.

Right to information – a Data Protection Privacy Notice (Notice) is provided via the app itself on those pages which request information and also in the app Settings. The Privacy Notice will also be published on the DoH website. The Notice contains information as prescribed under Article 13 and 14 of the GDPR.

Right to rectification – since no personal data is collected or retained by DoH, it would not be possible for DoH to comply with a request for rectification.

Right of access – since no personal data is collected or retained by DoH, it would not be possible for DoH to comply with a request for access.

Right to erasure – the user can select the Leave function, delete the app at any time, and delete ENS data via device settings – erasing all data processed on the phone. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for erasure.

Right to restriction – the user can revoke their ENS permission, revoke their exposure notification permission and decide not to upload keys. Ultimately the user can decide to Leave and/or delete the App from their device. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for restriction.

Right to portability – it is not possible for users to port their keys, for example, from one device to another device as the user does not have access to such keys on their device (save to delete them) and as regards those uploaded to the DoH, the DoH cannot identify which keys belong to which user. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for portability.

Right to object – the user can use the Leave function to delete the information from the app; the user can delete the app from their device and the user can delete ENS data via device settings.

Right not to be subject to solely automated decision-making including profiling – if the ENS detects a match between a Rolling Proximity Identifier on the App and a Diagnosis Key downloaded from DoH Diagnosis Key Registry, a decision is made that a close contact has taken place. This decision is based solely on the automated processing of identifiers and keys and does significantly affect users. However, this processing is based on the explicit informed consent of the user, during the on-boarding process. The automated decision-making is an essential feature of the proximity app solution provided, and is core to nits function in delivering the public health objective of infection control. If App users wish to speak to someone in relation to an 'Exposure Notification' that they have received via the App, they can call '0300 200 7896' and select the option to speak to someone about the notification at the following times: Monday-Friday (excluding bank holidays) between the hours of 830am – 530 pm. Someone will answer the call and explain the 'Exposure Notification'. They will have no way of knowing with whom, where or when the 'high risk' contact took place, but they will try to explain the process to App users and its purpose. **App users can express their point of view and contest the decision.** These steps should enable the App user to make an informed decision as to whether to self-isolate to prevent spreading the infection to others. Ultimately if they are still not satisfied or need clinical advice they will be advised to seek clinical assessment by their GP or GP OOH (See 'Appendix C').

7.7 International Transfers

There will be no international transfers of data. The AWS account is hosted in London region. The BSO servers infrastructure is hosted in Belfast. The backend integration with the ROI to support interoperability is hosted within the EU and is GDPR compliant. It appears likely that Germany will