THE CORONA WARNING APP IN GERMANY: DATA PROTECTION ASPECTS

PROF. DR. FRANZISKA BOEHM AND DIANA DIMITROVA

INTELLECTUAL PROPERTIES RIGHTS DEPARTMENT
FIZ-KARLSRUHE – LEIBNIZ INSTITUTE FOR INFORMATION INFRASTRUCTURE

July 2020

I. ABOUT THE GERMAN CORONA WARNING APP

In mid-June 2020, the German government released its Corona Warning App.[1] Within a short period of time, by July 6, the number of users had reached about 15 million.[2] The declared purpose of the app is to help users know whether they have had long enough contact to a person infected with COVID-19 and might thus be at risk of being infected. The broader goal is to break the infection chain.[3] The app is offered by the German government for free and it is an open source application.[4]It is available to both iOS and Android users.

Its main features are, according to the official governmental website, as follows.[5] When two smartphones which have installed the app "encounter" each other, they exchange random encrypted codes (rolling proximity identifiers) via Bluetooth. The app is thus supposed to know which phones were in promiximity to each other, for how long and what the distance was. On the basis of this information, the app calculates a risk score/level that someone might have infected himself through contact with an infected person. It is claimed that no identity information of the users of the app or their location is collected and exchanged. If a user has been tested positive for COVID-19, he/she may voluntarily enter the information that they are infected after it was certified that they are indeed infected. The user may then decide to trigger the notification process, whereby a pseudonymised code

1 Die Bundesregierung, „Corona-Warn-App," https://www.bundesregierung.de/breg-de/themen/corona-warn-app and Die Bundesregierung, „Corona-Warn-App: Die Wichtigsten Fragen und Antworten," https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-faq-1758392. For more technical information see Corona-Warn-App Open Source Project, https://www.coronawarn.app/de/#privacy; and Corona-Warn-App Solution Architecture, https://github.com/corona-warn-app/cwa-documentation/blob/master/solution_architecture.md.

2 Robert Koch Institut, „Infektionsketten digital unterbrechen mit der Corona-Warn-App," https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html.

3 Die Bundesregierung, „Corona-Warn-App," https://www.bundesregierung.de/breg-de/themen/corona-warn-app.

4 Corona-Warn-App Open Source Project, „Häufig gestellte Fragen zum Corona-Warn-App-Projekt," https://www.coronawarn.app/de/faq/#application.

5 Die Bundesregierung, „Corona-Warn-App," https://www.bundesregierung.de/breg-de/themen/corona-warn-app.

associated with their phone/app and the positive result of the test are sent to the central server, which forwards this code to the other app users. The apps on the different smartphones check whether the code is registered in the anonymous log of the encounters on the app for the past 14 days. This processing takes places locally, i.e., entirely on the smartphone via the decentralised software architechture.

II. CORONA APPS AND DATA PROTECTION ISSUES

Since the Corona outbreak, the broader academic, NGO and data protection regulatory communities have issued a high number of critical analysis and recommendations with regard to the different corona tracing apps.[6] In April 2020 the IGR Team at FIZ Karlsruhe identified the major data protection problems in the framework of the first proposals for Corona related apps or the first operational apps across Europe. On the basis of the main identified issues and taking into account the provisions of the GDPR, it made a list of recommendations for compliance of Corona apps with the GDPR.

Briefly, FIZ Karlsruhe concluded that Corona tracing apps should: (1) have a valid legal basis for processing; (2) be secure and private by design; (3) allow access to the processed data only to authorised persons and on a need-to-know basis; (4) data should be processed locally on the device and centralized storage should be avoided; (5) there should be deleting/dismantling possibilities for the app as a whole; (6) there should be possibilities for data deletion/anonymisation; (7) the processing of personally identifiable information should be avoided and re-identification risks should be reduced; (8) data flows should be transparent; (9) apps should allow data subjects to exercise their data subject rights; (10) there should be adequate safeguards; (11) should data be re-used for other purposes, this reusage should comply with the GDPR; (12) before an app becomes operational, a Data Protection Impact Assessment (DPIA) should be carried out; (13) the app should process accurate input data and produce accurate results; (14) the usage of the app should be voluntary.

III. THE GERMAN CORONA WARNING APP AND DATA PROTECTION

The following paragraphs will examine whether the German Corona Warning App app complies with the above recommendations. For better flow of the text, the above recommendations will be examined in a different order and some points will be merged.

1. Anonymous and pseudonymous data

According to the available information, the app does not collect personal information such as name, e-mail address or tephone number when users register. It is understood that it does not collect location data or track the movements of its users. The randomly generated codes are anonymous and in case someone gets a warning that they have been in contact with an infected person, the app does not allow app users to know which person that was, and the infected person does not know to which other app users their anonymous code will be disclosed. [7] For data protection reasons the app does not give real-time warnings.[8]

However, it seems to be the case that the users are rather pseudonymous instead of anonymous.[9] This is especially because a person may register in the app the fact that they have taken a test. This allows them to receive a QR code with

6 VUB/LSTS, „Contact Tracing Apps," https://lsts.research.vub.be/en/corona-apps.

7 Robert Koch Institut, „Infektionsketten digital unterbrechen mit der Corona-Warn-App," https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html, See in the drop-down menu, „Warum die Daten der Nutzerinnen und Nutzer sicher und geschützt sind."

8 Corona-Warn-App, „Bericht zur Datenschutz-Folgenabschätzung für dieCorona-Warn-Appder Bundesrepublik DeutschlandVersion 1.0.1, 18.06.2020," https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf, p. 45.

9 Robert Koch Institut, „Infektionsketten digital unterbrechen mit der Corona-Warn-App," https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html, See in the drop-down menu, „Warum die Daten der Nutzerinnen und Nutzer sicher und geschützt sind."

the result of the test via the app if the health institution carrying out the test is connected to the app. If it is not connected, the app user may request a Transaction Number (TAN) from the Robert Koch Institute (RKI) via a telephone hotline if he provides the RKI his phone number and possibly additional information such as his name in order to allow the RKI to allocate his test result.[10] This is to ensure that it is officially confirmed that the given app user is indeed infected.[11] If the app user has been tested positive, and decides to make this information available to the app, then the app will know the test result. The apps of those users who choose to trigger the notification process will send a code to the central server which will then send it to the other app users.[12]

According to the data protection notice, information that someone has been in contact with an infected person, information that someone has taken a COVID-19 test and information that the test is positive is treated as health data in the sense of Article 9 GDPR and is thus considered tob e sensitive information.[13]

Therefore, one cannot argue that the data processing via the app is exclusively anonymous. On the other hand, it is noted that, in comparison to other apps, the amount of pseudonymised and anonymised data as processed by the app is minimal and seems to have been selected exclusively in relation to the purpose of the processing.

2. Legal basis

The usage of the app, the decision to allow it to communicate with other devices via bluetooth, the decision to enter in the app information about the fact that a COVID-19 test has been made and the result of the test, are based on the user's consent as per Article 6 1 (a) and Article 9 (1) (a) GDPR. It is explicitly stated that the consent may be revoked at any time. [14] According to the DPIA drafted for the contact tracing app, other legal bases were also considered. However, it was concluded that relying on other legal bases might have prejudiced the voluntary nature of the app usage.[15]

As to whether the usage of the app can be practically always voluntary, according to some media reports this might not always be the case, especially in an employment context. Thus, according to certain lawyers, employers may sometimes order employees to use the app "in the case of purely business mobile phones and frequent contacts with colleagues and customers." [16] However, this raises the question of whether this might be legal under both employment and data protection laws, and should this be the case – it is questionnable whether in these cases it is the consent of the user/employee which can be relied on as a legal basis.

3. Controller

The designated controller for the processing of data by the app is the Robert Koch Institute (RKI). As explicitly mentioned, it is responsible only for the data processed via the app and not for those processed by the smartphones themselves, which might also collect logs of the encounters, in which case Google and Apple remain responsible. The data protection notice also guides users into finding the features of their phones which are connected to the app and how they can delete their logs from the phone.[17] The owner of the

10 These steps are to ensure that people will not misuse the app to send fake notifications on purpose. „Datenschutzerklärung Corona-Warn-App," https://www.coronawarn.app/assets/documents/cwa-privacy-notice-de.pdf, p. 4-6.
11 „Corona-Warn-App starts in Germany," *Berlin.de*, https://www.berlin.de/en/news/coronavirus/6204357-6098215-corona-warn-app-starts-in-germany.en.html.
12 „Datenschutzerklärung Corona-Warn-App," https://www.coronawarn.app/assets/documents/cwa-privacy-notice-de.pdf, p. 4-6.
13 „Datenschutzerklärung Corona-Warn-App," https://www.coronawarn.app/assets/documents/cwa-privacy-notice-de.pdf, p.3.
14 Ibid, p. 1 -2.
15 Corona-Warn-App, „Bericht zur Datenschutz-Folgenabschätzung für dieCorona-Warn-Appder Bundesrepublik DeutschlandVersion 1.0.1, 18.06.2020," https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf, p. 83 ff.
16 „Corona-Warn-App starts in Germany," *Berlin.de*, https://www.berlin.de/en/news/coronavirus/6204357-6098215-corona-warn-app-starts-in-germany.en.html.
17 „Datenschutzerklärung Corona-Warn-App," https://www.coronawarn.app/assets/documents/cwa-privacy-notice-de.pdf, p.1, 3 and 8

app software is SAP.[18] The DPIA indicates that because of the role of the verification hotline, operated by RKI in processing information to confirm the positivie result of those who who do not have a QR code, the hotline is part of the whole process.[19] Thus, it is assumed that the RKI is also the controller in relation to the hotline.

It is positive that the controller is clearly designated and that the data protection notice is transparent about the fact that Google and Apple also collect data, for the processing of which they are a designated controller. It is also welcome that the controllership responsibilities of RKI, on the one hand, and those of Google and Apple, on the other hand, are clearly separated.

4. Transparency

In terms of transparency in relation to the different data processing aspects of the app, it is noted that there is a publicly available detailed privacy notice, a data protection impact assessment and further information on the website of the RKI and the German government. Information on who was involved in the development of the app is also disclosed.[20] The contact details of the data protection offcer at RKI and BfDI are also made available.[21] The privacy notice indicates that data will not be disclosed to third parties beyond communicating the random code of infected persons to other app users, unless RKI would be legally requested to disclose information in case of attacks on the system.[22] As to the data processed by Apple and Google, the privacy notice indicates that users should consult the data protection notices of these companies.[23]

5. Accuracy

The RKI acknowledges that there are certain accuracy weaknesses with regard to the Bluetooth contact function. The most commonly cited problem is that sometimes proximity may be calculated wrongly or a certain encounter might remain unregistered. Another limitation is that the success of the app and the accuracy of calculating the risk of being infected are determined by how many people will be using the app and decide to disclose the fact that they have been infected.[24] Furthermore, we argue that the accuracy of the assessment of the level of the risk that someone has become infected will depend also on the abstract criteria and parameters for this assessment,[25] as the algorithm is developed and updated by RKI.[26] Therefore, the success of the app in creating accurate warnings and thus achieving the overall goal of breaking the infection chain is largely determined by the accuracy of the technology, e.g., how accurately it collects the input information, assesses it on the basis of the algorithm and returns correct results.[27] Therefore, accuracy issues should be closely monitored and if serious problems are identified, they should be either fixed or the app should stop operating.

A positive measure in terms of accuracy is the verification mechanism that someone has indeed tested positive for COVID-19 via the QR code or the verification hotline if no QR code is available.[28] In this way the system is expected to prevent abuse of the app by people who are actually not infected but try to enter a false diagnosis and trigger unnecessary warnings.

18 „Corona-Warn-App Nutzungsbedingungen," https://www.coronawarn.app/assets/documents/cwa-eula-de.pdf, p. 8.
19 Corona-Warn-App, „Bericht zur Datenschutz-Folgenabschätzung für die Corona-Warn-App der Bundesrepublik Deutschland Version 1.0.1, 18.06.2020," https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf, p. 42.
20 Corona-Warn-App Open Source Project, „Open-Source-Projekt für Corona-Warn-App," https://www.coronawarn.app/de/ (See bottom of the page).
21 „Datenschutzerklärung Corona-Warn-App," https://www.coronawarn.app/assets/documents/cwa-privacy-notice-de.pdf; p. 1 and 11.
22 Ibid, p. 9-10.
23 Ibid, p. 3.
24 „Corona-Warn-App Nutzungsbedingungen," https://www.coronawarn.app/assets/documents/cwa-eula-de.pdf, p. 2 and 7.
25 See a similar argument from the profiling in the frameowrk of Passenger Name Record (PNR), Case *Opinion 1/15* of the Court (Grand Chamber) (2017), ECLI:EU:C:2017:592 (Canada PNR Opinion), par. 172.
26 „Datenschutzerklärung Corona-Warn-App," https://www.coronawarn.app/assets/documents/cwa-privacy-notice-de.pdf, p. 4
27 Some problems have been reported already: Dietmar Neuerer, „Corona-Warn-App: Nutzen der Anwendung nur schwer ermittelbar," *Handelsblatt*, 03. 07. 2020, https://www.handelsblatt.com/politik/deutschland/kampf-gegen-corona-corona-warn-app-nutzen-der-anwendung-nur-schwer-ermittelbar/25965796.html?ticket=ST-7791611-OUdJ3BN2BLWHwOQOm2gE-ap3.
28 Corona-Warn-App, „Bericht zur Datenschutz-Folgenabschätzung für die Corona-Warn-App der Bundesrepublik Deutschland Version 1.0.1, 18.06.2020," https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf; p. 65.

6. Data storage

According to the data protection information notice, the data processed via the app is stored only in Germany or in another EU or European Economic Area (EEA) Member State.[29] Therefore, the data is not supposed to be processed outside the European Union/EEA. However, if data collected via the app is also processed by Google and Apple, as indicated above, this might mean that data which is processed by the smartphone but not the app might be processed outside the EU/EEA. This should be clarified and communicated to the app users.

As to the storage deadlines, it is indicated that the rolling proximity identifiers are deleted automatically from the app after 14 days. However, the storage duration of information concerning the encounters (e.g. duration of contact, etc) which is stored on the contact protocol of the smartphone is determined by Google and Apple. Reportedly, currently it is 14 days. Options for manual deletion are reportedly available.[30]

The risk level of an app user, as assessed by the app, is stored until the next assessment takes place, i.e., until the new list of rolling proximity identifiers of those infected has been sent.[31]

The hashed identifier of the registered test is stored for 21 days. In case of a negative result, the hashed ID is deleted immediately after the test result has been received by tha app. In case of a positive result, this hashed ID is deleted when the stored copy of the TAN is deleted from the server. The token which is stored on the server is stored for 21 days. The token which is stored on the app is deleted when the app is deleted or when the user triggers the notification button. In cases of triggering the notification, the rolling proximity identifiers, TANs and the token which is stored on the server are deleted from the server after 21 days.[32] The telephone number which users provide the verification hotline is deleted within one hour.[33]

We argue that the mentioned deadlines seem to be realtively short and well adjusted and proportionate to the purpose for which they are processed. Especially the 14 day deadline, the period within which it is said that one may feel the COVID-19 symptoms and would usually get a test, seems to be appropriate.

7. Central vs de-central storage

It is noted that the app relies mainly on de-centralised storage. However, there is a central server as well. The latter is needed in order to process the (anonymous) identifiers of those who were tested positive, whereas the matching of these identifiers against the list of the encounters of each app user is performed on the app of those users.[34]

The fact that the app does not rely on a completely centralised architecture is positive because it gives app users more control over their data and prevents from illegal access and misusage of the information for incompatible purposes by the controller or third parties.

8. Other data subjects rights

The data protection notice mentions clearly the applicability of the rights of the data subjects – access, rectification, erasure, partability, restriction of processing and the right to obejct. It clarifies that due to the pseudonymous/ anonymous processing, these rights might not be exercised without the provision of additional information to enable RKI to identify the data of

29 „Datenschutzerklärung Corona-Warn-App," https://www.coronawarn.app/assets/documents/cwa-privacy-notice-de.pdf, p. 10.
30 Ibid, p.8.
31 Ibid.
32 Ibid, p.9.
33 Corona-Warn-App, „Bericht zur Datenschutz-Folgenabschätzung für die Corona-Warn-App der Bundesrepublik Deutschland Version 1.0.1, 18.06.2020,"https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf, p. 54.
34 „Corona-Warn-App starts in Germany," *Berlin.de*, https://www.berlin.de/en/news/coronavirus/6204357-6098215-corona-warn-app-starts-in-germany.en.html; Corona-Warn-App, „Bericht zur Datenschutz-Folgenabschätzung für die Corona-Warn-App der Bundesrepublik Deutschland Version 1.0.1, 18.06.2020," https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf, p. 58.

the individual wishing to exercise his rights.[35] The privacy notice and the DPIA do not clarify that the right not to be subject to automated decision-making, including profiling, unless an exemption such as consent applies, is also applicable. However, bearing in mind that the RKI criteria will calculate some risk score as to whether someone has come into contact with the virus, this could be considered to be profiling in the sense of the General Data Protection Regulation (GDPR).[36] This should be expressed more clearly.

9. DPIA

It is welcome that an extensive and comprehensive DPIA in relation to the Corona Warning App has been carried out and published. It contains a detailed technical description of the app, an elaborate legal analysis, including the data protection risks and security and privacy-by-design measures.[37] It explicitly calls for a periodic re-assessment as to whether there is a continued necessity to operate the app, e.g. when one day the pandemic will be considered to be over, and possibly end the operation of the app. In addition, the DPIA recommends that an ongoing evaluation of the accuracy of the BLE contact tracing be carried out.[38]

IV. CONCLUSION

We conclude that the German Corona Warning App appears to ensure a high level of data protection. First, because it processes the data either in anonymous or pseudonymous form and these are stored for a very short period of time. Second, it is an open source app. Third, its architecture relies on both central and de-centalized data storage. However, it is noted that the centralised storage concerns only the anonymous IDs of those who were tested positive and chose to notify the other app users of their infection. Fourth, the government and RKI seem to have provided detailed information related to the app and the data processing related to it, including a comprehensive Data Protection Impact Assessment (DPIA).

We note that whereas we did not assess the security features of the app. However, the involvement of the Federal Office for Information Security signals that security features have been carefully assessed and implemented.[39]

We recommend that despite the anonymous/pseudonymous features of the app, it could be clarified that the assessment of the risk that one might have come in contact with an infected person could be considered to be profiling in the sense of the GDPR. Users should also be informed clearly if Google and Apple transfer their (anonymous) information outside the EU/EEA.

In addition, it should be clarified if employers may request their employees to install and use the app.

Finally, it is very important to monitor the accuracy of the processing of the information via the app and the appropriateness and accuracy of the algorithm, and to measure the overall success of the app in achieving its designated goal of breaking the infection chain. This should contribute to the necessity of the continual operation of the app.

35 „Datenschutzerklärung Corona-Warn-App," https://www.coronawarn.app/assets/documents/cwa-privacy-notice-de.pdf; p.11.
36 See Article 4 (4) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88: „'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;"
37 Corona-Warn-App, „Bericht zur Datenschutz-Folgenabschätzung für die Corona-Warn-App der Bundesrepublik Deutschland Version 1.0.1, 18.06.2020," https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf.
38 Ibid, p. 115-116.
39 Die Bundesregierung, „Corona-Warn-App: Die Wichtigsten Fragen und Antworten," https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-faq-1758392.