EXTERNAL

Information from the processor to the joint controllers regarding the European Federation Gateway Service for the purpose of their Data Protection Impact Assessments (DPIA-Draft)

Version 1.4

1. Disclaimer

This document contains version 1.4 of DPIA-Draft regarding the European federation gateway Service (EFGS). This document incorporates by reference further documents as explained in section 11. It was prepared by the European Commission and its contractors in order to fulfil the Commission's obligation resulting from Annex III paragraph 12 of the Commission Implementing Decision (EU) 2020/1023. that stipulates that the European Commission shall support the Member States by providing information concerning the federation gateway, in order to implement the obligations pursuant to Articles 32, 35 and 36 of the General Data Protection Regulation. It is to be highlighted that this document is not a self-standing DPIA, but it is a supporting document from the processor (the European Commission) for the benefit of the joint controllers that they may use when carrying out their DPIAs, as remains their responsibility.

As a result of the expected rapid technical development of the EFGS, this document will also be subject to updates. Accordingly, the present document is subject to change once the EFGS itself is modified in a way that is relevant regarding the assessments contained herein.

The current version is based on the state of development of the 28.09.2020. The change history is shown in table form below.

This document was created by SAP SE and T-Systems International GmbH for the benefit of the European Commission and the joint controllers as documentation. This document does not assume the role of data protection impact assessment by the joint controllers, this role being reserved for documents by the joint controllers which they may - at their discretion - base on this document.

Any legal opinions and considerations expressed in this document as well as any legal conclusions and assessments made do not constitute legal advice. Rather, they are intended to enable the technical or legal reader to assess and to form an opinion regarding the concepts pursued in order to ensure compliance with the GDPR, the EU-DPR, Article 16 TFEU and Article 8 Charter.

The present document is based - insofar as the functionality, data processing and scope of data processing in the exposure notification tool (ENF) by the providers Apple and Google is described - on the available data protection concept and further documentation regarding EFGS frameworks.

The authors are unable to perform an in-depth investigation of the internal functioning of these frameworks and to ascertain the correctness of their documentation. The frameworks are implemented in a way that precludes this type of investigation by the authors. In this respect, the correctness of the processing of personal data in these frameworks and their documentation has been relied upon in the preparation of this document, just as the correctness of the data processing and its documentation must be relied upon in the operation of the frameworks. In any event, this document may not be relied on as a guarantee, binding description or assertion of pertinent knowledge regarding the correctness of the processing of personal data in Apple's and/or Google's implementation of the ENF or their respective documentations.

The considerations regarding the EFGS are based on privacy and data protection law as well as the data subject's right to the protection of personal data. This document therefore contains considerations regarding data security, but more detailed security considerations and measures can be found in the EFGS security concept.

In so far as gender-specific spelling is used in this document, it is intended for the sole purpose of improving readability. All personal designations in this document are therefore to be understood as gender-neutral.

The rights to copy, distribute, modify and make available online regarding this document and annexes are limited with regard to the operation of the EFGS and the use by the member states. This includes licenses for the member states to use the documents in order to meet their obligations concerning

their own national corona contact tracing systems, including the reuse or translation of the documents mentioned above or parts thereof.

2. Change history

Version.	Date	Content
0.1	22.08.2020	Initial creation
0.2	23.08.2020	First draft of single chapters
0.5	25.08.2020	First draft of whole document
0.8	29.08.2020	Incorporate remarks of EU Commission
1.0	30.08.2020	Second Draft for EU Commission
1.1	12.09.2020	Incorporate further risks and design decisions
1.2	14.09.2020	draft (V 1.2)
1.3	28.09.2020	Incorporate comments of SANTE – Draft (V1.3)
1.4	07.10.2020	Updated final draft (V1.4)

3. Table of contents

4. List of figures

5. List of tables

6. Authors

Name	Company
Kerstin Harzendorf	T-Systems Multimedia Solutions GmbH
Susanne Koch	T-Systems Multimedia Solutions GmbH
Martin Schick	Attorney for T-Systems International GmbH
Sandy Schöne	T-Systems Multimedia Solutions GmbH
	T-Systems Multimedia Solutions GmbH
Benny Rolle	SAP SE
Tobias Schmidt	SAP SE

7. Introduction

The purpose of this document, referred to as DPIA Draft, is 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[1] for the exchange of personal data via the European Federation Gateway Service (EFGS).

In order to facilitate the cross-border interoperability of national contact tracing and warning mobile application, a digital infrastructure, referred to as European Federation Gateway (EFGS), was developed with the support of the European Commission by the member states participating in the eHealth Network. They decided to advance their cooperation on a voluntary basis, in order exchange relevant data between them[2].

This DPIA-Draft has been started well before the start of processing and incorporated into the EFGS's development process. Therefore, potential risks for data subjects' rights and freedoms were assessed at time when the means of processing were designed. This DPIA was not an ad-hoc or random exercise. It had a structural place in the project and its' processes. It is not intended as a static document and is going to be subject to modifications during the project (particularly when risks are changing).

According to Article 25 (1) GDPR appropriate technical and organisational measures are implemented to minimize the risks assessed, referred to as "design decisions". The design decisions are described in Annex 2.

The DPIA-Draft includes a description of the envisaged processing operations and the purposes of the processing, an assessment of the necessity and proportionality of the processing, an assessment of the risks to the rights and freedoms of data subjects and the measures envisaged to address the risks.

[1]According to the Commission Implementing Decision (EU) 2020/ 1023 p. 1:

"(10) The participating Member States, represented by the designated national authorities or official bodies determine together the purpose and means of processing of personal data through the federation gateway and are therefore joint controllers.".

8. General information/joint controllership

Record reference	*(Automatically assigned by the system upon creation of a record (e.g., 1234.1)*
Title of the processing operation	*European Federation Gateway Service (EFGS)*
Controller entity	*The participating Member States having joined the EFGS are joint controllers.*
Joint controllers	☐N/A ☒ YES, fill in details below
Names and contact details of respective joint controllers	*Click here to enter text.*
Main responsibilities of each of the controllers	According to Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic, OJ L 227I , 16.7.2020, Annex II: - division of diverse responsibilities according to (1) (1), - handling requests of and informing data subjects ((1) (2)), - management of security incidents, including personal data breaches (2) - Data Protection Impact Assessment (provide information to another controller) (3).
Joint controllership	☒ Link: Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic, OJ L 227I , 16.7.2020, p. 1–9. ☒Attachment

	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.LI.2020.227.01.0001.01.ENG
Processor(s)	☐N/A ☒ YES, fill in details below
Internal organisation(s)/entity(ies) Names and contact details	☐N/A ☐ YES *Click here to enter text.*
External organisation(s)/entity(ies) Names and contact details	☐N/A ☒ YES *European Commission*
Contract with the processor, or other legal act under EU or MS law	☒Link: Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic, OJ L 227I , 16.7.2020, p. 1–9. ☒Attachment https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.LI.2020.227.01.0001.01.ENG
Planned review of the DPIA	*The DPIA should be reviewed periodically and the processing should be re-assessed regularly, at least when there is a change of the risks posed by processing the operation.* *Date*

Table 1: General information / joint controllership

9. Preparation of the DPIA-Draft

9.1. Description

According to WP 248[3]"the DPIA should be started as early as practical in the design of the processing operation even if some of the processing operations are still unknown. As the DPIA is updated throughout the lifecycle project, it will ensure that data protection and privacy are considered and promote the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses because the selection of certain technical or organizational measures may affect the severity or likelihood of the risks posed by the processing."

Therefore, the DPIA-Draft is carried out accompanying the development of the EFGS by the service providers. Risks for rights and freedoms of the data subjects were listed, described and determined in the course of the project. Countermeasures were discussed and incorporated in design decisions, considering the state of the art and the nature, scope, context and purposes of processing personal data (according to Article 25 GDPR).

The risks were listed in a risk matrix, an Excel-worksheet named "risk analysis", in order to carry out an overall risk assessment as described below (see section 14).

Particularly pertinent security risks were addressed to architecture and development workstreams of the EFGS' developing process. Therefore, daily meetings with representatives of the workstreams took place.

Results of the consulting by the DPIA team were considered when drafting the technical and organisational measures of the service providers.

9.2. Stakeholder engagement

9.2.1. Roles

According to the European Data Protection Boards' (EDPB') Statement on the data protection impact of the interoperability of contact tracing apps[4], the roles and responsibilities of the different actors involved in any processing were considered when designing.

9.2.2. View of data protection officer

The joint controller must seek the advice of the Data Protection Officer (DPO), where designated (Article 35(2) GDPR). The DPO' advice and the decisions subsequently taken, should be documented within the DPIA.

The DPO should also monitor the performance of the DPIA according to Article 39(1)(c) GDPR.

9.2.3. Views of data subjects or their representatives

See section 12 below.

9.2.4. "DSFA Team"

[3]Article 29 Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/67, WP 248 rev.01, p. 13

[4]Statement on the data protection impact of the interoperability of contact tracing apps, 16 June 2020, paragraph 13

In workshops on 21stAugust 2020 and 26thAugust 2020 an overall risk assessment for the identified risks was carried out by T-Systems and SAP in order to provide the results as assistance for the DPIAs of the joint controllers (according to Article 28 (3) (f) GDPR).

The assessment was carried out by an interdisciplinary team of experts in different relevant fields (IT-Architects, technicians, IT-Security- and data protection experts, developer and lawyer).

The method of risk assessment is described below (section 14).

10. Identification of high-risk processing operations and requirements for a data protection impact assessment (DPIA)

10.1. Pre-assessment

This section describes the requirements for the necessity of a DPIA in case a type of processing is using new technologies and is likely to result in a high risk to the rights and freedoms of natural persons.

According to the statement of the EDPB any operation or set of operations that pursue the purpose of ensuring the interoperability of contact tracing applications in addition to the processing on the member state level has to be assessed separately from prior or subsequent processing operations because of the additional purpose. Therefore, this additional processing should be a separate processing[5].

An additional DPIA has to be carried out when this additional processing is "likely to result in high risks".

Article 35(3) GDPR provides some examples when a processing is "likely to result in high risks", in particular:

> *"(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*
>
> *(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*
>
> *(c) a systematic monitoring of a publicly accessible area on a large scale".*

In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, the following criteria were developed by the Article 29 Working Party[6]:

- Criterion 1 – Evaluation and Scoring
- Criterion 2 – Automated-decision making with legal or similar significant effect
- Criterion 3 – Systematic monitoring
- Criterion 4 – Sensitive Data or data of a highly personal nature
- Criterion 5 – Data processed on a large scale
- Criterion 6 – Matching or combining datasets
- Criterion 7 – Data concerning vulnerable data subjects
- Criterion 8 – Innovative use or applying new technological or organisational solutions

[5] EDPB's Statement on the data protection impact of the interoperability of contact tracing apps, 16 Juni 2020, paragraph 14

[6] WP 248, p. 9

- Criterion 9 – Data transfer across borders outside the European Union
- Criterion 10 - the processing itself prevents data subject from exercising right or service.

In a preliminary assessment of the processing activities in the EFGS, the criteria1, 4, 5, 6, 7, 8 were fulfilled. A detailed description of the processing activities and, the processed personal data follows below (see section 11).

The WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA[7]. As a rule of thumb, a processing operation meeting less than two criteria may not require a DPIA due to the lower level of risk to the rights and freedoms of data subjects. Any processing operation that exceeds these two criteria is assumed to present an increased risk, and therefore to require a DPIA.

10.2. Overall result of risk level assessment

In consequence, 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.

Furthermore, in the present context, the necessity of a Data Protection Impact Assessment is stipulated by all stakeholders and the European Data Protection Board (EDPB) opines that a DPIA must be carried out before implementing "*such tool*"[8]. The EFGS is considered to be such a tool, because cross-border processes concern an increasingly high quantity of data and create new risks for data subjects.

11. Description of the processing operations

11.1. Context

The processing in the EFGS is required to describe the functions, architecture and data flow.

11.2. Purpose and description of the processing

11.2.1. Purpose

The processing in the EFGS pursues a specific and legitimate purpose. The purpose of the 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. The pursuit of this purpose permits enabling the cross-border interoperability of the national contact tracing and warning mobile applications for the COVID-19 pandemic within the territory of the European Union.

11.2.1.1. Legitimacy of the purpose

The support and facilitation of the exchange of information among member states is a legitimate concern of the European Union according to Article 14 (1) of the directive 2011/24/EU. It serves to establish a high level of human health protection according to Article 168 (1) TFEU as an act of the Union complementing member states' policies in the pursuit of improving public health and fighting against major health scourges.

According to current epidemiological knowledge, the COVID-19 pandemic is a fast spreading, contagious disease with the potential to threaten life and health of the population of the European

[7] WP 248, p. 9f.

[8] EDPB guideline 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, p. 39

Union to a major degree. The contagiousness results in an eventual high rate of infection, especially in a mobile population. According to Articles 20 (2), lit a), 21 (1) TFEU the mobility of the citizens of the European Union is one of the rights fundamental to the citizenship of the European Union.

In order to curb the rate of infection with the COVID-19 virus, several member states have introduced mobile applications that enable contact tracing and warning functions regarding infections with COVID-19. These mobile applications serve to facilitate an early break of an eventual infection chain. With regard to the mobility of the citizens of the European within the territory of the European Union, such mobile applications offer the potential to enable an early breaking of infection chains beyond the national borders of the member states. It is therefore beneficial and legitimate vis-à-vis the goals agreed in Article 168 (1) TFEU to enable the cross-border interoperability of the national contact tracing and warning mobile applications for the COVID-19 pandemic within the territory of the European Union by means of an exchange of information among member states according to Article 14 (1) of the directive 2011/24/EU.

11.2.1.2. Specificity of the purpose

This purpose is specific both regarding its subject and its temporal extent.

11.2.1.2.1. Subject related specificity of the purpose

Under Article 7a (1) of the Implementing Decision (EU) 2020/1023, the purpose of the processing in the EFGS is limited to the enabling of interoperability of those mobile applications that the member states operate in order to facilitate the breaking of infection chains of the COVID-19 virus. Thus, the purpose is highly limited subject-wise and its achievement can be monitored by the incidence of infections with the COVID-19 virus in the territory of the European Union. The effectiveness of the interoperability can be ascertained by the observation of the occurring infection chains, their length and the incidence of their termination, including the observation of the means of discovery. The latter observations can only be performed outside the operation of the EFGS and the member states' mobile apps since these mobile apps do not collect the relevant statistical data for reasons of privacy preservation. These observations are therefore outside of the scope of the processing by the EFGS.

11.2.1.2.2. Temporal specificity of the purpose

The purpose of the processing of personal data in the EFGS carries a temporal limitation in itself: Once the incidence of infections with the COVID-19 virus is low and remains foreseeably low, the processing of the personal data in the EFGS is no longer effective and is no longer required to help break infection chains. Article 7a(7) of Implementing Decision 2020/1023 stipulates a termination clause for the gateway, imposing that the gateway *"be deactivated at the latest 14 days after all the connected national contact tracing and warning mobile applications cease to transmit keys through the federation gateway."* Consequently, the purpose is limited and specific regarding its temporal application.

11.2.2. Processing for further purposes

☒N/A

☐ Yes, if so, specify the purpose:

☐ Archiving in the public interest

☐ Scientific or historical research purposes

☐ Statistical purposes

11.2.3. Safeguards in place to ensure data minimisation/purpose limitation

☒ Pseudonymisation

☒ Any other

Description of the requirements according to Article 5 (1)(b) GDPR and their observance (purpose limitation).

11.2.4. Modes of processing

1. ☐ Automatic processing (including automated individual decision-making, including profiling (Article 24))
   ☒ Computer/machine
   ☐ Any other, specify
2. ☐ Manual processing
   ☐ Word documents
   ☐ Excel sheet
   ☐ Any other, specify
   Click here to enter text
3. ☐ Any other mode, specify

11.2.4.1. Description

Find the comprehensive description of the data points being processed by the system and their way through the system (Data Flow) and of the data processing below (p. 8.4, 8.5)

11.2.5. Storage medium

11.2.5.1. Checklist

1. ☐ Paper
2. ☒Electronic
3. ☒Databases
4. ☐ Word documents
5. ☒ Servers
6. ☒ External contractor premises
7. ☐ Cloud
8. ☐ Others, specify

11.2.5.2. Description

Find the comprehensive description of the data points being processed by the system and their way through the system (Data Flow) and of the data processing below (section 11.4, 11.5).

11.3. Functional description

Most European countries are using the Exposure Notifications API by Google and Apple for contact tracing. While the proximity detection mechanisms of these apps are compatible, the national back-ends behind the different national apps do not talk to each other yet. This is unfortunate as Europeans commute and travel all over the EU/EEA. Therefore, interoperability of the national back-ends is essential and that is where the EFGS comes into the picture.

All apps in the EU/EEA using the Exposure Notification Framework (ENF) by Google and Apple for proximity detection can join the network. Fortunately, most European countries have subscribed to this approach. If two citizens, no matter where they are from, are using such an app, the framework detects proximity and duration of contact in a non-traceable manner on both devices.

There are two different scenarios that should be distinguished in order to understand the reason for the architecture of the EFGS.

In the first case, the citizen travels from Member State A to Member State B. Later, he gets a positive test result and wants to warn the citizens in Member State B. When uploading his diagnostic keys via his national app, he therefore voluntarily adds as "country of interest" the member state B. The information about the "countries of interest" is attached to the diagnostic keys and sent to the national back-end. The back-end also adds the information "country of origin" to the keys and forwards it to the EFGS. The EFGS provides the keys of the last 14 days of all participating countries for download to the connected national back-ends. By the information "country of interest" the back-end of member state B knows that these diagnostic keys must be made available to all users of its country. They are therefore made available for download "in one pot" together with the national diagnostic codes. All other member states recognize by means of the "country of origin" from which country the keys come and make them available for download to their users in their national back-end, sorted by origin. From there, however, they will only be retrieved on demand. This is explained in more detail in the next example.

In the second case, the user from member state B stayed at home, but e.g. because he lives in a large city visited by many tourists he is concerned that he had contact with a person who was tested positive and does not use the national app, but the app of another member state. This user can indicate in his app which countries he is interested in for the diagnostic keys by choosing “the countries of interest”. The national back-end creates a folder for the keys of each participating member states by the information “country of origin” and makes the keys available. The national app makes a request to the back-end and downloads the keys the user is interested in. The ENF that runs on the mobile device then compares whether the user had a dangerous contact with the owner of one of the downloaded keys.

Due to the architecture of the EFGS, the user cannot restrict sharing to certain member states. All connected member states download all diagnosis keys available for Europe.

So, the main purpose of the EFGS is to provide the new diagnosis keys to all citizens of the participating countries. All countries upload their new diagnosis keys to the EFGS which stores the keys and provides them for download for the national back-ends. That's why a direct back-end-to-back-end communication between the national back-ends is not necessary.

Google and Apple defined an exposure key export file format[9]. Each national back-end can transfer exchange information for diagnosis keys in this GAEN TEK format including “country of origin” and “countries of interest”, key by key in a batch to the Federation Gateway Service.

Since only specific back-ends can communicate with the EFGS, each back-end has to provide – with its payload – security measures as certificates and signatures. During the upload, the uploader identity is extracted from the client certificate. If the client certificate is valid, the submitted content is validated, split, and stored in the database. The size of the payload is limited to avoid requests that are too large.

[9] https://developers.google.com/android/exposure-notifications/exposure-key-file-format.

When a batch of diagnosis keys is received, the EFGS stores each key set as a single small document. This avoids query performance gaps, ensures flexibility, and makes it easier to query the data.

The documents need to be split into batches to minimize download problems. During upload, the EFGS bundles incoming documents into batches of a fixed size so that downloads are split into bite-sized chunks – the batches – by design. After the upload is complete, the documents are marked with a unique batch tag.

The national back-end now triggers the download of stored diagnosis keys.

The download is triggered by calling the download URL with the batch tag of the last query. If the client certificate is valid and the requested content type is available, the data will be queried and transformed into the response.

If a download is triggered, there might be thousands of diagnosis keys available, so that the EFGS API just returns the first batch with a tag. The same download call is then repeated but includes the received tag so that the next batch is returned.

To obtain all data, the download operation needs to be performed multiple times if the number of batches exceeds one. The last call is empty and returns the same timestamp as requested.

Each national back-end then is responsible for packing and publishing keys for their own citizens. The implementations of the various national back-ends can be different and is not part of the scope of this description.

11.4. Architecture

11.4.1. Introduction

11.4.1.1. About this section

This section describes the architecture of the European Federation Gateway Service (EFGS); the usage scenarios that require cross-border exchange of diagnosis keys; and how the EFGS can be integrated with the back ends of national corona warning systems.

The European Commission adopted a recommendation[10] to support mitigation strategies for the corona virus pandemic through mobile data and applications. The member states in the eHealth Network, supported by the Commission, adopted an EU toolbox[11] on mobile applications setting out a common approach to support digital contact tracing in the EU's fight against Corona. Furthermore the Commission also prepared a guidance on data protection[12] related to mobile applications to support contact tracing. The eHealth Network adopted interoperability guidelines and has agreed on common technical specifications for the exchange of data between decentralised national contact tracing apps.[13]

[10] Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data.

[11] eHealth Network Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States, Version 1.0, 15.04.2020.

[12] Commission Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data.

[13] eHealth Network Guidelines to the EU Member States and the European Commission on Interoperability specifications for cross-border transmission chains between approved apps, Detailed interoperability elements between COVID+ Keys driven solutions, V1.0, 2020-06-16.

The EFGS Architecture is based on all these technical specifications.

The architectural descriptions following in this chapter are based on the concept paper[14] the architecture paper[15], as well as the Commission implementing decision[16] and focus on the data protection aspects of the architecture. Additional aspects, e.g., assessments concerning, different technical approaches regarding the EFGS, can be found in the concept paper.[17] The explanations in this section presuppose knowledge about the ENF functionality.[18]

11.4.1.2. Boundary conditions and design goals

The EFGS can only connect national back-ends provided that the mobile device applications are based on the Exposure Notification API from Apple and Google.[19] Furthermore, the infected user must report their positive diagnosis in the national contact tracing and warning system of their home country, if they only have the corresponding contact tracing and warning app of their home country installed; positive diagnoses from countries outside the EU/EEA are out of scope — at least in this version.[20]

The architecture of EFGS should meet the following design goals:

1. to protect national corona warning systems from imperilment by diagnosis keys without adequate testing;[21]
2. to minimize the data traffic between the national back-ends and the national mobile applications;
3. to minimize implementation complexity in the national mobile applications;
4. to minimize implementation complexity in the integration of national back-ends; and
5. to ensure a sufficient data protection level.[22]

11.4.2. Involvement in the overall process

When two users of different ENF-based contact tracing and warning applications meet, both applications can collect the RPIs that the other person's mobile device broadcasts[23]. However, a national contact tracing and warning application will not receive any diagnosis key from other countries' users, if the national corona warning systems do not share diagnosis keys, which their users upload.

Figure 1 depicts how the EFGS can be used to replicate diagnosis keys from one national corona warning system to another national corona warning system in order to provide users who encountered

[14] Citations refer to: T-Systems / SAP: *European Proximity Tracing. Interoperability Conceptual View.* Version 1.2 from June 21, 2020. Hereafter referred to as *Conceptual View*. This paper is not yet published.
[15] T-Systems / SAP: *European Proximity Tracing. An Interoperable Architecture*. Version 1.0 from June 16, 2020. Hereafter referred to as *Architecture*. https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interoperabilitydetailedelements_en.pdf
[16] Implementing Decision (EU) 2020/1023 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic.
[17] cf. *Conceptual View*.
[18] Explanations on the functionality of the Exposure Notification Framework
[19] cp. *Conceptual View*, p. 8. For further explanations cf. ibid., p. 11.
[20] cp. ibid., 8.
[21] See section 11.4.4.5.
[22] cp. *Conceptual View*, p. 12.
[23] cf. Architecture, p.10.

users of other ENF-based contact tracing and warning mobile applications, with more accurate risk information. After the users shared their TEKs with the national Corona app's back end, the TEKs (now called diagnosis keys) will be supplemented with some metadata and uploaded to the EFGS, if the user consents to this sharing. Other national back-ends can download the diagnosis keys and provide these to their respective ENF-based contact tracing and warning mobile application, installed on the user's mobile device. The details on how and when one national corona warning systems shares diagnosis keys with the EFGS and how the diagnosis keys can be interpreted by other corona warning systems will be explained in subsequent sections.

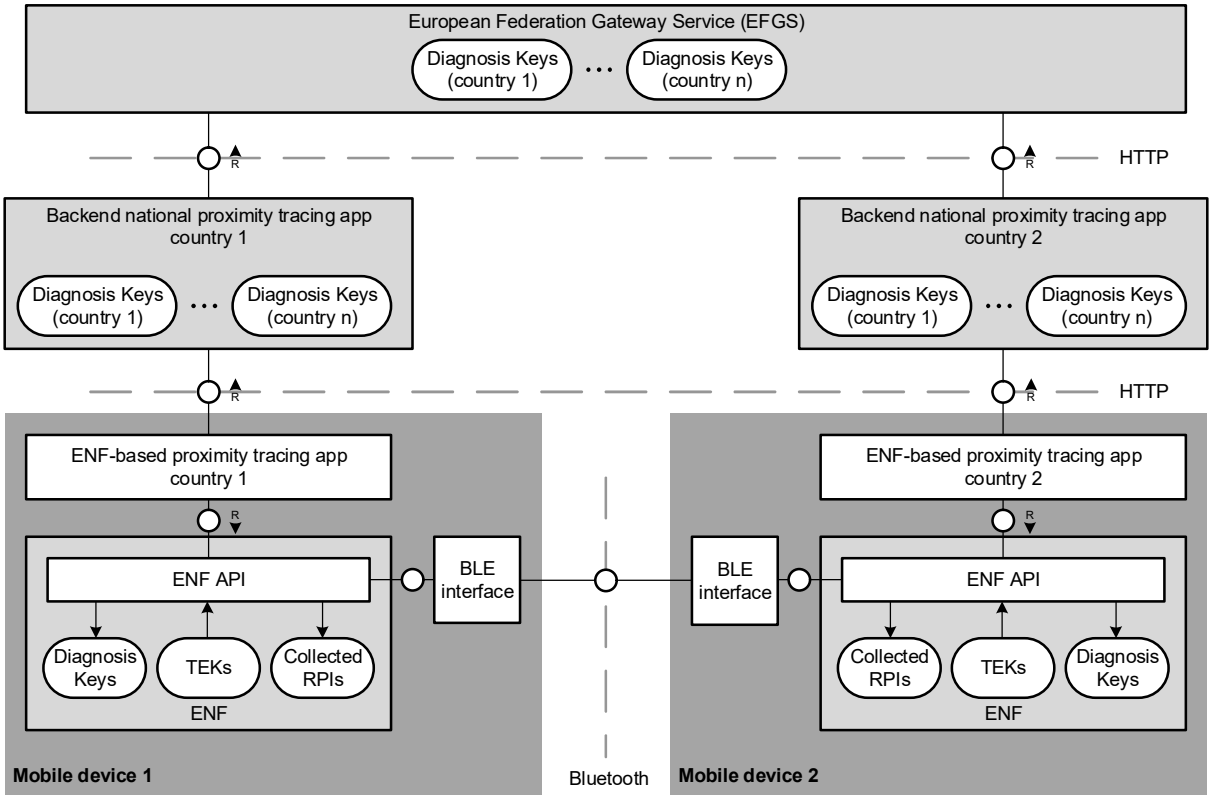


Figure 1: Block diagram showing the involvement of the EFGS in the overall process

11.4.3. Diagnosis key meta data

The pseudonymised personal data exchanged through and processed in the European Federation Gateway Service is regulated by means of a binding decision of the European Commission and will only comprise the following information[24]:

- the keys transmitted by the national contact tracing and warning mobile applications up to 14 days prior to the date of upload of the keys;
- log data associated to the keys in line with the technical specifications protocol used in the country of origin of the keys;
- the verification of an infection;
- the countries of interest and the country of origin of the keys.

This information is transmitted by the national back-ends to the EFGS. Accordingly, diagnosis keys shared by the national corona warning system back-ends with the EFGS must be transmitted to the EFGS in combination with specific metadata per diagnosis key. The semantics of the data is as follows:[25]

1. The diagnosis keys together with the parameters “Transmission risk level” or “Days since onset of symptoms” form a semantic cluster to assess the occurrence of a contact with an infected user and the severity of the risk resulting from that contact. The diagnosis keys and the associated risk parameter express the two dimensions of the exposure, i.e. the existence of the risk of the exposure and an approximated extent of the risk;
2. The “origin” and “report type” parameters enable the national corona warning system back-ends to interpret the data correctly. They allow the national corona warning system back-ends to determine which set of rules govern the semantics of the data fields transmitted and to translate the data into information that the national contact tracing and warning mobile applications are able to parse and interpret. The “origin” parameter may serve as a selector for the national corona warning system back-ends to determine a set of rules to apply to normalize the data received via the EFGS, the “report type” parameter may be used to filter data according to national epidemiological policy; and
3. The “countries of interest” parameter may be used by the national corona warning system back-ends to repackage the data received via the EFGS in order to enable smaller download sizes. If national epidemiological policy permits, a further minimization of data to be downloaded by the national contact tracing and warning mobile application may be achieved by using this parameter as a selector for the download of data.

The metadata types origin, countries of interest and report type are used by the national back-ends of the receiving corona warning system only. A national back-end might use the metadata in decisions regarding how to keep diagnosis keys available for the users of that national contact tracing and warning mobile application for download, but they do not influence the sharing of the diagnosis keys

[24] Implementing Decision (EU) 2020/1023 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic. Article 7a (3).
[25] cf. Architecture, p. 19 s.

by selecting target countries of the sharing operation. The sharing operation keeps the shared data available for all participating member states.

11.4.4. Interfaces for the integration of national corona warning system back-ends

This section describes how a national back-end can share diagnosis keys with the EFGS, how it can fetch diagnosis keys from the EFGS, and how the received diagnosis keys including their metadata are intended to be used by the respective national corona warning system.

Some descriptions and figures include national corona warning systems. However, the implementations within the national corona warning systems might vary from the descriptions and the depicted activity diagrams. The flows describe only one of many possible implementations, and any specific implementation within a national corona warning system is not part of this EFGS architecture. Descriptions are only provided to facilitate the understanding of the EFGS within the overall process.

The EFGS provides four interfaces: An upload interface, a download interface, a callback interface, and an auditing interface.[26]

11.4.4.1. Upload diagnosis keys to the EFGS

The back-end of the national corona warning system receives diagnosis keys from its users. Only diagnosis keys that are allowed to be shared with the EFGS may be used in the following process. The diagnosis keys are supplemented with metadata (see section 11.4.3). The national corona warning system back-end can then combine multiple diagnosis keys into a batch for the upload to the EFGS in order to upload multiple diagnosis keys with one API call.

The metadata supplementation is performed by the national corona warning system. For example, the countries of interest might be reported by the user of the contact tracing and warning mobile application while the report type might be set by the national back-end. Due to the architecture, the EFGS can not influence how the metadata is set within the national corona warning systems on a technical basis.

When the national back-end uploads the batch (possibly after a self-defined delay), the national back-end generates an arbitrary upload batch identifier and calculates a signature of the whole batch. The batch identifier is part of the response of the EFGS to the national back-end to confirm the successful reception and processing of the batch. Several http parameters and response codes are defined, e.g., for error cases.[27] The EFGS validates the uploaded batches, splits the batches into single diagnosis keys with the corresponding metadata, and stores the respective data.[28]

Error! Reference source not found. is an activity diagram and depicts the upload of diagnosis keys from country 1 to the EFGS. The processing activities within the national contact tracing and warning mobile application from country 1 and the national back-end country 1 are only shown schematically because the implementations might vary from country to country.

[26] cf. Architecture., p. 26.
[27] For the http parameters and response codes cf. ibid., p. 32. ss.
[28] For details about the verification and the processing within the EFGS, cf. ibid., p. 34.

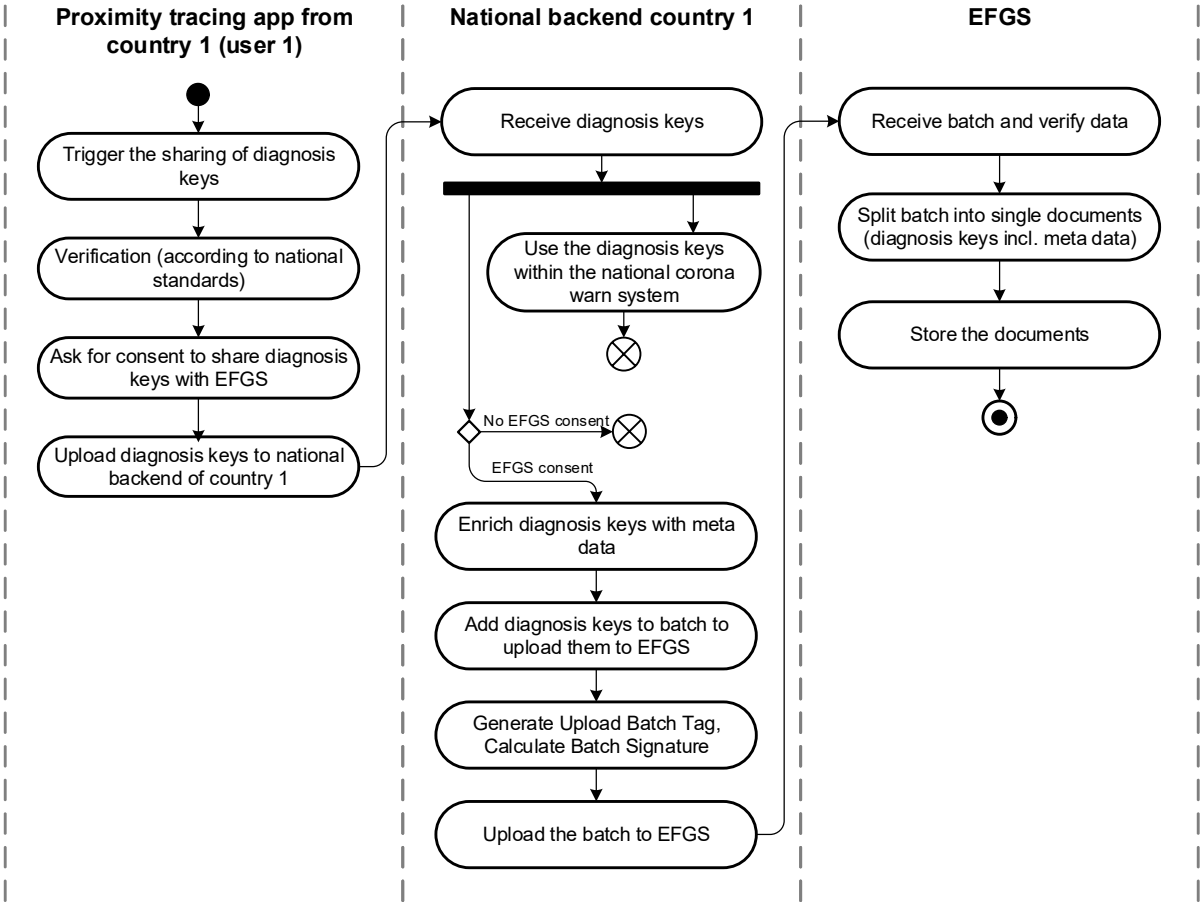


Figure 2: Simplified activity diagram for the upload of diagnosis keys to EFGS[29]

11.4.4.2. Download diagnosis keys from the EFGS

A national back-end can download diagnosis keys that were uploaded by other countries' back-ends to the EFGS.[30]The API call must include the date as a parameter. Furthermore, the API call can include the download batch tag if this value is known (see section 11.4.4.4). The EFGS verifies the request, queries the diagnosis keys to return from its database, transforms the response into the requested content type, adds a download batch tag[31], and provides the result to the national backend, which processes the result. The processing includes (1.) the treatment of the received diagnosis keys (see section 11.4.4.5), and (2.) the processing of the included download batch tag. The national back-end can call the download API again and add the received download batch tag as a parameter to receive the next download batch of diagnosis keys. This might happen several times until no further download batch is available (indicated by an empty response).[32]The data for download is split up into several batches to improve performance and fault tolerance.[33]

Error! Reference source not found. is an activity diagram and depicts the download of diagnosis keys by the national back-end of country 1 from the EFGS. The actions within the national back-end country 1 are only shown schematically, because the implementations might vary from country to country.

[29] cf. Architecture., p. 34 s.
[30] This excludes diagnosis keys uploaded by itself, cf. ibid., p. 28.
[31] The download batch tag is independent from any upload batch tag, cf. ibid., p. 28, p. 32.
[32] cf. Architecture., p. 30.
[33] cf. ibid., p. 28.

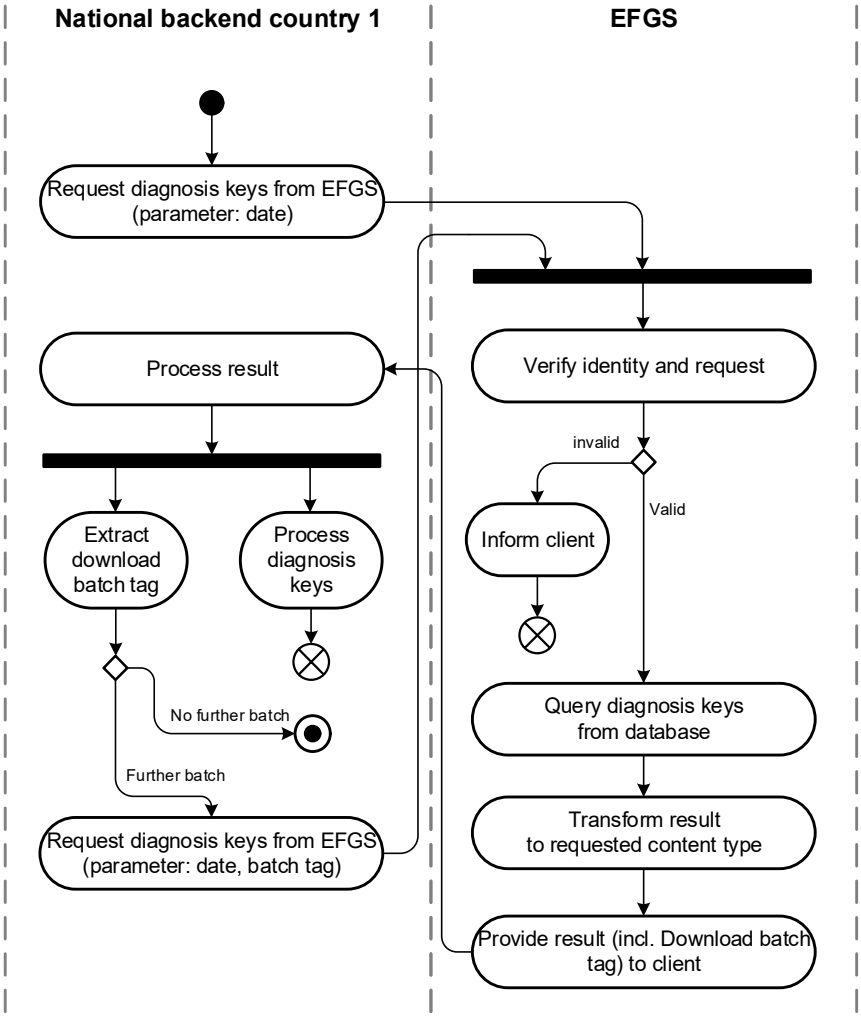


Figure 3: Simplified activity diagram for the download of diagnosis keys from EFGS[34]

11.4.4.3. Callback interface

The EFGS offers the possibility for national corona warning systems to register themselves to receive a callback when a new batch of diagnosis keys can be downloaded. The callback registration interface offers options to add a new callback URL, to list the added URLs, and to remove a URL. The details on how the callback can be registered can be found in the corresponding documents.[35]

Error! Reference source not found. depicts the callback of the EFGS to a national back-end at runtime when a new batch of diagnosis keys can be downloaded. After the national back-end received the call, it can extract the parameters to fetch the new batch. If the call towards the national back-end is not successful (HTTP response code other than 200), the EFGS marks this call for retry. Although a national back-end should receive any callback, it might attempt to fetch new diagnosis keys from the EFGS according to a schedule without having received a callback in order to avoid any technical issues presently preventing a successful callback operation. Although the direct download of a diagnosis key batch might also not be successful due to technical errors, the national back-end is informed about this error when it tries the direct download while it might not realize a failed callback.

[34] cf. Architecture., p. 34 s.
[35] cf. ibid., p. 37 ss.

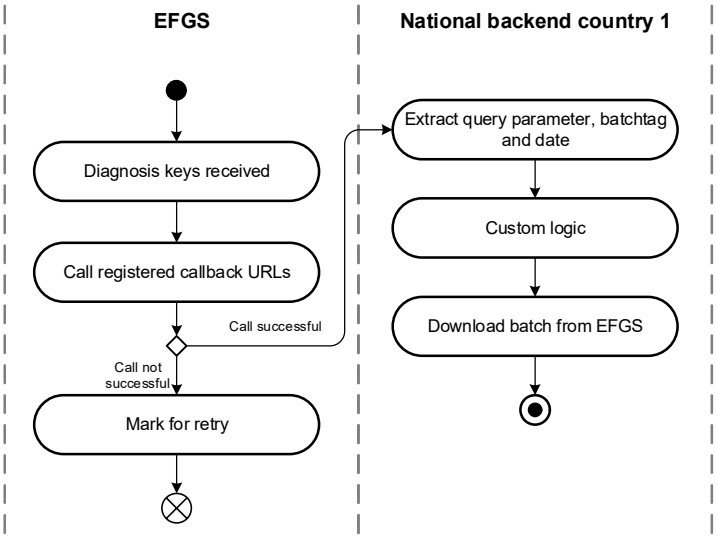


Figure 4: Simplified activity diagram for the callback informing about a new diagnosis key batch[36]

11.4.4.4. Audit interface

The EFGS offers an audit interface that can be used to fetch supplementary information regarding a download batch. The interface requires the provision of the parameters data and batch tag and returns for the countries, that are contained in the batch, the batch signature by country, and further upload information available, for example.[37]

11.4.4.5. Processing of shared diagnosis keys within a national corona warning system

A national back-end may evaluate the received diagnosis keys and decide on which diagnosis keys to make available for the users of the respective national contact tracing and warning mobile application. It is also within the purview of the national back-end to decide how the users can fetch these diagnosis keys. For example, based on the report type, the national back-end can decide to filter the diagnosis keys so that diagnosis keys will not be forwarded to the national contact tracing and warning mobile application that are associated with a verification that is deemed to be too insubstantial. Other metadata such as the countries of interest might be used to group the diagnosis keys and create own subsets of all diagnosis keys, so that within the national contact tracing and warning mobile application, a user can select the subset they are interested in. The EFGS architecture does not enforce any particular treatment of diagnosis keys by the national corona warning systems. Section 11.4.5 describes some of the possible usage scenarios. However, other implementations of the national corona warning system are possible as well.

11.4.4.6. Assumptions regarding the behaviour of national back-ends

The processing of data shared via EFGS in the national corona warning systems occurs outside of the technical sphere of influence for the EFGS. Therefore, the technical operation of the EFGS is based on the general assumption that all connected national corona warning systems are compliant with relevant laws including GDPR by themselves and that the data they share with or receive from EFGS complies with these laws including the GDPR. The EFGS's architecture does not contain any *technical* mechanisms to verify whether the exchanged data is processed in accordance with the applicable legislations.

[36] cf. Architecture., p. 41 ss.
[37] cf. ibid., p. 44 s.

11.4.5. Usage scenarios

This section describes scenarios in which the national corona warning systems use the EFGS for the cross-border exchange of diagnosis keys to warn their users of encounters with other users that were infected and that use another EFGS participants' national corona warning system. These scenarios are supported by the design of the EFGS. However, it also depends on the implementation within the national corona warning systems as to whether these scenarios apply as described.

To simplify the description, these conventions apply:

- User 1: user of country 1's ENF-based contact tracing and warning mobile application.
- User 2: user of country 2's ENF-based contact tracing and warning mobile application.
- Countries of interest: a list of countries that the user marks as relevant for themselves.

11.4.5.1. Warn travellers that visit the home country and get warnings while visiting another country

User 1 travels to country 2. When user 1 encounters user 2 in country 2, user 1's contact tracing and warning mobile application captures user 2's RPIs. Country 1's contact tracing and warning mobile application provides the possibility to select countries of interest, and user 1 marks country 2 as relevant for themselves. Later, user 2 reports themselves as infected in country 2's contact tracing and warning mobile application. User 2 consents to share the diagnosis keys with the EFGS. Country 1's national back-end receives the diagnosis keys, marks these as relevant for country 2 (with information from the metadata, here: origin) and offers those diagnosis keys to country 1's users for download. User 1 fetches the diagnosis keys based on their country of interest selection and the risk for user 1 can be calculated.

11.4.5.2. Corona infection after visiting another country

User 1 travels to country 2. When user 1 encounters user 2, user 2's contact tracing and warning mobile application captures user 1's RPIs. Later, user 1 reports their status as infected in country 1's contact tracing and warning mobile application. User 1 consents to share the diagnosis keys with the EFGS. Additionally, user 1 adds the metadata that they visited country 2 within the last 14 days. Country 2's national back-end receives the diagnosis keys, marks these as relevant for country 1 (with information from the metadata, here: countries of interest), and offers them to country 2's users for download. User 2 fetches the diagnosis keys because the national back-end decided that these diagnosis keys are relevant for all users of country 2's contact tracing and warning mobile application. The risk for user 2 can be calculated.

11.4.5.3. One traveller infects another traveller in another country

User 1 and user 2 travel to country 3. Country 1's contact tracing and warning mobile application provides the possibility to select countries of interest and user 1 marks country 3 as relevant for themselves. When user 1 encounters user 2, user 1's contact tracing and warning mobile application captures user 2's RPIs. Later, user 2 reports themselves as infected in country 2's contact tracing and warning mobile application. User 2 consents to share the diagnosis keys with the EFGS. Additionally, user 2 adds the metadata that they visited country 3 within the last 14 days. Country 1's national back-end receives the diagnosis keys, marks these as relevant for country 3 (with information from the metadata, here: countries of interest) and offers them to country 1's users to download. User 1 fetches the diagnosis key based on their country of interest selection and the risk for user 1 can be calculated.

11.4.5.4. Two users of the same contact tracing and warning mobile application encounter

User 1 and user 2 are users of the contact tracing and warning mobile application of the same country. When they encounter one another (in their home country or at any other place) and one of the users reports themselves as infected, the national corona warning system distributes the diagnosis keys from one user to the other user without EFGS being involved.[38]

11.4.6. Encryption

11.4.6.1. Between national backend and the EFGS

For the communication between the national back-ends and the EFGS, the Transport Layer Security (TLS) is used to encrypt the payload. TLS is a cryptographic protocol designed to provide communication security over a computer network.

11.4.6.2. Between EFGS and the dataset

The connection to the database and the database itself are not encrypted. In order to ensure confidentiality, certain data is secured by application layer encryption. Application layer encryption is a technique that allows applications to encrypt and decrypt data during the processing operations on the application layer, so that applications can store encrypted information in databases that do not provide encryption natively. In the present case, the EFGS receives data that was encrypted in transit using TLS 1.3. This data is then processed in the EFGS's application program and encrypted before it is stored in the database. When the data is required by the application, the data is fetched in encrypted form, decrypted by the application program of the EFGS itself, processed and then sent to the national back-ends via encrypted transports using TLS 1.3. Anyone who may gain access to the database information will only be able to see encrypted contents.

11.5. Data flow

This section describes the data flow for the Federation Gateway Service. The section is split into three major parts (Import Interfaces/Export Interfaces/Data (Field) Catalogue). Each part is split into subsections in order to differentiate between different areas.

Figure 5 illustrates the EFGS dataflow from a high-level perspective. One can see the EFGS database, the National back-end and the National Health Authority. The Figure shows how the different entities can communicate with each other. The EFGS's scope covers three APIs (Upload/Download/Call Back).

[38] EFGS does not forward diagnosis keys from country back to the country itself, cf. *Architecture*, p. 26.

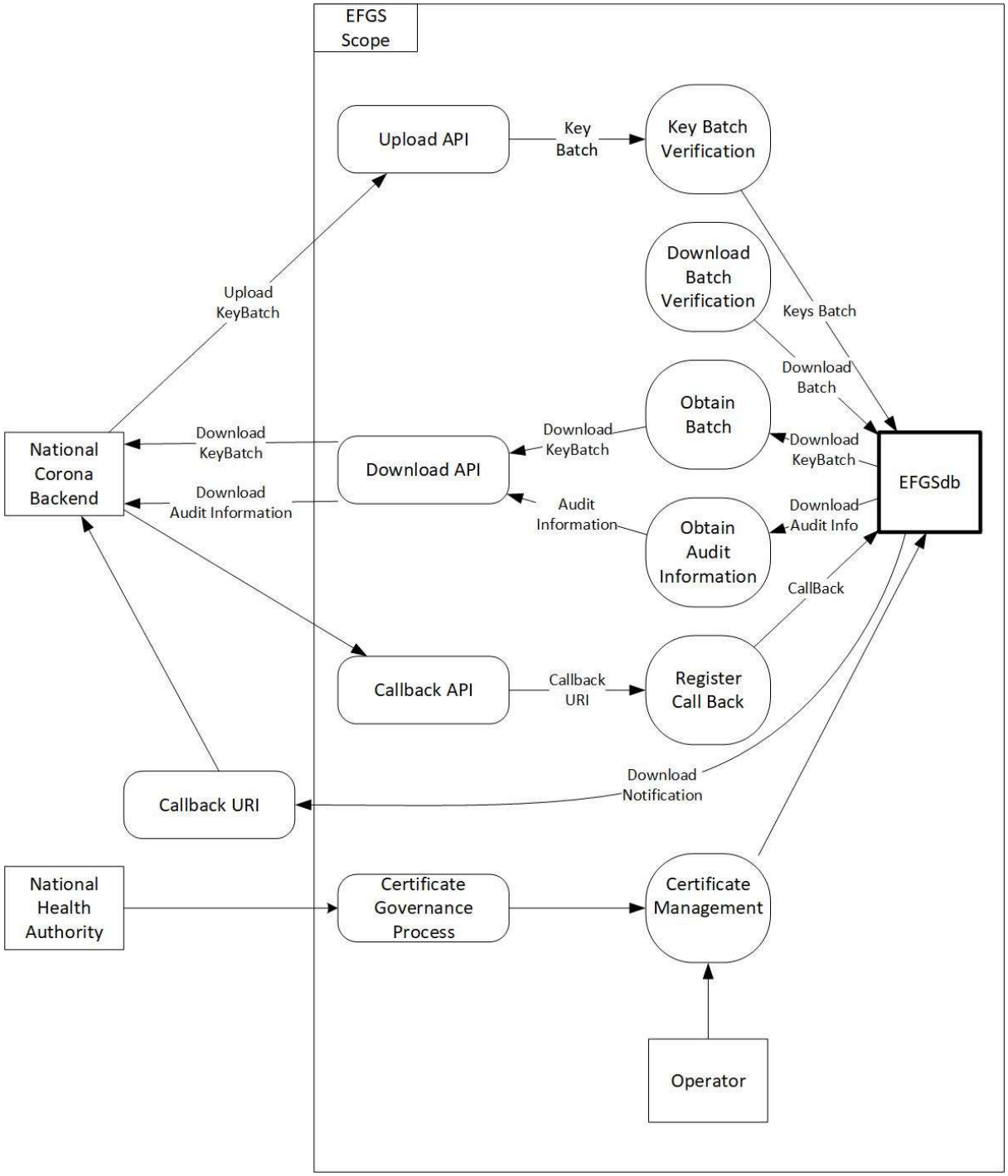


Figure 5: overview Dataflow EFGS

The EFGS is designed with four different interfaces. A list of the different interfaces can be seen in Table 2. It is possible to group the different interface into two major groups. The first group are the import interfaces and the second group are the export interfaces. The import interfaces' objective is the import of new data into the database. The export interfaces focus on the export of data from the EFGS to the national back-ends.

No.	**Interface Name**	**Partner System**
001	Upload Interface	National back-end of the member states
002	Callback Interface	National back-end of the member states

003	Download Interface	National back-end of the member states
004	Auditing Interface	National back-end of the member states

Table 2: Overview of the EFGS interfaces

Section 11.5.1 provides information regarding the import interface and section 11.5.2 focuses on the export interfaces. Each section contains detailed information regarding the corresponding interfaces.

11.5.1. Import interfaces

The Federation Gateway Service provides a simple REST API with a total of four access points. Two of these are designed for importing data. Table 3 provides a basic overview of the importing interfaces. Table 4 and 5 provide a general technical description of the interfaces. They contain information regarding the 'Purpose', 'Encryption', 'Type of Interface', and a list of 'Transferred Data'. The 'Transferred Data' field defines the different data fields transmitted over the interface. An explanation of the different numbers listed in the section "List of transferred data" can be found in subsection **Error! Reference source not found.**.

No.	**Interface Name**	**Partner System**
001	Upload interface	National back-end of the member states
002	Callback interface	National back-end of the member states

Table 3: Overview of the Import Interfaces

11.5.1.1. Upload interface

The upload interface consists of one call to upload a set of diagnosis keys, which might be separated into several batches. If an upload is triggered, the Federation Gateway Service accepts a batch tag as a group identifier for uploaded payloads. This supports possible delete, update, and release actions in the future. The uploader's identity is extracted from the client certificate during the upload. If the client certificate is valid, the submitted content is validated, split, and stored in the database. The size of the payload is also limited to avoid excessively large requests.

Interface name (partner system)	**Upload Interface**
Purpose and description of the transferred Data	Upload of diagnosis keys from the national back-end to the EFGS.
Encryption	TLS 1.3
Interface Type	HTTPS
List of transferred data	5-19

Table 4: General Technical Description of the Upload Interface

So far, the section provided a basic understanding regarding the upload interface. The following will focus on a more detailed description of the data flow.

Figure 6 shows the activity diagram for the upload of diagnosis keys from the national back-end to the EFGS. A national back-end receives diagnosis keys from the proximity tracing app user. After the keys have been received, the national back-end determines if a sufficient legal basis can be established for sharing the keys with the EFGS. If a legal basis to share the keys with the EFGS can not be established, the personal data remains at the national back-end and is only processed in the national corona warning system.

If the legal basis can be established, the keys will be processed further. The data will be supplemented with metadata and added to a batch. This batch of keys will be uploaded later by the national back-

end to the EFGS. The national back-ends can decide when they transfer a batch of diagnosis keys to the EFGS. However, before the national back-end can upload the data, the national back-end generates a batch tag and calculates the batch signature. Once this step is finished, the batch of keys will be uploaded to the EFGS. After successfully receiving the transferred data from the national backend, the EFGS verifies the data. Since a batch can carry more than one key, the keys inside the batch are separated and each key is stored inside a single database document. This document contains the diagnosis keys including the metadata supplemented by the national backend. Furthermore, the document also stores metadata from the EFGS, which is necessary for further processing (see also 11.4.3). Figure 6 might differ from country to country as different countries might implement their back-ends differently, but the basic process should be identical.

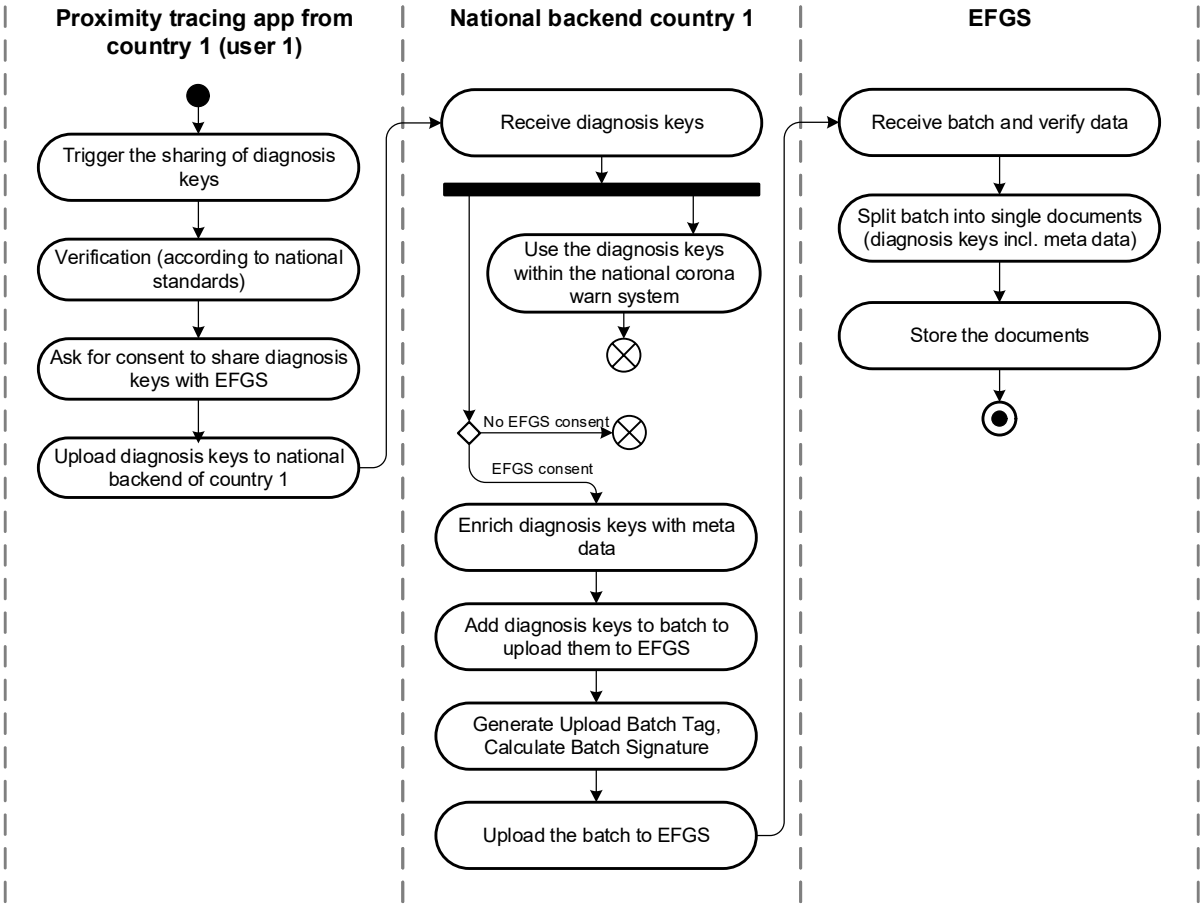


Figure 6: Simplified activity diagram for the upload of diagnosis keys to EFGS[39]

11.5.1.2. Callback interface

The callback interface consists of three operations for managing callback URLs:

- Obtain the current callback URLs
- Put or update new callback URL
- Delete callback URL

With this operation, it is possible for each national back-end to register a callback GET operation, which receives data changes. This way, there is minimal lag between new uploads and downloads. The

[39] cf. *Architecture*, p. 32 s.

Federation Gateway Service acts virtually as a forwarding gateway. A more detailed description of the data flow follows.

Interface name (partner system)	**Callback Interface**
Purpose and description of the transferred Data	Notification of the new data packet through the EGFS.
Encryption	TLS 1.3
Interface Type	HTTPS
List of transferred data	2,3

Table 5: General Technical description of the Callback Interface

Figure 7 shows the activity diagram for the callback notification process regarding new diagnosis keys established between the EFGS and the national back-ends. The EFGS offers the possibility for the national back-ends to register themselves for receiving a callback when a new batch of diagnosis keys can be downloaded. The callback registration interface contains options to add a new callback URL, to list the added URLs, and to remove a URL. The details on how the callback can be registered can be found in the corresponding documents. Figure 7 displays the callback of the EFGS to a national back-end at runtime when a new batch of diagnosis keys can be downloaded. The EFGS received new diagnosis keys which triggered a function to call the registered callback URLs. If the call towards the national back-end was not successful, the EFGS marks this call for retry. If the call was successful, the national back-end extracts the query parameter, batch tag, and date from the callback. The national back-end can now decide how to proceed further. Normally, the custom logic would trigger a download request in order to receive the new diagnosis keys from the EFGS. Figure 7 might differ from country to country as different countries might implement their back-end differently, but the basic process should still be the same.

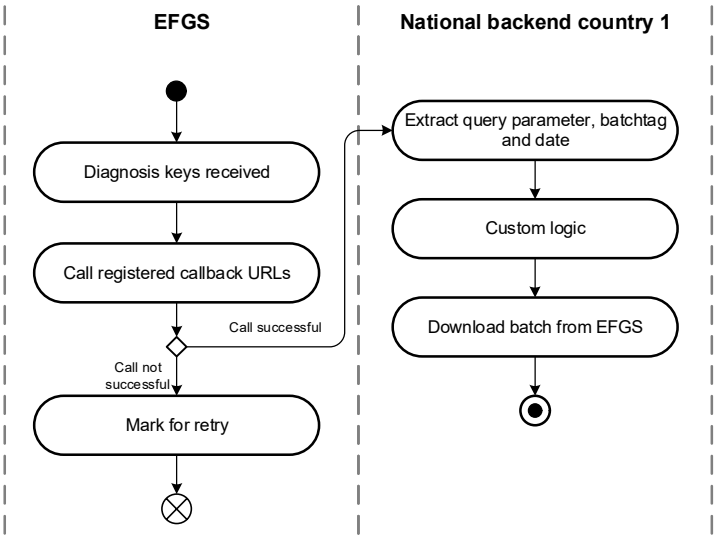


Figure 7: Simplified activity diagram for the callback informing about a new diagnosis key batch[40]

11.5.2. Export interfaces

[40] cf. *Architecture*, p. 40 ss.

In contrast to the import interfaces, the export interfaces are used in order to implement an auditing function as well as a download interface. Table 6 provides a basic overview of the different export interfaces.

Nr.	Interface Name	Partner System
001	Download Interface	National back-end of the member states
002	Auditing Interface	National back-end of the member states

Table 6: Overview of the Export Interfaces

11.5.2.1. Download interface

The download interface consists of one possible request for retrieving a batch of diagnosis keys. The request only accepts a "date" variable. This indicates the maximum age of requested diagnosis keys. This means only diagnosis keys newer than "date" will be downloaded from the Federal Gateways Server. If the client key is valid and the requested content is available, the data will be queried and transformed into the response. If a download is triggered, there may be thousands of diagnosis keys available. The API will return the first batch with a tag. The same download call is then repeated but includes the received tag in order to receive the next batch of keys. This improves the performance and the fault tolerance of the system.

Export Interface 001: Download Interface

Interface name (partner system)	Download
Purpose and description of the transferred data	Data distribution to member states
Encryption	TLS 1.2
Interface type	HTTPS
List of transferred data	3, 5-12

Table 7: General technical description of the Download Interface

So far, the section provided a basic understanding regarding the download interface. The following will focus on a more detailed description of the data flow. Figure 8 shows the activity diagram for the download of diagnosis keys from the EFGS to the national back-ends. A national back-end can download diagnosis keys that were uploaded by other corona warning system back-ends to the EFGS. The national back-end requests diagnosis keys from the EFGS via an API call. The API call must include the data as a parameter. Optionally, the call can also include a batch tag. The EFGS verifies this request, queries the diagnosis keys for return from its database, transforms the response into the requested content type, adds a download batch tag, and provides the results to the national backend, which in return processes the result. The processes include the processing of the included download tag and the processing of the diagnosis keys. The national back-end can call the EFGS again with the batch tag, which was received previously in order to download the next batch of diagnosis keys. This recall can happen multiple times until the EFGS has no further keys. Figure 7 might differ from country to country as different countries might implement their back-end differently but the basic process should still be the same.

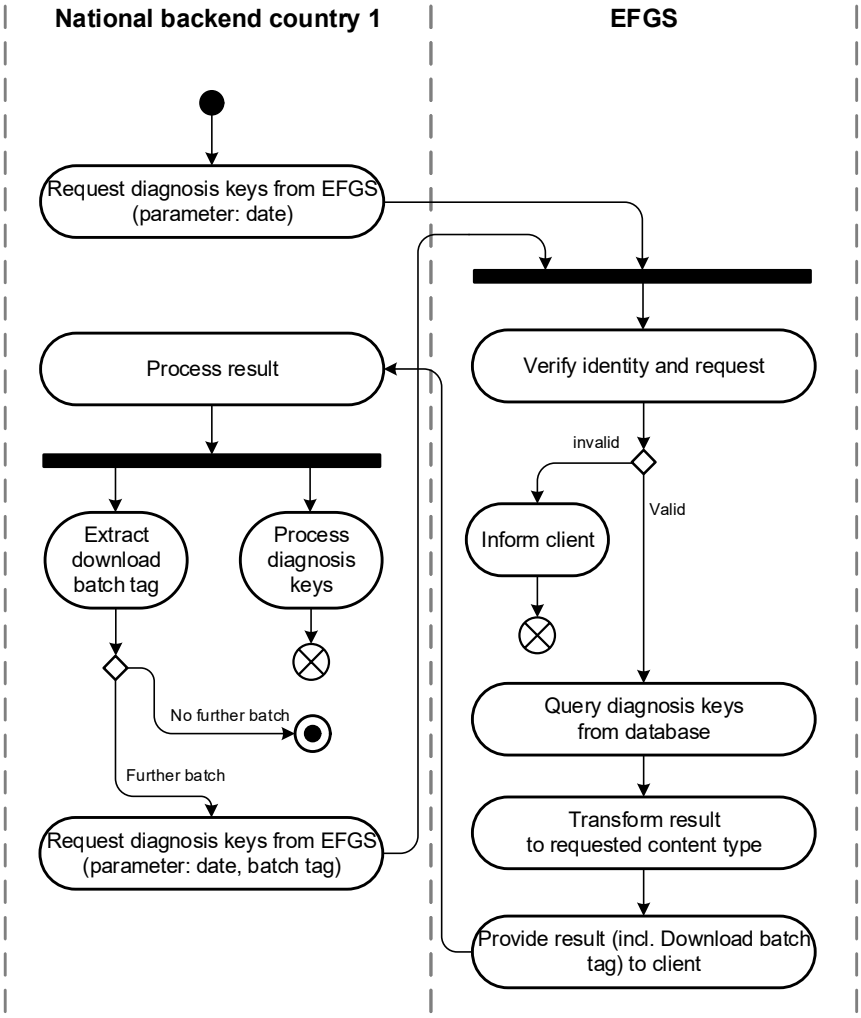


Figure 8: Simplified activity diagram for the download of diagnosis keys from EFGS[41]

11.5.2.2. Auditing interface

The audit interface contains an operation to audit parts of the service by the external clients to validate the integrity of the running system. This audit operation provides the possibility to verify data integrity within a batch. The operation returns information about the batch, for instance:

- Countries contained in the batch
- Batch signatures by country
- Uploading information

Export Interface 002: Auditing Interface

Interface name (partner system)	**Auditing**
Purpose and description of the transferred data	Data distribution to member states
Encryption	TLS 1.2
Interface type	HTTPS

[41] cf. *Architecture*, p. 28 s.

List of transferred data	16-19

Table 8: General technical description of the Auditing Interface

11.5.3. Data (field) catalogue

This section gives an overview of the different data fields inside the database of the EFGS.

11.5.3.1. Data inside the database of the EFGS

Error! Reference source not found. shows an overview of the different data fields inside the database of the EFGS. It presents information regarding the "Format", "Data Field Name", "Group of People", "Usage Alternation", "Processing/Deletion", and the "DPP Quality". "Format" defines the data format in which the data is stored and "Data Field Name" is the name of the variable. The field "Group of People" specifies where the data originates, for example the "national back-end" or "App User". Uploaded diagnosis keys are stored for 14 days. While theoretically unnecessary if direct forwarding is used, practical consideration makes temporary buffering worthwhile:

- Packets get lost and back-ends may be unavailable. With stored data, download retries are possible.
- Timing of download is left to the back-ends instead of forcing a schedule.
- Newly onboarded countries get the data for the past 14 days at once, so they do not miss important data.

Since newly infected citizens initially submit up to 14 daily keys, stored keys can be up to 28 days old.

A document-oriented NoSQL DB or any other database which supports JSON documents can be used to ensure compatibility with current and future formats. A document in the database needs the uploader metadata, a payload, a flag "diagnosis type" in order to differentiate between self-diagnosis and different lab tests, "format information", and a "batch tag" related to the upload. The document itself represents a single diagnosis key together with uploader, format, and batch information. Each diagnosis key is stored in a single document. This means the size of the document is small. If a batch of diagnosis keys is retrieved, the API stores each key set as a single small document. This avoids query performance gaps, ensures flexibility, and makes it easier to query the data. The documents expire automatically after 14 days.

As seen in 11.5.2.2, the data storage documents have two batch tags. The reason why is that the uploader tag is used to identify the documents of the uploader. The other tag is used to identify the documents across all uploaders, which is important during the download. Therefore, both have a different data type. The uploader tag is an arbitrary unique value provided by the uploader. The other tag is an object which needs to be incremental and unique per day as it is used to "navigate" within the day.

- This page was intentionally left blank. -

Nr.	Table	Format	Data Field Name	Data subject	Usage Alternation	Processing/Deletion	**DPP Quality** (Value, Pseudonym, Anonymous)
1	diagnosiskey	BIGINT	(PK) ID	FGS	Unique Identifier of the row	Rest API/14 Days	Value
2	Diagnosiskey	DATETIME(2)	created_at	FGS	Creation Date	Rest API/14 Days	Value
3	Diagnosiskey	VARCHAR(64)	batch_tag	National back-end	Batch Assignment	Rest API/14 Days	Value
4	Diagnosiskey	VARCHAR(64)	payload_hash	FGS	Duplication protection	Rest API/14 Days	Value
5	Diagnosiskey	VARBINARY(100)	payload_key_data	App User	Diagnosis key of the App User	Rest API/14 Days	Pseudonym
6	Diagnosiskey	INT	payload_rolling_start_interval_number	App User	Diagnosis key of the App User	Rest API/14 Days	Subordinate data to a pseudonym (diagnosis key)
7	Diagnosiskey	INT	payload_rolling_period	App User	Diagnosis key of the App User	Rest API/14 Days	Subordinate data to a pseudonym (diagnosis key)
8	Diagnosiskey	INT	payload_transmission_risk_level	App User	Diagnosis key of the App User	Rest API/14 Days	Subordinate data to a pseudonym (diagnosis key)
9	Diagnosiskey	VARCHAR(64)	payload_visited_countries[42]	App User	Diagnosis key of the App User	Rest API/14 Days	Subordinate data to a pseudonym (diagnosis key)
10	Diagnosiskey	VARCHAR(64)	payload_origin	National back-end	Diagnosis key of the App User	Rest API/14 Days	Subordinate data to a pseudonym (diagnosis key)
11	Diagnosiskey	INT	payload_report_type	App User	Diagnosis key of the App User	Rest API/14 Days	Subordinate data to a pseudonym (diagnosis key)

[42]Represents countries of interest, The metadata field visited countries ("countries of interest") is provided from the application user. He marks the countries he visited in the last 14 days. This information is used to determine for which countries the information is relevant. Therefore, it can be used to warn other application user (with the same "countries of interest"), which had contact with the positive tested person.

12	Diagnosis-key	INT	Payload_days_since_onset_of_symptoms	APP User	Diagnosis key of the App User	Rest API/ 14 Days	Subordinate data to a pseudonym (diagnosis key)
13	Diagnosiskey	VARCHAR(64)	format_format	FGS	Internal field	Rest API/14 Days	Value
14	Diagnosiskey	INT UNSIGNED	format_major_version	FGS	Internal field	Rest API/14 Days	Value
15	Diagnosiskey	INT UNSIGNED	format_minor_version	FGS	Internal field	Rest API/14 Days	Value
16	Diagnosiskey	VARCHAR(64)	uploader_information_batch_tag	National back-end	Identification of the national back-ends	Rest API/14 Days	Value
17	Diagnosiskey	VARCHAR(2080)	uploader_information_batch_signature	National back-end	Identification of the national back-ends	Rest API/14 Days	Value
18	Diagnosiskey	VARCHAR(64)	uploader_information_thumbprint	National back-end	Identification of the national back-ends	Rest API/14 Days	Value
19	Diagnosiskey	VARCHAR(2)	uploader_information_country	National back-end	Identification of the national back-ends	Rest API/14 Days	Value
20	Certificate	BIGINT	(PK) ID	FGS	Unique Identifier of the row	Database	Value
21	Certificate	DATETIME(2)	created_at	FGS	Creation Date	Database	Value
22	Certificate	VARCHAR(64)	Thumbprint	FGS	Thumbprint of the certificate	Database	Value
23	Certificate	VARCHAR(2)	Country	FGS	Country Certificate	Database	Value
24	Certificate	VARCHAR(14)	Type	FGS	Type of the Certificate	Database	Value
25	Certificate	BOOLEAN	Revoked	FGS	Status of the Certificate	Database	Value

Table 9: Overview of the data fields inside the database of the FGS

- This page was intentionally left blank. -

11.5.3.2. Data inside logfile “webserver”

To meet auditing requirements, all requests to the Federation Gateways Service pass an audit module creating an audit log, which produces log files, event streams, or tables within the database. This data can be displayed on a dashboard via standard visualization tools like Tableau, Kibana, Splunk, Grafana, etc.

An overview of the different data stored inside the webserver log file can be found in Table 10.

Nr.	Format	Data Field Name	Group of People	Usage Alternation	Processing and Deletion	**DPP Quality** (Value, Pseudonym, Anonymous)
1	String	Uploader batch tag	FGS	Logging of the Uploads	webserver, Rolling Log	Value
2	String	Batch tag	FGS	Logging of the batchings	webserver, Rolling Log	Value

Table 10: Overview of the data inside the log file of the "Webserver"

11.6. Data erasure and deletion periods

Hereafter, the deletion process of the EFGS is described. The data that is stored in the EFGS server is considered. Only the necessary data for the respective process steps are kept in the databases in accordance with the purpose limitation principle Article 5 (1)(b) GDPR, Article 7a (1) and Annex III (3)(e) and (f) of the Implementing Decision (EU) 2020/1023.[43]

11.6.1. Data erasure requirements

The disposal of redundant personal data has to be ascertained in accordance with the requirements for the deletion of personal data (disposal after achievement or futility of purpose or expiry of the deletion period).

The data must be rendered unrecognizable or destroyed in such a way that its recovery is not possible or not possible with proportionate means.

11.6.2. Implementation of the data deletion function

The EFGS stores diagnosis keys, log files, metadata and configuration data.

According to Annex III of the Implementing Decision (EU) 2020/1023[44], 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 EFGS stores the personal data that was uploaded for 14 days. After this period of time, the data is deleted with the help of a scheduling system that executes a job to delete data whose retention period has expired. The scheduling system used is a part of the provided runtime environment, a regular cron job is being used.

[43] Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic.

[44] Commission Implementing Decision (EU) 2020/ 1023, Article 1 (5)

The data is erased by a run scheduled every 6th hour which deletes all data records intended for erasure.

Automated data deletion is realized by implementing the deletion routines by a cron job. During the daily EFGS process, these routines receive all the information necessary for the deletion. This is all data which is flagged for deletion. The data field “Created_at” (Source: DFC) is decisive here. Every data record is linked to this attribute. If this data contains a date that is older than the set time limit of 14 days, then all associated data records in the system are completely deleted. Every 6th hour, this deletion routine runs through the system and deletes all flagged data.

Log files do not store personal data. The EFGS application records two types of logs:

- Tomcat log via console
- EFGS log via file

The log files are kept for 90 days. The application deletes the log files automatically.

After the end of the provision of service, any remaining data will be deleted, unless Union or Member State law requires storage of the personal data[45].

11.7. Processing of data

11.7.1. Overview recipients and processing operations

Origin of the recipients of the data	
1. ☒Within the EU organization	Recipients
2. ☐ Outside the EU organization	Recipients

Categories of the data recipients
1. ☒A natural or legal person
2. ☐ Public authority

[45]Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic. Annex III (3)

3. ☐ Agency

4. ☐ Any other third party, specify:

Specify who has access to which parts of the data:

see section 11.7.2 to 11.7.7

Table 11: Data recipient

The following processing operations take place within the framework of the EFGS process:

No.	Description of the processing	Purpose
001	Upload of diagnosis keys	Contributing the diagnosis keys of this country to the EFGS
002	Split of received diagnosis keys into single documents	Technical purpose, avoids query performance gaps, ensures flexibility, data query is easier
003	Storing of the documents	Forwarding the documents until national back-ends call to receive them
004	Certificate whitelisting	Whitelisting of member state certificates in the system
005	Querying and transformation to requested content type	Preparation for download to national back-end
006	Download diagnosis keys	Download to national back-end for providing diagnosis keys to user of national corona app

Table 12: Overview of processing of data

11.7.2. Detailed description of processing 001 upload of diagnosis keys

Used data fields referring to DFC	01-14
Authorized role(s)	Administrator
Purpose	Sharing the diagnosis keys of this country with the EFGS
Download required for further processing?	No

Table 13: Processing 001 Upload of diagnosis keys

11.7.3. Detailed description of processing 002 split of received diagnosis keys into single documents

Used data fields referring to DFC	01-20
Authorized role(s)	Administrator

Purpose	Technical purpose, avoids query performance gaps, ensures flexibility, data query is easier
Download required for further processing?	No

Table 14: processing 002 split of diagnosis keys

11.7.4. Detailed description of processing 003 storing the documents

Used fata fields referring to DFC	01-20
Authorized role(s)	Administrator
Purpose	Persisting the documents until national back-ends call to receive them
Download required for further processing?	No

Table 15: processing 003 storing the documents

11.7.5. Detailed description of processing 004 certificate whitelisting

Used data fields referring to DFC	19-24
Authorized role(s)	Administrator
Purpose	Whitelisting of member state certificates in the system
Download required for further processing?	No

Table 16: processing 004 certificate whitelisting

11.7.6. Detailed description of processing 005 Querying and transform to requested content type

Used data fields referring to DFC	01-20
Authorized role(s)	Administrator
Purpose	Persisting the documents until national back-ends call to receive them
Download required for further processing?	No

Table 17: processing 005 querying and transformation

11.7.7. Detailed description of processing 006 download diagnosis keys

Used data fields referring to DFC	19-24
Authorized role(s)	Administrator

Purpose	Download to national back-end for providing diagnosis keys to users of national contact tracing and warning mobile application
Download required for further processing?	Yes

Table 18: processing 006 download diagnosis keys

11.8. Authorization

11.8.1. General consideration

All components of the EFGS are designed in such a way that there is no direct user interface. On the one hand, this has security advantages and on the other hand it reduces the effort for the corresponding user administration. Additionally, there is no explicit user authorization process which is used. Therefore, there are only two types of roles/users:

- Administrator roles,

responsible for technical configuration of the components;

- Technical users,

necessary for the interaction between the EFGS and the corresponding national back-end components.

From a data privacy view, it is important to monitor and log all access to personal data and only authorized persons can access such data.

Since the application does not provide direct user access to the system, the only way to access the data is as a database administrator. To prevent this possibility of direct access to plain text data, it is encrypted by the application before it is saved in the database. Therefore, there is no way to directly access the personal data in the database. In addition to this technical mechanism to enforce data privacy, every administrator in the system is committed to confidentiality.

11.8.2. Roles for operators of the application

Technical Name	Role (name within the system)	User of this role	Description	Data	Permissions	
					Read	Write[46]
	Loadbalancer Administrator	Administrator	Manages access to the internal network of the Directorate-General for Informatics	Client certificate information for access to the system	X	X
	Database administrated	Administrator	Backup/schema changes and user assignment	User, passwords, all data in the DB	X	X
	Web server administrated	Administrator	Manages the web server setup.	Access to the software		

Table 19: roles for operator

[46] The group "write" includes all changes such as create/create, change/modify, delete/delete.

11.8.3. Technical user

Technical name	Name of technical user	Conversion in the system	Description of the technical user	Data	Permissions	
					Read	Write[47]
FTP-Sys_1	FTP system delivery	Unix USER / GROUP: if_app1_app2/ USERS	Local user account for data delivery via FTP protocol (FTPoverSSH). Supplier is Application_1.	File with personnel master data	X	X

Table 20: roles for technical users

11.9. Operation and monitoring

All personal data in electronic format (emails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the European Commission. The processing of personal data by the Commission must be carried out in accordance with Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data. All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of January 10, 2017 on the security of communication and information systems in the European Commission.

The Commission's contractors are bound by a specific contractual clause for any processing operations of the personal data on behalf of the Commission and by the confidentiality obligations deriving from the transposition of the General Data Protection Regulation in the EU member states ('GDPR' Regulation (EU) 2016/679).

In order to protect personal data, the Commission has put in place a number of technical and organizational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data, or unauthorized access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organizational measures include restricting access to the personal data solely to authorized persons with a legitimate need to know for the purposes of this processing operation.

For the EFGS in particular, the Implementing Decision (EU) 2020/1023 applies. Concrete security measures as well as operational instructions according to a safe and lawful processing of data is set out in Annex III of the Implementing Decision (EU) 2020/1023. The following specific arrangements for the operation of the EFGS are in line with these requirements.

[47] The group "write" includes all changes such as create/create, change/modify, delete/delete.

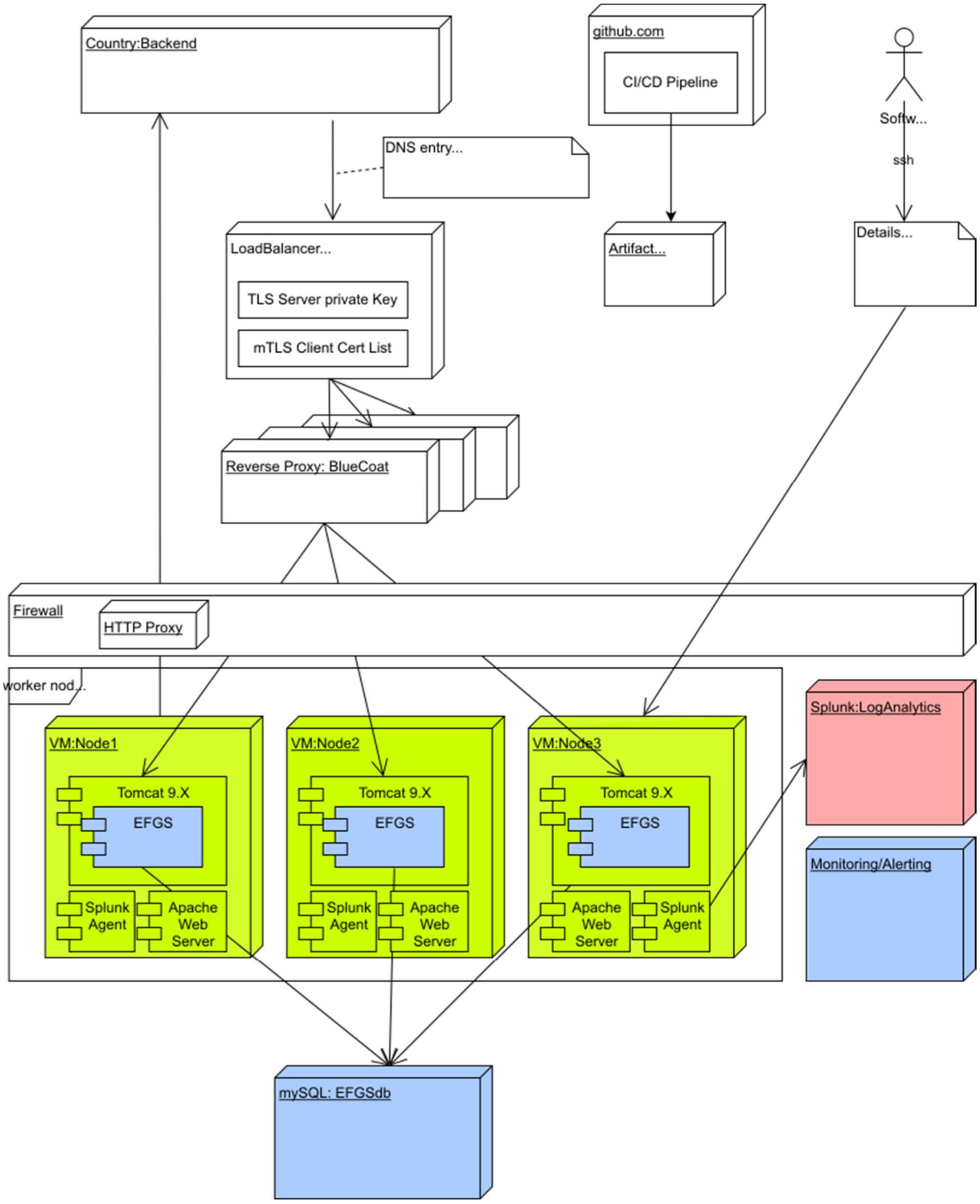


Figure 9: Operating Architecture Overview

11.9.1. General operational architecture

The EFGS operational architecture is mainly divided into 3 parts:

- Basic operation and monitoring (VM Hosting, OS Operation, Webserver Operation)
- Application operation
- Application monitoring

The operational responsibility for the different parts is distributed and shown in the following table and colored according to the architectural overview.

Operational item	List of components	Company, country, place of service provision
Basic operation and monitoring	VM Hosting	Directorate-General for Informatics, European Commission, Brussels (DIGIT)
	Operating System	
	Apache Tomcat	
Application operation	Custom Java Application	T-Systems International GmbH, Germany, Munich
Application monitoring	Custom Java Application	Deutsche Telekom Security GmbH, Germany, Bonn

Table 21: Overview of operational responsibilities

The basic infrastructure is operated by DIGIT in an EU data center. Operational upper edge is the Apache Tomcat Webserver infrastructure. Application operation and monitoring is carried out by T-Systems International GmbH, Security Monitoring by Deutsche Telekom Security GmbH.

Basic infrastructure components used are:

- Virtual Machine Layer
  - VM Worker nodes
  - Apache Tomcat 9.X
  - Apache Web Server
  - Splunk Agent
- Application Layer
  - Custom EFGS Application
- Monitoring Layer
  - Splunk

11.9.2. Monitoring and audit logging

Overall there are two monitoring layers:

- Layer 1: Basic Operation Monitoring including VM, OS and Webserver

and

- Layer 2: Application Monitoring

Data transferred according to the monitoring concept is defined as follows:

Monitoring Layer	List of components	Log data

Layer 1	VM Hosting	No personal data logged [48]
	Operating System	No personal data logged [30]
	Apache Tomcat Webserver	No personal data logged [30]
Layer 2	Custom Java Application	No personal data logged [49]

Table 22: application monitoring

All log messages use one format. Each log message contains key value pairs which will represent the required data. All of these log messages consist of mandatory and additional fields. The following mandatory fields will be sent with each log message:

Field	Content	Example Value
Timestamp	ISO-8601 formatted timestamp (always UTC)	2020-08-04T16:44:45.999Z
Level	Log level	INFO
Hostname	The hostname of the current node	srv01
Pid	Process ID	44929
Trace	Correlation ID for tracing	d058309145b9f7a3
Span	Span ID for tracing	d058309145b9f7a3
Thread	ID of the thread	Main
Class	The class from which the message is coming from	e.i.f.service.DiagnosisKeyBatchService
Message	Information about what has happened	started document batching process

Table 23: Log message overview

The security monitoring of the application is performed in order to detect potential attacks e.g.,

- High peak of malicious key injections
- Exceeding of alarm thresholds
- High peak of unsuccessful country registrations

No personal data is typically required for these use cases.

11.9.3. Backup

Backups of the database are performed by dumping the database once weekly. After the initial dump, for every day, an incremental backup is made based on the initial backup. Since the personal data in the database at rest is encrypted, the backups only contain encrypted data.

A backup chain consisting of an initial dump for a week and the subsequent incremental backups for the following days of the week is kept for 7 days beginning with the day of the last full backup and the

[48] We assume that there is no personal data at machine level, OS level, or Tomcat as it is not logged in the custom Java application. This must be verified again at the end of the application development if it corresponds to reality.

[49] The custom Java application operated within the infrastructure handles no personal data from smartphones or users. The target environment for the service is an Apache Tomcat Server. Therefore, all log output will be written to stdout which is redirected to the catalina.out log file. The content of this file needs to be shared between the operational units.

backup chain is then disposed of. The maximum retention of the encrypted data in the backup data storage is 14 days.

11.10. Rights of data subjects

Data subject rights are precluded according to Article 11 (2) GDPR, Article 12 (2) EU-DPR respectively. They are also subject to a right of refusal by the controllers according to Article 12 (2) GDPR, 14 (2) EU-DPR.

The processing in the EFGS and the subsequent processing concern pseudonyms that are no longer correlated to identities. The processing in the national warning systems, the processing in the EFGS and the subsequent processing after the sharing of the pseudonyms is designed in a way to avoid linking the pseudonyms as well as avoiding the re-identification of the natural persons behind the pseudonyms. The design of the processing emphasises the data minimisation in terms of minimising the correlation between the data collected and processed and the identities behind that data.

Demonstrably, this results in the controllers' inability to discharge any obligations regarding data subjects' rights or the withdrawal of consent due to a design in compliance with the principles relating to processing of personal data according to Art. 5 (1) GDPR, Art. 4 (1) EU-DPR. Since the controllers can not establish a relationship between the specific data points that they process and the identity of the natural person behind these data points, they are unable to ascertain that an individual who claims to be the bearer of the data subject rights and the right to withdraw the relevant consent is in fact entitled to these rights and the right to withdraw consent. Even when the claimant discloses the claimant's identity, the legitimacy of any claims or any withdrawal of consent can not be established by the controllers.

In consequence, according to Article 11 (2), 12 (2) GDPR and Article 12 (2), 14 (2) EU-DPR, the provisions regarding the data subjects' rights are not applicable and the controllers are entitled to refuse claims based on these rights.

☐Guidance for Data subjects on how/where to consult the privacy statement is available.

12. View of data subjects and their representatives

According to Article 35 (9) GDPR the controller shall seek the views of data subjects or their representatives on the intended processing, where appropriate.

The WP29 considers that[50]:

- those views could be sought through a variety of means, depending on the context (e.g. an internal or external study related to the purpose and means of the processing operation, a formal question to the staff representatives or trade/labour unions or a survey sent to the data controller's future customers);
- if the data controller's final decision differs from the views of the data subjects, its reasons for going ahead or not should be documented;
- the controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate.

12.1. Identify data subjects or their representatives

[50]WP 248, p. 13

The range and number of data subjects or their representatives to be consulted should be a function of the privacy risks and the numbers of citizens who could be impacted[51]. If the risks are expected to impact everyone in the participating member states, then the organisation should consult widely with external stakeholders.

In order to identify all the stakeholders who might have an interest or might be impacted by the processing, examples are listed below. Representatives of data subjects to be consulted on the member states' level of processing could be:

Data subject/ representative	Specification / Conduct (member state level)
☐ worker / temporary worker representatives	
☐ consumer representatives	
☐ patient representatives	
☐ refugee representatives	
☐ representatives of privacy/ data protection community or organisations, privacy stakeholders	
☐ people from other organisations who have appropriate concerns relevant to DPIA, e.g. children, students, elderly people:	

Table 24: List of data subjects' representatives (suggestion)

12.2. Establish consultation plan

In order to develop a plan to communicate and consult with the data subjects/representatives a schedule for consultation and further communications should be considered, e.g.:

☐ seek for a generic study related to the purpose and means of the processing operations,

☐ send a questionnaire to representatives with deadline for feedback

☐ survey sent to the data controllers' future customers

☐ public hearings/ workshops

☐ interviews

☐ E-Mail setup.

[51] ISO / IEC 29134 2020-1, S. 13

13. Lawfulness and fairness

13.1. Legal basis

13.1.1. Checklist

Possible legal basis for the processing of personal data under Articles 6, 9 GDPR	
☒6(1)(a), 9(2)(a)	The data subject was given clear and comprehensive notice regarding the controllers and the processing and has given consent concerning the processing of their personal data for one or more specific purposes.
☐6(1)(b)	Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
☐6(1)(c)	Processing is necessary for compliance with a legal obligation to which the controller is subject.
☐6(1)(d)	Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
☒6(1)(e),9(2)(g)	The processing is necessary for reasons of substantial public interest on the basis of the relevant Member State's law that is proportionate to the aim pursued, respects the essence of the fundamental right to the protection of personal data and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
☒6(1)(e), 9(2)(i)	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 or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
☐6 (1) (f)	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Table 25: possible legal basis for the processing of personal data under Article 6 GDPR

13.1.2. Description

The legal basis of the processing of personal data in the EFGS may consist of a qualified consent or a statutory law. In both cases, the legal basis is subject to qualified requirements resulting from the fundamental right of the citizens of the European Union regarding the protection of their personal data according to Article 16 (1) TFEU and Article 8 (1) Charter. The qualified requirements for the legal basis of processing data according to Article 16 (1) TFEU are only detailed in Article 8 (2) Charter. These latter requirements are to be applied in order to determine the parameters, the legal basis of the processing has to observe.

13.1.2.1. Triple elements of protection

Article 8 (1) Charter combines three elements of protection in one fundamental right. It serves as a protective right against processing of personal data by the state, as an entitlement vis-à-vis the state regarding protection of personal data against processing by third parties and as a guarantee regarding certain rights of the data subject concerning its' personal data such as a right to accuracy of the processed personal data, disclosure requirements regarding the processing and relief regarding the cessation of the processing of personal data.

The protective right is qualified further by the qualifications of permitted processing in Article 8 (2) sent. 1 Charter. Legitimate processing of personal data requires the pursuit of a legitimate and specific purpose while processing, the justification of the processing in terms of either a voluntary and informed consent or a legitimate statutory basis and the inherent fairness of the processing.

The entitlement requires the relevant authority not only to abstain from illegitimate processing itself but to prevent illegitimate processing by others. The relevant authority is thus obligated to design its processing in a way that ensures that any further processing is legitimate in the same way as the relevant authority's processing itself.

The guarantee of the data subject rights finally requires the relevant authority to design its processing in a manner as friendly to the exercise of the data subjects' rights as possible.

13.1.2.2. Application of Article 8 Charter

The EFGS processes personal data according to Article 8 (1) Charter. It processes the temporary exposure keys of a user, the time when the respective temporary exposure key was generated (as "rollingStartIntervalNumber"), the time of validity of the respective temporary exposure key (as "rollingPeriod") and the level of infection risk associated with the time of validity of the respective temporary exposure key (as "transmissionRiskLevel") or the number of days associated to the temporary exposure key since symptoms of an infection began to be noticed by the user (as "daysSinceOnsetOfSymptoms").

The temporary exposure keys are pseudonyms of the user. A temporary exposure key is a random number generated by the mobile handset of the user and stored in a trusted execution environment that limits access to the temporary exposure keys. If the member states' mobile applications respect the EU Commission's guidelines regarding the design of the applications, the temporary exposure keys are not linked to further data identifying the user. However, due to the nature of the temporary exposure keys as being random numbers taken from a large pool of possible numbers so that a collision – the generation of the same random number by two different handsets – is highly unlikely, they exist in a 1:1 relationship with the identity of the user. Consequently, they act as pseudonyms for the respective user. The fact that the temporary exposure keys may not be resolved to the identities of the natural persons behind the pseudonyms does not contradict their classification as pseudonyms: Articles 11 (2), 12 (2) GDPR refer to cases, in which the controller is unable to establish the identity of the data subjects behind the processed personal data as cases involving the processing of personal data. An inability of the controller to resolve pseudonyms therefore does not affect the nature of a pseudonym as personal data.

Since the temporary exposure keys are constrained to be shared only – according to the relevant Member State's established processes –in case of a test resulting in the indication of an infection with the COVID-19 virus or in case of a self-assessment of an infection with the COVID-19 virus, they are data concerning a person's health and thus sensitive information according to Article 9(1) GDPR. Additionally, the processing of the temporary exposure keys is combined with the processing of the level of infection risk associated with the time of validity of the respective temporary exposure key so that the processed data points state an information regarding the respective user's health and therefore are sensitive information.

In consequence, the requirement that a pseudonym only loses its character as personal data and becomes anonymous data if it is impossible to resolve the identity of a person by reasonable means,

is fortified. Due to the sensitive nature of the temporary exposure key, it is reasonable to require proof that the processing of the temporary exposure keys may never result in the re-identification of the natural person behind the temporary exposure keys. This proof would need to take into consideration any mistake, software bug and security issue since concerning sensitive data, an attacker may consider using means that in the ordinary course of behaviour would be considered extreme, unreasonable and impossible.

Such a proof of the temporary exposure keys withstanding unreasonable attempts of re-identification is currently unavailable. The temporary exposure keys can thus be determined to be pseudonyms for the purpose of determining the legal basis of their processing in the EFGS.

In consequence, Article 8 (1) Charter is applicable since the EFGS processes pseudonyms of users of the member states' mobile applications.

13.1.2.3. Interference of the EFGS with the fundamental right to protection of personal data

The EFGS interferes with the fundamental right to the protection of personal data in all three stages of the processing as well as in the stage of the subsequent processing by the member states in the national back-ends and in the member states' mobile applications.

13.1.2.3.1. The stages of processing in the EGFS

The processing in the EFGS is performed in three stages.

In the first stage, the temporary exposure keys of a user, the time when the respective temporary exposure key was generated, the time of validity of the respective temporary exposure key and the level of infection risk associated with the time of validity of the respective temporary exposure key are uploaded to the EFGS by the national back-ends. In the second stage – that follows the first stage immediately –, the EFGS processes these data points into batches suitable for processing by the national back-ends. In the third stage, the batches containing these data points are made available to national back-ends for retrieval purposes. The national back-ends can retrieve the batches containing the data points for up to 14 days from the day of the processing in the second stage.

The processing in all three stages is an interference with the fundamental right to the protection of personal data: The personal data is stored, subjected to operations and reordered into batches that are then made available for retrieval.

13.1.2.3.2. Subsequent processing by the member states

The subsequent processing in the national back-ends of the member states as well as the subsequent processing in the member states' mobile applications may also interfere with the fundamental right to the protection of personal data. This subsequent processing, however, is distinct from the processing in the EFGS. The controllers may need to take the subsequent processing into account in their DPIAs.

13.1.2.4. Justification of the interference and requirements for the legal basis

The justification of the interference has to observe the requirements of Article 8 (2) Charter as well as to ensure the proportionality of the achievement of the objective of public interest vis-à-vis the interference with the fundamental right to protection of personal data.

13.1.2.4.1. Requirements of Article 8 (2) Charter

The legal basis of the processing can consist of either a consent - see below in section 13.1.2.4.3 - or a statutory law - see below in section13.1.2.4.4.

Both types of bases have to meet the requirements of Art. 8 (2) Charter, i.e. both types of bases have to pursue a legitimate specific purpose while ensuring the fairness of the processing by defining the constraints and guarantees of the processing.

13.1.2.4.2. Legitimate purpose of the processing in the EFGS

The processing in the EFGS pursues a specific and legitimate purpose, see section 11.2 of this document.

13.1.2.4.3. Requirements for a consent

If the legitimate basis for the processing in the EFGS is a consent, this consent has to observe the requirements of a voluntary, informed decision of the data subject to consent as well as to define the constraints and guarantees of the processing in order to meet the fairness requirement according to Article 8 (2) Charter and Article 6(1)(a), 7 and 9(1)(a) of the GDPR.

13.1.2.4.3.1. Informed decision: Transparency

If the legal basis of the processing is a consent, the processing in the EFGS is subject to heightened transparency requirements according to Article 13 (2) GDPR, Article 15 (2) EU-DPR that have to be observed at the time of the consent. The consent concerns the processing of data subject to Article 9 (1) GDPR, Article 10 (1) EU-DPR since the temporary exposure keys relate to the physical health of the user.

In order to observe the fairness requirements in Article 13 (2) GDPR, Article 15 (2) EU-DPR as well as in Article 8 (2) Charter, at the time of consent, the user needs to be informed regarding:

(1) the identity and the relevant contact details of the controllers of the processing;

(2) the contact details of the controller's relevant data protection officers;

(3) the legitimate purpose of the processing in the EFGS;

(4) the legal basis of the processing of the user's personal data, namely the user's consent according to Articles 6 (1) lit. (a), 9 (2) lit. (a) GDPR;

(5) the categories of recipients of the user's personal data, namely the controllers in their capacity as operators of the national back-ends and the national contact tracing and warning mobile applications;

(6) the period of storage and processing of the user's personal data in the EFGS;

(7) the information, that the data subject's rights regarding access, rectification, erasure, restriction of processing, objection to processing and data portability do not apply due to the impossibility of the fulfilment of these rights;

(8) the information, that the data subject's right to withdraw the consent at any time is limited to require the cessation of further provisions of personal data by the national contact tracing and warning mobile application, while due to the impossibility to establish the user's relationship with such personal data, already provided personal data is still going to be processed;

(9) the right to lodge complaints with the relevant data protection authorities and the contact details of these authorities.

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant information as referred to in Article 13(2) GDPR.

The user may be notified of parts of this information by means of a data privacy notice that links to a website containing more detailed information. This website in turn may link to the data privacy notices of the controllers in order to describe the details of the subsequent processing. The use of a website is not unduly onerous for the user: In order to collect the consent and to share the temporary exposure keys with the national back-ends that then share the personal data with the EFGS, an internet connection is required from the outset. Consequently, the provision of more detailed information via the internet is adequate to satisfy the user's requirements for detailed information since the means to obtain this information is at the user's immediate disposal and the information provided can be more detailed and more clearly organized.

Regarding the specific requirements for information:

Concerning issue (1): The identities of the controllers of the processing need to be disclosed explicitly and comprehensively in order to allow the user to form a well informed opinion of whether to grant the consent.

This requirement may be observed by disclosing all controllers: Those who actually participate in the EFGS at the time of the consent and those who are potentially going to participate in future. Since the consent does not constitute an obligation to process personal data, it can be granted in reserve for controllers, who may join the EFGS at a later state. The fact that not all of the controllers may actually process the shared temporary exposure keys has to be disclosed to the user at the time of consent, while notifying the user also of the fact that the controllers who do not process the user's personal data may begin processing at a later stage.

The information concerning issues (2) and (9) regarding the contact details of the Data Protection Officer, where relevant, and of the competent Data Protection Authority should be provided by in the national contact tracing and warning mobile application.

The information concerning issues (3), (4), (5), (6), and (7) should be provided in the national contact tracing and warning mobile application without recourse to a website on the internet.

The information regarding the processing in the EFGS needs to be available in the data privacy notice of the national contact tracing and warning mobile application of the participating Member States. To increase transparency, the privacy notice of the controllers should be made publicly available for example by means of a link from the EFGS website. .

The information regarding the subsequent processing may be disclosed in the data privacy notices of the respective controllers of the subsequent processing. The uploading national contact tracing and warning mobile application may link to the information website of the EFGS which in turn would link to the respective notices of the controllers. . In order to allow the user to form a well informed opinion on the subsequent processing, the publicly available information from the individual controllers regarding their own subsequent processing should highlight any particular deviation from the eHealth Network's guidelines "Mobile applications to support contact tracing in the EU's fight against COVID-19, Common EU Toolbox for Member States Version 1.0" and "Interoperability guidelines for approved contact tracing mobile applications in the EU", and the European Data Protection Board's guidelines "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak".

13.1.2.4.3.2. Informed decision: specificity and explicitness

Any of the foregoing transparency requirements need to be discharged explicitly by using a language that is specific enough to determine the exact nature and extent of the processing of the user's personal data in the EFGS and to inform about the subsequent processing.

This requires the disclosure of the specific purpose being pursued by the processing. Since a consent may cover different operations, as long as these operations serve the same purpose, it is permissible for the controllers to pursue one explicitly named and described purpose by means of the processing in the EFGS and the further subsequent processing. However, due to the purpose limitation according to Article 5 (1) lit. (b) GDPR and recital 32 GDPR as well as Article 4 (1) lit. (b) EU-DPR and recital 19 EU-DPR, any additional processing not in pursuit of the express purpose requires a separate express consent in order to ensure that the user remains in control of the processing of their personal data. In consequence, the processing of the user's shared temporary exposure keys is limited with regard to the specific purpose stated in that user's consent. In order to be able to rely on the consents declared by the users, the controllers have to ascertain that each consent enquired by means of the national mobile apps is sufficient for their subsequent processing and the processing in the EFGS.

Furthermore, in order to confirm the users' understanding that while granting consent, they exercise control over their personal data, the information of the users needs to contain a comprehensive description of the processing activities in the EFGS as well as information on the subsequent processing by the controllers.

13.1.2.4.3.3. Informed decision: age of consent

Neither in Articles 6 (1) lit. (a), 8 GDPR nor in Article 5 (1) lit. (d), 8 EU-DPR, the age of consent regarding a consent for privacy purposes was harmonized outside the scope of application of offers of information society services. The EFGS and the subsequent processing do not concern themselves with offers according to Article 1 (1) lit. (b) directive (EU) 2015/1535.

The determination of the age of consent for privacy purposes was therefore left to the jurisdiction of the member states. This may result in a situation, where a member state collects a valid consent according to its national law, while that consent collected in another member state would be contrary to the laws and regulations of that member state.

With regard to the processing in the EFGS and the subsequent processing in the controllers' national warning systems, the compliance of the consent with the national law of the member state that collects the consent is adequate to form a legal basis also for the processing in the EFGS and the subsequent processing. Privacy law is harmonized law. Its application is required to be uniform throughout the EU in order to exercise the fundamental freedoms guaranteed by the European treaties. In consequence, a member state is only entitled to refuse legal positions that - while they were created in pursuit of the rights created by the European treaties - were only created under the cover of these rights in order to circumvent the member states' national legislation improperly while taking advantage of provisions of community law.

The member states collect the consents of the relevant user according to their national law in order to operate their national warning systems as well in order to participate in the EFGS. The collection is not intended at all to circumvent the applicable national law at the time of collection, this being the law of the collecting member state. In consequence, any consent collected in compliance with the laws of the member state that collected the consent, forms a valid basis regarding the subsequent processing by the other member states participating in the EFGS, provided that the requirements of the European laws applicable were met.

13.1.2.4.3.4. Fairness: granularity

If a consent forms the legal basis of the processing, that consent is required to be sufficiently granular. The consent may not confound purposes that are – by their nature – separate and independent of one another.

The EFGS provides a mechanism to share personal data of users with all participating member states. A consent thus has to allow for sharing the data with all member states, even though they may not yet participate in the EFGS since they may take up participation at a later date when the user's personal data is still available in the EFGS. In order to avoid processing of the user's personal data under a consent that does not cover all controllers, the consent applies to all member states.

This consent is sufficiently granular, as it does not confound several separate and distinct purposes. The legitimate purpose of the EFGS is indivisible concerning the member states it is being pursued in. It is aligned with the basic freedoms of mobility according to Articles 20 (2) lit. (a), 21 (1) TFEU and pursues a high level of human health protection according to Article 168 (1) TFEU. Neither the right to mobility nor to human health is specific to certain parts of the European Union. Due to its contagious nature, the COVID-19 virus can result in cross-border infection chains without reservations as to specific member states. A pursuit of the EFGS's purpose only for a select number of member states would therefore be antithetic and the pursuit needs – by nature – to comprise all of the member states.

13.1.2.4.3.5. Fairness: data subject rights and withdrawal in case of consent as legal basis

In order to observe the fairness requirement according to Article 8 (2) Charter, the data processing based on a consent has to preserve the sovereignty of the user as the data subject by providing means to withdraw the consent as easily as to grant it and to provide for effective means to exercise the data subject's rights.

However, Articles 11 (2), 12 (2) GDPR and Articles 12 (2), 14 (2) EU-DPR permit the controller to design the processing in a way that the natural persons behind the personal data being processed are no longer identifiable. In this case of a pseudonym that can not be reasonably resolved any longer, the user has to accept the limitation of the data subject's rights. These rights do not apply any longer once the controller can demonstrate that the controller is not in a position to discharge these obligations due to a lack of correlation between the processing data and the identity behind the pseudonyms. This approach is reinforced by recitals 57 GDPR and 32 EU-DPR: In principle, the controller is not required to comply with a construction of the GDPR or the EU-DPR that would require him to identify a data subject solely for the purposes to meet certain requirements under the GDPR and the EU-DPR.

In the present case, the processing in the EFGS concerns pseudonyms that are no longer correlated to identities. This processing in the EFGS is designed in a way to avoid linking the pseudonyms as well as avoiding the re-identification of the natural persons behind the pseudonyms. The design of the processing emphasises the data minimization in terms of minimizing the correlation between the data collected and processed and the identities behind that data.

This results in the inability of the controllers to ascertain the legitimacy of any claim regarding data subject's rights. Since the controllers can not establish a relationship between the specific data points that they process and the identity of the natural person behind these data points, they also are unable to ascertain that an individual that claims to be the bearer of the data subject rights and the right to withdraw the relevant consent is in fact entitled to these rights and the withdrawal.

Even in the case that the claimant discloses the claimant's identity, the legitimacy of the claims or the withdrawal of consent can not be established by the controllers. The EFGS processes the temporary exposure keys of a user and their associated metadata, i.e. the time when the respective temporary exposure key was generated (as "rollingStartIntervalNumber"), the time of validity of the respective temporary exposure key (as "rollingPeriod") and the level of infection risk associated with the time of validity of the respective temporary exposure key (as "transmissionRiskLevel") or the number of days since symptoms of an infection began to be noticed by the user (as "daysSinceOnsetOfSymptoms").

Since the temporary exposure key is a random number, generated from a very large pool of random numbers, it is not linked to the identity of the natural person whose mobile phone chose the random number at the moment of its generation. Once the temporary exposure key is shared, it becomes publicly known and available. However, since the process of sharing does not reveal the identity behind the shared temporary exposure key – the member states national mobile applications do not record or share further identifying information stored on the mobile phone –, it is impossible to establish a reliable link between the respective temporary exposure keys and any information later supplied because of a complete lack of evidence for this link.

Demonstrably, the controllers are unable to discharge any obligations regarding data subjects' rights as they are unable establish the legitimacy of any claims due to lack of identifying information.

Regarding withdrawal of consent, the data subject's right is limited to the cessation of further provisions of personal data by the national contact tracing and warning mobile application, while due to the impossibility to establish the user's relationship with such personal data, already provided personal data is still going to be processed. Since a relationship between the data subject and personal data already provided to the EFGS can not be established, the data subject is incapable of designating the processed personal data as its own and is unable to prove such an ownership. This design of the EFGS is legitimate as it results from the pursuit of the data minimisation principle by ensuring that a correlation between the data subject and the personal data being processed is concealed to the utmost extent. The resulting inability to claim and prove the relationship that was concealed due to the pursuit of a privacy principle complies with the GDPR and the EU-DPR as established by recitals 57 GDPR and 32 EU-DPR.

In consequence, according to Articles 11 (2), 12 (2) GDPR and Articles 12 (2), 14 (2) EU-DPR, the provisions regarding the data subjects' rights are not applicable. Because of the principles established in recitals 57 GDPR and 32 EU-DPR, a withdrawal of a consent regarding the processing of the personal data processed in the EFGS can not result in the cessation of the processing of personal data already provided as the data subject can not designate or prove specific personal data as the data subject's one. It should be noted that such data already provided by the data subject will only be retained in the EFGS for a maximum period of 14 days, after which they are disposed of.

13.1.2.4.3.6. Fairness: purpose limitation

Article 8 (2) Charter limits the processing to the specified purposes. Further processing for other incompatible purposes requires compliance with the conditions of Article 6 (4) GDPR. The purpose limitation on the EFGS is imposed by Article 7a (1) of the Implementing Decision (EU) 2019/1765.

13.1.2.4.3.7. Fairness: guarantees

The fairness requirement according to Article 8 (2) Charter requires the processing of the personal data to be sufficiently secure, restrained and accurate.

The data subject is unable to influence the security of the processing. This results in a responsibility for the controllers to design the processing in a secure manner providing adequate safeguards. These safeguards convert to damage claims if the controllers fail to provide adequate security and the data subjects incur damages.

In the present case, the users may not easily enforce claims against the controllers due to the nature of the processed personal data. As the users may not prove a relationship between them and specific data points, the controllers may not rely on the stabilizing effect of such claims. Furthermore, the data subjects may not enforce their data subjects' rights due to the lack of a provable ownership of specific data points.

Regarding the processing in the EFGS, Article 7a (5) of the Implementing Decision (EU) 2020/1023 mandates that the European Commission ensures the security of processing, including the

transmission and hosting, of personal data within the federation gateway. The European Commission furthermore discharges specific obligations imposed on it as the processor for the controllers according to Annex III of the Implementing Decision (EU) 2020/1023. The processing in the EFGS is thus subject to binding provisions under public law that are enforceable by the data protection authorities. In consequence, the controllers can rely on the effective supervision according to Article 8 (3) Charter in order to compensate the absence of damage claims and ensure the fairness of the processing.

13.1.2.4.3.8. Fairness: voluntary consent

If consent is to be the legal basis of the processing, in order for the consent to be an adequate basis for the processing, it needs to be given voluntarily. This precludes the member states from attaching any detrimental effects to the refusal of the consent or any rewards to the grant of the consent. Specifically, the available features and the service quality of the member states' national mobile application need to be identical regardless of whether consent was granted or not.

13.1.2.4.3.9. Proof of consent

In order to be able to prove the grant of the consent while retaining as little data as possible, the member states relying on a consent need to establish an upload process that only executes if the consent was granted. The member states may rely on an indicator within the uploaded data structure containing the temporary exposure keys, provided that this indicator is secured against accidental or malicious alteration by means of a hash value or similar data structure. Furthermore, the upload process needs to filter reliably and demonstrably any data structure that does not contain the respective indicator with the required semantics. In order to be able to demonstrate this process including its effectiveness, the respective source code is going to have to be publicly available.

13.1.2.4.4. Requirements for a statutory basis

The legal basis of the processing may also consist of a statutory law, most likely a law pursuant to Article 6 (1) lit. (e), (2), (3) GDPR. In order to constitute a justification for the interference with the fundamental right to the protection of personal data, this statutory law needs to observe the requirements in Article 8 (2) Charter as well as those in Article 6 (3) GDPR.

13.1.2.4.4.1. Subsequent processing

As much as the consent, the statutory law needs to comprise provisions concerning the processing of the personal data shared via the EFGS and processed subsequently by the participating member states. This subsequent processing – being distinct from the processing in the EFGS - requires a legal basis permitting the interference with the fundamental right to the protection of personal data.

A member state collecting the user's personal data should provide the legal basis for the subsequent processing in its statutory law if it chooses to base the sharing of users' personal data with the EFGS by means of its national mobile warning application on statutory law.

The user using this national mobile warning application is subject to the collecting member state's jurisdiction according to the use of this application, while such jurisdiction may not be established for the member states receiving the user's personal data by means of the EFGS. Furthermore, the user relies on the collecting member states legal framework as evidenced by the user's use of this application.

13.1.2.4.4.2. Legitimate objective of the law

In order to serve as a justification of the interference, the statutory law has to pursue a legitimate objective according to Article 8 (2) Charter. The processing of personal data in the EFGS pursues the

legitimate interest detailed in section 11.2.1 of this document, namely the improvement of public health and the safeguarding of the mobility rights of the European citizens.

Furthermore the subsequent processing by the receiving member states needs to pursue a legitimate object as well. The statutory law may rely on the general principle of the member states' compliance with European law.

13.1.2.4.4.3. Specific and transparent law

The justification provided by a statutory law requires that the law justifying the interference must define the scope of any limitation of the exercise of the fundamental right itself. The justifying law needs to be specific regarding clear and precise rules governing the scope and application of the measures interfering with the fundamental rights. This requirement serves to establish a transparent framework that enables the data subject to assess to which extent the data subject's personal data is going to be processed and thereby the statutory law in question exacts and imposes the interference with the fundamental right.

13.1.2.4.4.4. Safeguarding of transparency requirements by the law

Furthermore, in this context, a statutory law that is intended to form the basis for the processing in the EFGS and the subsequent processing also has to provide the foundations – be it by means of a legal requirement or by the establishment of relevant infrastructure such as competences and budgets or by reliance on other statutory laws - to safeguard the requirements of Article 13 (2) GDPR, Article 15 (2) EU-DPR. At the time of the execution of the function to share the personal data with the EFGS, the user needs to be informed regarding:

(1) the identity and the relevant contact details of the controllers of the processing;

(2) the contact details of the controller's relevant data protection officers;

(3) the legitimate purpose of the processing in the EFGS

(4) the legal basis of the processing of the user's personal data, namely the statutory law according to Article 6 (1) lit. (e) and 9 (2) lit. (g) or (i) GDPR;

(5) the categories of recipients of the user's personal data, namely the controllers in their capacity as operators of the national back-ends and the national contact tracing and warning mobile applications;

(6) the period of storage and processing of the user's personal data in the EFGS;

(7) the information, that the data subject's rights regarding access, rectification, erasure, restriction of processing, objection to processing and data portability do not apply due to the impossibility of the fulfillment of these rights;

(8) the right to lodge complaints with the relevant data protection authorities and the contact details of these authorities.

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant information as referred to in Article 13(2) GDPR.

The user may be notified of parts of this information by means of a data privacy notice that links to a website containing more detailed information. This website in turn may link to the data privacy notices of the controllers in order to describe the details of the subsequent processing. The use of a website is not unduly onerous for the user: In order to use the app and to share the temporary exposure keys with the national back-ends that then share the personal data with the EFGS, an internet connection is required from the outset. Consequently, the provision of more detailed information via the internet

is adequate to satisfy the user's requirements for detailed information since the means to obtain this information is at the user's immediate disposal and the information provided can be more detailed and more clearly organized.

Regarding the specific requirements for information:

Concerning issue (1): The identities of the controllers of the processing need to be disclosed explicitly and comprehensively in order to allow the user to form a well informed opinion on the processing.

This requirement may be observed by disclosing all controllers: Those who actually participate in the EFGS at the time of information and those who are potentially going to participate in future. The fact that not all of the controllers may actually process the shared temporary exposure keys has to be disclosed to the user at the time of information, while notifying the user also of the fact that the controllers who do not process the user's personal data may begin processing at a later stage.

The information concerning issues (2) and (9) regarding the contact details of the Data Protection Officer, where relevant, and of the competent Data Protection Authority should be provided by in the national contact tracing and warning mobile application.

The information concerning issues (3), (4), (5), (6), and (7) should be provided in the national contact tracing and warning mobile application without recourse to a website on the internet.

The information regarding the processing in the EFGS needs to be available in the data privacy notice of the national contact tracing and warning mobile application of the participating Member States. To increase transparency, the privacy notice of the controllers should be made publicly available for example by means of a link from the EFGS website. .

The information regarding the subsequent processing may be disclosed in the data privacy notices of the respective controllers of the subsequent processing. The uploading national contact tracing and warning mobile application may link to the information website of the EFGS which in turn would link to the respective notices of the controllers. . In order to allow the user to form a well informed opinion on the subsequent processing, the publicly available information from the individual controllers regarding their own subsequent processing should highlight any particular deviation from the eHealth Network's guidelines "Mobile applications to support contact tracing in the EU's fight against COVID-19, Common EU Toolbox for Member States Version 1.0" and "Interoperability guidelines for approved contact tracing mobile applications in the EU", and the European Data Protection Board's guidelines "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak".

13.1.2.4.4.5. Fairness: Data subject rights

In order to observe the fairness requirement according to Article 8 (2) Charter regarding the data processing, the data subject's rights have to be considered.

However, Articles 11 (2), 12 (2) GDPR and Articles 12 (2), 14 (2) EU-DPR permit the controller to design the processing in a way that the natural persons behind the personal data being processed are no longer identifiable. In this case of a pseudonym that can not be reasonably resolved any longer, the user has to accept the limitation of the data subject's rights. These rights do not apply any longer once the controller can demonstrate that the controller is not in a position to discharge these obligations due to a lack of correlation between the processing data and the identity behind the pseudonyms. This approach is reinforced by recitals 57 GDPR and 32 EU-DPR: In principle, the controller is not required to comply with a construction of the GDPR or the EU-DPR that would require him to identify a data subject solely for the purposes to meet certain requirements under the GDPR and the EU-DPR.

In the present case, the processing in the EFGS concerns pseudonyms that are no longer correlated to identities. This processing in the EFGS is designed in a way to avoid linking the pseudonyms as well as

avoiding the re-identification of the natural persons behind the pseudonyms. The design of the processing emphasises the data minimization in terms of minimizing the correlation between the data collected and processed and the identities behind that data.

This results in the inability of the controllers to ascertain the legitimacy of any claim regarding data subject's rights. Since the controllers can not establish a relationship between the specific data points that they process and the identity of the natural person behind these data points, they also are unable to ascertain that an individual that claims to be the bearer of the data subject rights.

Even in the case that the claimant discloses the claimant's identity, the legitimacy of the claims can not be established by the controllers. The EFGS processes the temporary exposure keys of a user and their associated metadate, i.e. the time when the respective temporary exposure key was generated (as “rollingStartIntervalNumber”), the time of validity of the respective temporary exposure key (as “rollingPeriod”) and the level of infection risk associated with the time of validity of the respective temporary exposure key (as “transmissionRiskLevel”) or the number of days since symptoms of an infection began to be noticed by the user (as “daysSinceOnsetOfSymptoms”).

Since the temporary exposure key is a random number, generated from a very large pool of random numbers, it is not linked to the identity of the natural person whose mobile phone chose the random number at the moment of its generation. Once the temporary exposure key is shared, it becomes publicly known and available. However, since the process of sharing does not reveal the identity behind the shared temporary exposure key – the member states national mobile applications do not record or share further identifying information stored on the mobile phone –, it is impossible to establish a reliable link between the respective temporary exposure keys and any information later supplied because of a complete lack of evidence for this link.

Demonstrably, the controllers are unable to discharge any obligations regarding data subjects’ rights as they are unable establish the legitimacy of any claims due to lack of identifying information.

In consequence, according to Articles 11 (2), 12 (2) GDPR and Articles 12 (2), 14 (2) EU-DPR, the provisions regarding the data subjects’ rights are not applicable.

13.1.2.4.4.6. Fairness: Guarantees

The fairness requirement according to Article 8 (2) Charter requires the processing of the personal data to be sufficiently secure, restrained and accurate. This results in a responsibility of the controllers to design the processing in a secure manner providing adequate safeguards. These safeguards convert to damage claims if the controllers fail to provide adequate security and the data subjects incur damages.

In the present case, the users may not easily enforce claims against the controllers due to the nature of the processed personal data. As the users may not prove a relationship between them and specific data points, the controllers may not rely on the stabilizing effect of such claims. Furthermore, the data subjects may not enforce their data subjects’ rights due to the lack of a provable ownership of specific data points.

Regarding the processing in the EFGS, Article 7a (5) of the Implementing Decision (EU) 2019/1765 mandates that the European Commission ensures the security of processing, including the transmission and hosting, of personal data within the federation gateway. The European Commission furthermore discharges specific obligations imposed on it as the processor for the controllers according to Annex III of the Implementing Decision (EU) 2019/1765. The processing in the EFGS is thus subject to binding provisions under public law that are enforceable by the data protection authorities. In consequence, the controllers can rely on the effective supervision according to Article 8 (3) Charter in order to compensate the absence of damage claims and ensure the fairness of the processing

13.1.2.4.4.7. Fairness: Voluntary use of the function to share personal data

In order to observe the fairness requirement according to Article 8 (2) Charter, the member states may not attach any detrimental effects to the non-use of the function to share personal data with the EFGS or make this function perform automatically in their national mobile warning application according to the statutory law forming the basis of the processing. While the statutory law pursues a legitimate objective, the user's sovereignty regarding the user's personal data as the data subject has to be preserved in essence. Removing the user's agency completely would result in the negation of the user's right to the protection of personal data according to Article 8 (1) Charter in order to complete the pursuit of the otherwise legitimate objective. This would constitute a complete disregard for the fundamental right to the protection of personal data, resulting in a disregard of the fairness requirement according to Article 8 (2) Charter.

In the present case, this fairness requirement is fulfilled, if the national mobile contact tracing and warning application's use altogether is not made mandatory by the law providing the legal basis of the processing.

The fairness requirement according to Art. 8 (2) Charter does not require the sharing of personal data with the EFGS to be an optional feature of the national contact tracing and warning application. According to Articles 6(1)(c) or (e), 9 (2) lit. (g) or (i), 6 (3) sent. 3 GDPR, the member state enacting the law may regulate the types of data which are subject to the processing. This legislative power includes the power to define the granularity of the processing of the personal data within the constraints of the essence of the fundamental right to the protection of personal data. It is within the purview of the legislative body to combine strands of data processing according to its own discretion provided that the combination is neither arbitrary nor effectively mandatory for the data subject.

If the choice to use the national mobile contact tracing and warning application altogether is left to the user as an option without detrimental effect, the combination of strands of data processing that are related to one another in the application does not affect the voluntary use of the application as a whole. A member state may thus choose to pursue the legitimate purpose by combining the use of the application for the domestic purposes and the use in combination with the EFGS without making the sharing of personal data with the EFGS an option for the user.

13.1.2.5. Proportionality

For both eventual legal bases – consent or statutory law –, the proportionality of the processing vis-à-vis the legitimate purpose is required under Art. 8 (2) Charter.

13.1.2.5.1. Objective of general interest

The processing in the EFGS is in the general interest in order to establish a high level of human health protection according to Article 168 (1) TFEU and to ensure an expedited return to full mobility for the citizens of the European Union according to Articles 20 (2), lit. (a), 21 (1) TFEU. Any subsequent processing has to pursue identical legitimate interests concerning the establishment of a high level of human health protection.

In order to attain these goals, contact tracing is used as a means to facilitate the breaking of infection chains for the COVID-19 virus. The EFGS and compliant subsequent processing activities serve these means by establishing an interoperability of the national mobile applications for contact tracing and warming. However, the processing in the EFGS and the subsequent processing interfere with the fundamental right according to Article 8 (2) Charter as detailed above. For this interference to be proportional to the objective in the general interest pursued, it needs to be appropriate, necessary and respect the essence of the fundamental right to the protection of personal data.

13.1.2.5.2. Appropriateness

The processing in the EFGS and the intended subsequent processing are appropriate to attain the objective in the general interest. By facilitating the breaking of infection chains of the COVID-19 virus, the processing improves the general health of the population of the EU/EEA. The enabling of the data exchange between in the national back–ends of the national mobile applications permits to return earlier to a state, during which travel within the territory of the EU/EEA can be accomplished without encumbrance such as self-isolation or social distancing detrimental to the utilization of public transport.

13.1.2.5.3. Necessity

The processing in the EFGS and the compliant subsequent processing activities are necessary since means, that would achieve the same level of effectiveness while interfering with the fundamental right to the protection of personal data in a less severe manner, are not available.

The processing in the EFGS and the subsequent processing concern health data. The processing of this sensitive data is necessary because only by processing the pseudonyms of infected data subject, the early warning of other data subjects - that may have been in contact with an infected data subject in a way contributing to the forming of an infection chain - is possible. The information that a data subject was infected and was in contact with other data subjects is thus necessary.

By using unresolvable pseudonyms, the processing already makes use of an indicator that is as far removed from the actual identity of the data subject as possible. The processing thereby already uses an approach that minimizes the interference with the fundamental right to the protection of personal data to a minimum.

13.1.2.5.4. Respect for the essence of the fundamental right

The processing in the EFGS and the compliant subsequent processing activities also respect the essence of the fundamental right to the protection of personal data.

The processing itself is aligned with the fundamental right to the protection of personal data. While it does interfere with the fundamental right, the interference is by means of pseudonyms that are no longer resolvable to the identity of a natural person. Pseudonyms constitute personal data because of the existing 1:1 relationship with the identity of a natural person. The pseudonyms do not contain any links to the identity behind the pseudonym any longer however, they correlate as little as possible with the natural person. The essence of the fundamental right to the protection of personal data is thereby respected because the personal data being processed is as economical with its relationship to the identity of the natural person behind the personal data as possible.

The processing also does not affect the core of the fundamental right to the protection of personal data. The core of the fundamental right to the protection of personal data is the sovereignty of the data subject with regard to the freedom of choice which personal data of the data subject is processed by whom to what extent.

The freedom of choice concerning the processing of personal data at all is maintained since the use of the national contact tracing and warning application relies on a voluntary basis. In case of a consent as the legal basis of the processing, the consent has to be given freely, in case of a statutory law, the data subject has to submit the personal data voluntarily and the law may not require the data subject to do so.

This choice also entails a choice concerning the controllers of the processing. At a minimum, by being able to choose whether to share their personal data or not, the user also determines who is enabled to process their data. A further option to share the personal data only with specific controllers in terms of specific member states would undermine the pursuit of the legitimate purpose as neither the right to mobility nor to human health are specific to certain parts of the European Union. Due to its contagious nature, the COVID-19 virus can result in cross-border infection chains without reservations

as to specific member states. A pursuit of the EFGS's purpose only for a select number of member states would therefore be antithetic and the pursuit needs – by nature – to comprise all of the member states.

Finally, the data subject's sovereignty regarding the extent of the processing is maintained by processing personal data that is uncorrelated to the identity of the respective data subject to an extent that it conceals this identity effectively. The choice to disclose an infection with the COVID-19 virus thereby remains with the data subject. The processing in the EFGS and the subsequent processing maintain the concealment of the identity and leave the disclosure of an infection to the data subject.

The processing in the EFGS and compliant subsequent processing activities are therefore proportionate to the objectives in the general interest.

13.2. Privacy considerations

The processing in the EFGS is required to observe the principles relating to the processing of personal data according to Article 5 (1), (2) GDPR and Article 4 (1), (2) EU-DPR.

13.2.1. Observation of privacy principles based on the use of personal data

The EFGS offers four functions to process data: Uploading and downloading temporary exposure keys supplemented with metadata, calling back national back-ends regarding newly uploaded temporary exposure keys and monitoring the EFGS. Only the upload, download and callback functions process personal data, the monitoring function only processes statistical data without any reference to identities of natural persons.

13.2.1.1. Upload function

The upload function processes the personal data described in detail in section 11.4.3.

13.2.1.1.1. Purpose limitation

The processing of the personal data by the upload function of the EFGS observes the requirements of the purpose limitation according to Article 5 (1) lit. (b) GDPR, Article 4 (1) lit. (b) EU-DPR and Article 7a (1) Implementing Decision (EU) 2020/1023. The processing is executed in furtherance of the legitimate purpose and respects the legitimate purpose's limitations as mandated in Article 7a (1) Implementing Decision (EU) 2020/1023. The upload of the personal data is required for the achievement of the legitimate purpose.

13.2.1.1.1.1. Purpose limitation: temporary exposure key

Each temporary exposure key is uploaded in order to facilitate the interoperability of the national back-ends and to continue the contact tracing effort in a cross-border context.

The contact tracing efforts are based on the use of non-resolvable pseudonyms in order to enable the detection of eventual contacts between infected users and users that are consequently eventually infected, without disclosing the identities of the infected users. In order to avoid a centralization of contact data leading to the possibility of establishing a social graph, the determination of a contact has to be performed in a decentralized way on the users' mobile devices. This requires the sharing of the unresolvable pseudonym, the temporary exposure key, once it is determined that a user is infected. Each temporary exposure key is therefore a necessary and adequate point of data that needs to be processed in order to achieve the purpose.

The processing in the form of the upload is necessary as the EFGS is the means to distribute the temporary exposure keys and thus enable the sharing. This requires the upload of this point of personal data to enable the later sharing of the temporary exposure keys.

Since the sharing of the infected user's temporary exposure key is voluntary and the respective infected user exercises their free will to share the temporary exposure keys, a stricter reading of the purpose, adding the voluntary facilitation of the interoperability and the voluntary continuity of contact tracing as a requirement, is also satisfied.

The temporary exposure key of an infected user contains "days since onset of symptoms" or "transmission risk level" parameters to enable the risk estimation of a contact with the infected user. Without these parameters, only the fact of a contact between an infected user and a potentially infected user in consequence of that contact can be established by means of the temporary exposure key. As the infectiousness of a contact varies depending on the stage of incubation of the infected user, the "days since onset of symptoms" parameter or the "transmission risk level" parameter associated to the respective temporary exposure key enable a clearer and more precise estimate of the infection risk of the contact. This in turn allows for a more precise and pragmatic warning of the potentially infected user, resulting in a better chance of breaking the infection chain while impacting the potentially infected user as minimally as possible.

These considerations are in line with the legitimate purpose of the processing and respect the boundaries of this purpose: The processing serves to improve public health. A more precise assessment of the infection risk and minimizing the impact of a warning on the potentially infected user achieves this purpose as it enables a more pin-point warning and allocation of resources to users with a high likelihood of infection while disrupting the lives of the users with a low risk as little as possible. The processing of the data parameter is therefore both necessary and adequate for achieving the purpose.

13.2.1.1.1.2. Purpose limitation: Countries of interest

The user is enabled to provide a list of countries that the user associated with during the infectious period. The provision of this information is voluntary. It enables the national back-ends downstream of the EFGS that downloaded the personal data, to package it in a way more suitable for the processing by the mobile devices of users that want to compare their contacts. It enables the national back-ends to generate smaller data packages for those users, who know that they did not leave the country of origin of their national warning application. Those users are interested in a smaller download of temporary exposure keys of infected users that associate with their country of origin.

The processing of this data point thus enables the national back-ends to allow a more targeted download of data for these users. In turn, this allows less powerful mobile devices to participate in the contact tracing effort by minimizing the amount of data downloaded and processed in the mobile device.

In consequence, the processing of this data point observes the legitimate purpose and respects the limits of this purpose. It furthers the contact tracing effort by allowing less powerful mobile devices to participate while limiting the amount of data distributed to the users.

13.2.1.1.1.3. Purpose limitation: Origin

The origin identifier is required to enable the national back-ends downstream of the EFGS to parse and process the downloaded data. The origin identifier allows the determination of the rule set that the downloaded data is subject to.

The identifier thus enables the facilitation of the interoperability of the national efforts since it is required for the accuracy of the interpretation of the provided data downstream of the EFGS.

13.2.1.1.1.4. Purpose limitation: Report type

The report type allows the national back-ends downstream of the EFGS to ascertain whether the provided data meets the requirements for the national back-end to trust the data. It enables the national back-ends to form a better understanding of the shared data and to avoid disruption of public life. If the parameters of the pandemic in a member state allow the consideration that it is safer to require a higher level of certainty regarding the test results than disrupting the lives of users with a lower level of risk of an infection, this consideration can be performed on the basis of the report type.

Therefore, the identifier enables the facilitation of the interoperability of the national efforts by enabling more finely tuned approaches according to the respective present situation in a country downstream of the EFGS.

13.2.1.1.2. Lawfulness, fairness and transparency

The processing of the personal data by the upload function of the EFGS observes the requirements of lawfulness, fairness and transparency according to Article 5 (1) lit. (a) GDPR, Article 4 (1) lit. (a) EU-DPR. The processing is lawful, fair and transparent.

As discussed in sections 13.1 of this document, the legal basis of the processing for the personal data needs to meet the fairness and transparency requirements in order to enable a lawful processing with regard to the fundamental rights according to Article 16 (1) TFEU and Article 8 (1), (2) Charter. The requirements for the respective legal basis have to be observed before the processing and can be stipulated.

In consequence, the processing of the personal data is lawful. It is transparent as the different steps of the processing are disclosed in this document, the code of the EFGS is disclosed and information regarding the processing in the EFGS and the subsequent processing by the member states has to be provided in the notices provided to the user prior to sharing the relevant personal data. The processing is fair since the fairness guarantees detailed in sections 13.1.2.4.1of this document have to be fulfilled.

13.2.1.1.3. Data minimization

The processing of the personal data by the upload function of the EFGS is limited to the minimum amount of data required according to Article 5 (1) lit. (c) GDPR, Article 4 (1) lit. (c) EU-DPR.

The data minimisation principle is not limited to assessing the amount of processed data in terms of bits. Rather, the correlation between the processed data and the identity of the natural person behind that data is to be considered.

The upload to the EFGS concerns pseudonyms that are designed to be unresolvable. The correlation between the temporary exposure keys and the identity of the natural person behind the temporary exposure keys is concealed as much as possible. Thus, the data minimization principle is observed.

13.2.1.1.4. Accuracy

The accuracy of the personal data processing in EFGS is ensured by the signing of the uploaded data by the uploading national back-end. The principle of accuracy according to Article 5 (1) lit. (d) GDPR, Article 4 (1) lit. (d) EU-DPR is observed.

13.2.1.1.5. Storage limitation

The uploaded data is retained in the EFGS for a maximum of two weeks as determined in the Commission Implementing Decision (EU) 2020/1023. The temporary exposure keys' maximum time of significance regarding the infectiousness of the person behind the temporary exposure keys is also limited to two weeks. The time of data retention is therefore limited to the time of significance of the temporary exposure keys. Since temporary exposure keys can not be matched to dates, the retention period for all temporary exposure keys is necessarily the same.

The principle of storage limitation according to Article 5 (1) lit. (e) GDPR, Article 4 (1) lit. (e) EU-DPR is observed.

13.2.1.1.6. Integrity and confidentiality

The EFGS's processing adheres to the security by design principles as described above. It uses appropriate mechanisms to ensure that the processing operates as documented in a secure and transparent manner.

The principle of integrity and confidentiality according to Article 5 (1) lit. (f) GDPR, Article 4 (1) lit. (f) EU-DPR is observed.

13.2.1.2. Upload function

The download function processes the same relevant data points of personal data as the upload function, see section 13.2.1.1 of this document. It does not add additional personal data to the data points described afore. The privacy considerations for the upload function therefore apply identically.

13.2.1.3. Callback function

The callback function only signalizes the upload and availability of new data to a national back-end downstream of the EFGS. Since the upload schedule of the uploading national back-end does not allow the derivation of timing information when the personal data was shared by the user with the national back-end, the callback function does not add additional personal information.

The processing following the callback is identical to the download function, the privacy considerations apply identically.

13.3. Design decisions based on data flow

The concept of privacy by design is a fundamental requirement for the effective implementation of data protection. There is a growing understanding that innovation, creativity, and competitiveness must be approached from a "design-thinking" perspective. Privacy must be embedded into technologies, operations, and information architectures in a holistic, integrated, and creative way. A holistic approach is required because additional, broader contexts must be considered. Integrative approaches are required because all stakeholders and interests should be consulted. Creative approaches are needed because embedding privacy sometimes means re-inventing existing choices as the alternatives are unacceptable. This results in data protection becoming an essential part of the

core functionality provided. Data protection is an integral part of the system without compromising functionality.

This chapter provides an overview of which design decisions have been made in order to design the EFGS in a way that protects fundamental rights.

Please, see the attached document “Design Decisions” to learn more about the design decisions made.

13.3.1. Transparency

How do you make sure that the information you provide actually reaches the individuals concerned? Is the information you provide complete and easy to understand? Is it targeted to the audience? E.g. children may require tailored information. In case you defer informing people, how do you justify this?

13.3.1.1. Description

This report provides a risk analysis but also serves as documentation of the data processing in the EFGS in order to increase transparency. In addition, information about the EFGS, the details of the relevant controllers, and a link to the privacy notices of the controllers containing information about the processing activities in the EFGS is going to be provided on a Commission webpage for EFGS. For technology enthusiast, there is also the possibility to obtain information regarding the architecture of the EFGS on Github and to follow up on and support the development, because the code of the EFGS is open source. Finally, the Commission is going to maintain a record of processing activities carried out on behalf of the controllers in accordance with Article 31(2) of Regulation (EU) 2018/1725.

For more details see chapter F.I.4 of the Design Decisions.

13.3.2. Purpose limitation

Have you identified all purposes of your process? Are all purposes compatible with the initial purpose? Is there a risk that the data could be reused for other purposes? How can you ensure that data are only used for their defined purposes? In case you want to make available / re-use data for scientific research, statistical or historical purposes, what safeguards do you apply to protect the individuals concerned?

13.3.2.1. Description

Personal data shall only be used within the scope of the original purpose of processing and shall not be combined with other data. Contact tracing applications can only be a temporary solution as part of a comprehensive public health strategy to fight the current pandemic. It is an obligation of the member states to use the national app and the interoperability solution only for as long as necessary to combat the pandemic. “Federation Gateway” means a network gateway operated by the Commission through a secure IT tool that receives, stores and makes available a minimum set of personal data between Member States’ back-end servers for the purpose of ensuring the interoperability of national contact tracing and warning mobile applications. The proximity data of an infected person (exposures) remain local on the mobile device and are not shared (decentralised solution). The calculations as to whether contact with an infected person may have led to an infection are only carried out locally on the device.

For more details see chapter F.I.7 of the Design Decisions.

13.3.3. Data minimisation

Is the amount of personal data collected adequate for the processing? Are the data itmes of sufficient quality for the purpose? Are there data items you could remove (or mask/hide) without compromising the purpose of the process? Do you clearly distinguish between mandatory and optional items in forms? In case you want to keep information for statistical purposes, how do you manage the risk of re-identification?

13.3.3.1. Description

The following provides an overview of the design decisions that serve the privacy goal of data minimisation. Accordingly, personal data must be adequate and relevant to the purpose and limited to what is necessary for the purposes of the processing. Developers have limited as much as possible the permissions of the application, minimized the data processed, where possible pseudonymized and/or anonymized data, protected any remaining sensitive data processed by the app or the back-end, and are going to delete it when no longer needed. Only pseudonyms that are designed to be unresolvable are uploaded to the EFGS. A correlation between the diagnosis keys and the identity of the natural person behind the diagnosis keys is concealed as much as possible. Only as little data as possible is logged and processed and deleted as soon as it's not needed anymore.

For more details see chapter F.I.6 of the Design Decisions.

13.3.4. Accuracy

What could be the consequences for the persons affected of acting on inaccurate information in this process? How do you ensure that the data you collect yourself are accurate? How do you ensure that data you obtain from third parties are accurate? Do your tools allow updating / correcting data where necessary? Do your tools allow consistency checks?

13.3.4.1. Description

Since the contact tracing applications are based on the voluntariness and willingness to cooperate of as large a part of the population as possible, design decisions must serve the goal of avoiding a loss of confidence on the part of the population. That is why measures need to be put in place to ensure data accuracy need to be maintained in the interoperable system. The audit interface of the EFGS contains operations to audit parts of the service by the users from outside to validate the integrity of the running system.This audit operation provides the possibility to verify data integrity within a batch. The operation returns information about the batch, for instance:

- Countries contained in the batch
- Batch signatures by country
- Uploading Information

All this information can be cross-checked over the certificate authority.

Currently there is a high risk because of self-reported test results that needs to be solved to ensure the accuracy of data in the system (see section**Error! Reference source not found.**).

It is suggested to start a bug bounty program by the institution responsible for the application in order to identify, correct, and announce errors in the software. The discoverers are promised a material or monetary prize as a reward. The initiation of a bug bounty program would significantly increase the public's confidence in the security of the EFGS.

Finally, data accuracy is supposed to be established by so-called penetration tests. Security researchers are engaged who search for security issues in the EFGS as a hacker would. The penetration tests should

be performed by different vendors as each team has its own focus and emphasis when performing the tests. The penetration tests are performed no later than before each release of a new version of the EFGS. The final reports of the tests are published.

For more details see chapter F.I.2.3 of the Design Decisions.

13.3.5. Storage limitation

Will personal data used in this processing operation regularly reviewed and kept no longer than it is needed (for the purpose it was collected)? Will it be erased or anonymised when it is no longer needed? Does EU legislation define storage periods for your processing operation? Is the retention period you established for your processing operation compatible with retention periods defined in the Common Retention List for European Commission Files? Can you distinguish storage periods for different parts of the data? If you cannot delete the data just yet, can you restrict access to it? Will your tools allow automated permanent erasure at the end of the storage period?

13.3.5.1. Description

In line with the data protection goal of data minimization, personal data may only be processed for as long as it is necessary to achieve the purpose. Accordingly, personal data must be adequate and relevant to the purpose and limited to what is necessary for the purposes of the processing.

Uploaded diagnosis keys are stored for 14 days. While theoretically unnecessary if direct forwarding is used, practical considerations make temporary buffering worthwhile:

1. Packets get lost and back-ends may be unavailable. With stored data, download retries are possible.
2. Timing of downloads is left to the back-ends instead of forcing a schedule.
3. Newly onboarded countries get the data for the past 14 days at once, so they don't miss important data.

The data is erased by a run scheduled every 6 hours which deletes all data records intended for erasure. Automated data deletion is realized by implementing the deletion routines by a cron job. During the daily EFGS process, these routines receive all the information necessary for the deletion; namely all data which is flagged for deletion. The data field "Created_at" (Source: DFC) is used as a marker. Every data record is linked to this attribute. If this field contains a date that is older than the set time limit of 14 days, then all associated data records in the system are completely deleted. After the end of the provision of service, delete any remaining data unless Union or Member State law requires storage of the personal data.

For more details see chapter F.I.6 and F.I.9 of the Design Decisions.

14. Risk assessment

14.1. Description of the method of risk assessment

14.1.1. Introduction

A risk assessment process considers the risk of processing personal data within the EFGS in terms of their likelihood of occurrence (likelihood) and the impact of their consequences (severity).

The GDPR provides data controllers with flexibility to determine the precise structure and form of the Data Protection Impact Assessment (DPIA) in order to allow the assessment to conform to existing working practises. Different methods can be used to assist in the implementation of the basic requirements set out in the GDPR. In order to allow these different approaches to exist, common criteria have been identified by the Article 29 data protection working party in their "*Guidelines on data protection impact assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679*"[52] (hereinafter referred to "WP 248"). Inconsequence, it is up to the data controller to choose a method, but this method should be compliant with the criteria provided in Annex 2 of WP 248[53]. The DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them.

An international standard also provides guidelines for methods used for carrying out a DPIA. It is ISO/IEC 29134, which is referred to in WP 248[54]. In this DPIA, the standard ISO/IEC 29134 is applied in order to prepare the assessment.

Furthermore, the template of the EU[55]was implemented in the risk-matrix for this DPIA.

14.1.1.1. Overview risk matrix

The risk matrix has been developed as a dynamic document to carry out the assessment during the design process of the EGFS (see Annex 1 to this DPIA-report).

14.1.1.1.1. Form and substance

The risk matrix is an Excel workbook consisting of the following Excel-worksheets:

1. Excel-worksheet "risk analysis",
2. Excel-worksheet "data protection level",
3. Excel-worksheet "severity of impact",
4. Excel-worksheet "Likelihood",
5. Excel-worksheet "management evaluation",
6. Excel-worksheet "offenders - risk sources",
7. Excel-worksheet "Types of attack".

14.1.1.1.2. Description of the excel-worksheet "risk analysis"

The risk assessment is carried out and documented in the Excel-worksheet "risk analysis".

---

[52] https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[53] WP 248, p. 17

[54] WP 248, Annex 1, p. 21

[55] EU-DPIA_template_part_1 and EU-DPIA_template_part_2

14.1.1.1.2.1. Columns

The columns A to S are used for the assessment in the following manner:

A-risk source

B- ID

C- threat / risk

D-further description of risk

E- Description of potential impact (see scenarios in table sheet "severity of impact")

F- Risks for specific groups of data subjects (optional)

G – Data protection level

H – vulnerability (yes / no)

I – Likelihood

J – Data minimisation

K- Confidentiality

L – Integrity

M – Availability

N – Authenticity

O – Resilience

P – Intervenability / Control

Q – Transparency

R- Purpose limitation / Unlinkability

S – Risk level.

14.1.1.1.2.2. Overview of the records

In the Excel-worksheet “risk analysis”, column “C”, the determined risks are listed. The list is freely extensible. The risk source (column A) is assigned to each risk, then each risk is given a short description (see column D) and specified further in the following columns.

14.1.2. Identification and description of relevant threats/risks

14.1.2.1. Sources of risk

This section describes the sources of risks identified regarding the relevant EGFS processing activities. Sources of risks are at first attackers (insiders/outsiders) with interest in unlawful processing activities and unlawful use of involved personal data. Furthermore, the data subject as well as the controllers themselves, while intending lawful processing, may create risks inherent in this lawful processing for data subjects.

The following sources of risk were identified and determined:

R1 – user CWA-App

R2 – Hacker

R3 – (commercial) data collector

R4 – software/ service provider

R5 – employer

R6 – criminals

R7 – healthcare

R8 – public authorities (member states).

In the Excel –worksheet “risk analysis”, in column A, the source of risk can be selected as required.

14.1.2.2. Description of risks/threats

This section describes the conditions and potential risks that may threaten or compromise personal data of the data subjects and impact everyone’s rights and freedoms, using the GDPR as the precept for the required standard of privacy, data protection targets to guarantee and individual rights of data subjects to protect. The specific risks are categorized - according to the untoward events to be avoided - as follows:

1. unlawful processing within the EFGS and processing interfering with the fairness requirement of Article 8 Charter
2. Non-transparent processing
3. Unauthorized disclosure or access to personal data
4. Unauthorized transfer of personal data (to a third country)
5. Unintended loss or damage of personal data
6. Disregard of data subjects’ individual rights
7. Use of personal data for new or different purposes
8. Processing of incidental and unexpected personal data
9. Processing of incorrect personal data
10. Incorrect processing of personal data (technical failures, software malfunction, human mistakes)
11. Processing of redundant personal data
12. Risks for data subjects resulting from the processing per se.

To determine the specific risks of the processing mentioned above, different sources are used, for instance threat modelling, testing, expert references in operative and technical data protection and IT-Security modelling.

14.1.3. Categories of personal data concerned

In column G, the data protection level is determined depending on the categories of personal data concerned. In the Excel-worksheet “data protection level”, categories are matched with the level “NORMAL (2)” or “HIGH (3)”, according to the following categories, mentioned in the EU Commissions’ template:

☐ Simple data *(e.g. contact details, full name, data on education, professional experience, data already available online)*

☐ Behavioural data *(e.g. location, traffic data, data on personal preference and habits)*

☐ Financial data *(e.g. financial transactions, bank statements, investments, credit cards, invoices)*

☒ Sensitive data *(personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data or data concerning a natural person's sex life or sexual orientation).*

Sensitive data needs to be classified with the level HIGH (3). Therefore, for the purposes of this DPIA, the level HIGH was assumed for each assessed risk.

14.1.4. Assessment of risks for specific groups of data subjects

The expected impact of a risk to data subjects' rights or freedoms may differ for various groups of data subjects. Affected groups can be selected in column F. Then, the risks can be determined for different groups, for example:

- minors
- epidemiological risk groups (elderly people, people with relevant medical history),
- cross-border workers.

For the version 1.4 of the DPIA-report, this assessment has not yet been carried out. The risk assessment has been carried out in general for generic users of national apps as data subjects in general.

14.1.5. Assessment of the likelihood

Likelihood is a value expressing the reasonable expectation for the occurrence of a risk based on the following phased model, which is recommended by the EU Commission:

Likelihood

1	LOW	Rare. Materialization of the risk would be very uncommon or very unusual, cannot be excluded but the risk normally should not materialize.
2	MEDIUM	May happen. Materialization of the risk would be uncommon or unusual, but the risk may materialize.
3	HIGH	Quite often. Materialization of the risk would not be uncommon, but it is not certain.
4	VERY HIGH	Very often. Materialization of the risk is expected.

Table 26: likelihood

As a part of this assessment, the required skills and resources of attackers, the volume of personal data concerned and the envisaged mitigation measures as described above were taken into account. For this purpose, the model was refined.

The model is described in the risk matrix, Excel-worksheet "Likelihood".

14.1.6. Assessment of severity

The severity of the consequences for a data subject of a risk materializing is assessed according to the following phased model, which is recommended by the EU:

Severity

1	LOW	Individuals either will not be affected or may suffer a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2	MEDIUM	Individuals may suffer significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3	HIGH	Individuals may suffer significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4	VERY HIGH	Individuals may suffer significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

Table 27: severity

As a part of this assessment the following types of damages for data subjects were taken into account:

- societal/social disadvantages (reputational damage or loss),
- "intimidating effects" (for fear of disadvantages, data subjects give up their rights or freedoms),
- damages to privacy (losing control over their own data, surveillance, publication of personal data, quarantine and violation of fundamental rights (freedom of speech, freedom of movement…) etc.),
- impairment of physical integrity (wrong medical treatment, exposing crimes),
- economic disadvantages/material damages (loss of job, disadvantages regarding the respective professional career, reduction of public services, increase of health insurance premiums).

For this purpose, the model was refined and described in the risk matrix Excel-worksheet “severity of impact”.

14.1.7. Potential impacts to the rights and freedoms of data subjects

The severity of impact for data subjects related to the described risks was assessed vis-à-vis the impact of the realization of the risk on the affected principles relating to the processing of personal data. The latter are used in the columns of the risk matrix as follows:

- data minimization (personal data limited to what is necessary for the processing),
- Confidentiality (no unauthorized access to personal data),

- integrity (no unauthorized modification and deletion of personal data),
- availability (ensure the availability of personal data as long as needed for processing)
- legitimate origin (the personal data originates from a legitimate source and is adequately authenticated)
- resilience (ensure the lawful processing of personal data even under difficult conditions),
- intervenability/ control (ensure the lawful processing of personal data by intervene in data processing, e.g. to ensure data subject's rights)
- transparency (ensure the transparent processing of personal data, all required information is provided to data subjects),
- purpose limitation/unlinkability (ensure purpose limitation of processing personal data, ensure that data are not linked, which is collected for different purposes).

The potential impact of a tangible or intangible damage for data subjects was considered for each risk according to the data protection principle concerned and documented in the risk matrix, Excel-worksheet risk analysis, columns J to R.

14.1.8. Risk level/index of risk

The index of risk is the result of the multiplication of the considered level of likelihood (1-4) and the level of severity (1-4). The highest level of severity observed is used as the factor in this multiplication. The result is documented in column S.

The following illustration shows the risk level as traffic light colours, the categorisation of risk/Index of risk. The column "Description" is used as a proposal for prioritisation.

Risk level	Risk-Category / Index of Risk	Description
LOW	0-4	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem. Materialisation of the risk would be very uncommon or very unusual.
MEDIUM	5-7	a) Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties. Materialisation of the risk would not be uncommon, but it is not certain. b) Individuals may encounter significant consequences, but no permanent or irreversible damages and breach of fundamental rights Materialisation of the risk would be uncommon or unusual, but the risk may materialize. Technical and organizational measures SHALL be implemented. As part of a cost-benefit analysis risks can be accepted.

	8-10	Individuals may encounter significant consequences, but no permanent or irreversible damages and breach of fundamental rights. Materialisation of the risk would not be uncommon, but it is not certain. Technical and organizational measures SHALL be implemented in a specific and short time period. The mitigation of risks by technical and organizational measures has to be controlled. As part of a cost-benefit analysis risks can be accepted, but a special management review is required. **Suggestion:** **If the risk index is higher than 8, the supervisory authority must be consulted. Please inform the DPO of the accordingly.**
HIGH	11-16	Individuals may encounter irreversible damages and breach of fundamental rights. Materialisation of the risk is expected. Immediate Attention and mitigation measures are needed and controlled. There is no acceptance of high risks by the controller alone. **Suggestion:** **Supervisory authority must be consulted. Please inform the DPO of the controller accordingly.**

Table 28: risk level (suggestion)

14.1.9. Envisaged measures

The risk assessment is based on envisaged measures and design decisions. These measures are described in the risk matrix, Excel-worksheet "risk analysis" columns T and R. Particularly, the design decisions (Annex 2 to this report) and technical and organisational (security) standards of the operators of the EFGS are referenced.

14.1.10. Summary

The risk matrix, particularly the Excel-worksheet "risk analysis" is an attachment to this DPIA-Draft (Annex 1: Risk matrix).

In the following section, specific risks are highlighted, which are considered as remaining high risks or as important otherwise (e.g. risks with high impact on data' subjects rights). Furthermore, the key issues mentioned by the EDPD[56]were included in this selection, particularly legal basis, transparency, data retention and minimisation, information security and data accuracy issues.

[56] EDPS's Statement on the data protection impact of the interoperability of contact tracing apps, 16 Juni 2020, p. 2-5

14.2. Risk assessment for specific risks

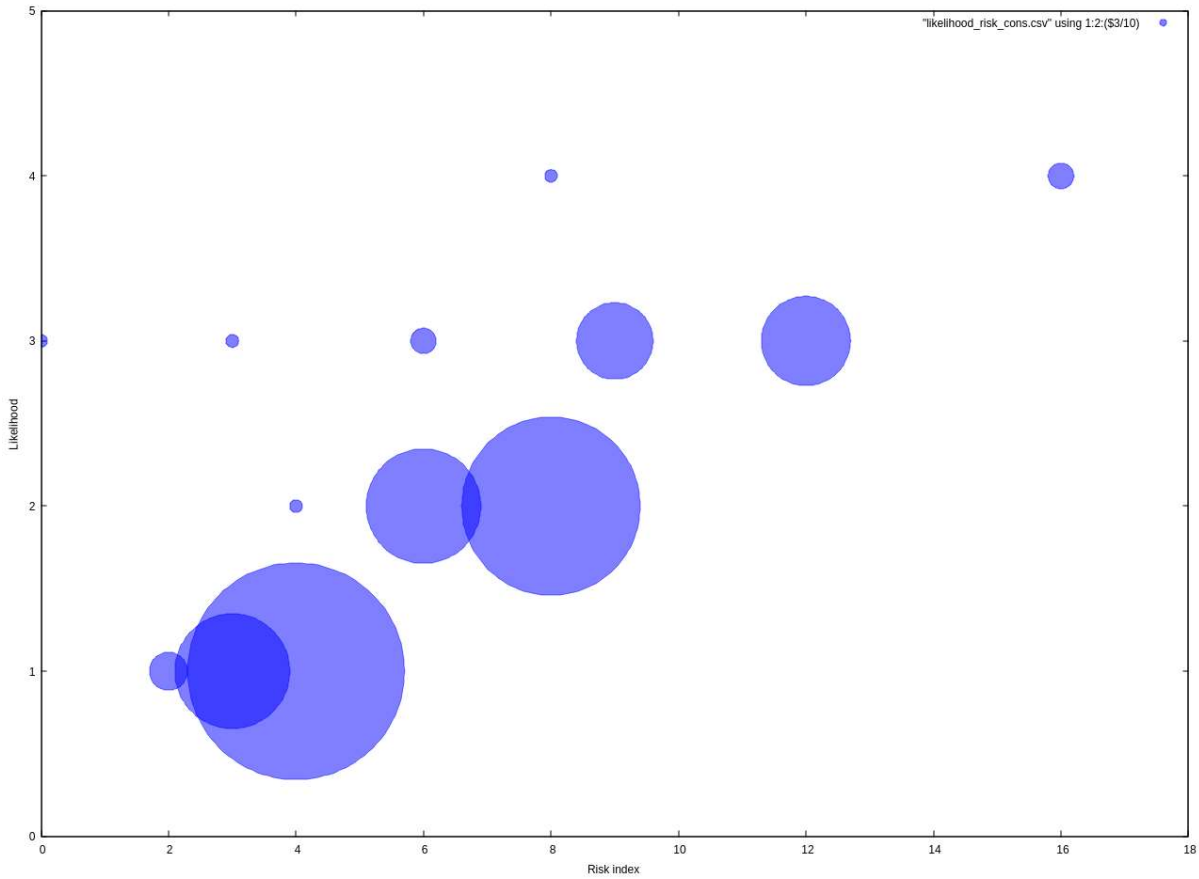
[CONFIDENTIAL PURSUANT TO ARTICLE 4(1)(a) OF REGULATION (EU) 1049/2001]

14.3. Risk Clusters

In so far as the risks have not been discussed in section 14.2. above, the risks can be clustered according to their risk index and their likelihood. The severity of a risk to the data subjects is an imminent concern when determining the proportionality of the acceptance of the risk and the use of this license in order continue the processing. Grouping risks according to their severity thus allows for a more focussed discussion of the balance to be achieved between the legitimate purpose of the processing and the possible implications for the data subjects.

Including the likelihood as a factor in this grouping ensures, that risks which carry potentially severe consequences while also being very probable in their realization are given considerable weight and are not undervalued vis-à-vis risks with considerably less probability of realisation.

The structure of the evaluation of the risks lends itself to this type of clustering since the scores regarding risk index and likelihood categorize the risks into islands to a smaller or larger extent. In the following graphic, the distribution is shown and larger circles represent more prominent occurrences of the same risk index and likelihood for risks:



14.3.1. Proportionality of risks with a very high risk index and a very high likelihood (risk_index=16, likelihood=4)

There are a total of three risks in this group, table rows 7, 69, 78. They concern the processing of personal data after the withdrawal of a consent, the upload of false positive test results or technical limitations of the technical basis of the exposure notification framework used in the national contact tracing and warning mobile applications. The risks are proportional to the legitimate purpose.

14.3.1.1. Withdrawal of consent, technical limitations

The processing of personal data after the withdrawal of a consent and the technical limitations of the technical basis of the exposure notification framework used in the national contact tracing and warning mobile applications concern themselves both with the randomness of the temporary exposure keys, used as unresolvable pseudonyms. Where the withdrawal of a consent has to remain ineffective due to the fact that the data subject can not prove a relationship concerning specific temporary exposure keys, the technical limitations express the concern that the temporary exposure keys as pseudonyms remain unresolvable.

In both cases, the likelihood of realising the risk is high because the inability of the data subject to prove its ownership of certain temporary exposure keys is virtually guaranteed, if the temporary exposure keys hold up against the condition to be random and unresolvable. The technical limitations may pose a risk due to actors with great resources and significant access, such as the providers of the exposure notification framework.

In both cases, incurring the respective risk is adequate to further the legitimate purpose. The operation of the EFGS enables the pursuit of the legitimate purpose and increases the chance of breaking cross-border infection chains, thus improving public health and assisting in a return to unhindered mobility within the European Union. It is also necessary as less onerous means are not available.

The use of the license to process also respects the essence of the fundamental right to the protection of personal data according to Article 8 (1) Charter. With regard to the inability of the data subject to enforce the data subject rights effectively, the risk can not be mitigated with regard to its realisation. However, while the inability to enforce these rights interferes severely with the fundamental right, the data is practically uncorrelated to the identity behind the pseudonyms. The design emphasis the data minimisation in contrast to the data subject rights. As discussed before, the GDPR allows for this prioritisation of the data minimisation principle. The use of the license thus still respects the essence of the fundamental right.

With regard to the technical limitations, the essence of the fundamental right is also preserved. The processing does not grant legal permission to access the personal data for actors such as the ones described. An access would still remain subject to the sanctions under the GDPR. The factual enabling of such an access can be mitigated by a strict auditing of the actions of the actors described and by scrutinizing their behaviour. This can be achieved by the correct use of regulatory oversight. In this case, the respect for the essence of the fundamental right is preserved. As much as the GDPR expresses the essence of the fundamental right to privacy in terms of a prohibition of blind trust, see e.g. Article 25, 28 and 32 GDPR, it does not require an overarching assumption of sanctionable behaviour of the providers of the exposure notification framework. A suitable regulatory regime and cooperation can be established and is appropriate in order to maintain the required respect for the essence of the fundamental right.

14.3.1.2. False positives

The operation of a distributed contact tracing system entails the risk of false positives as it relies heavily on the processing of data in the mobile phones of the users, thus allowing them a certain amount of

freedom to determine the outcome of the processing. The license to process the personal data in light of the risk is thus adequate and necessary as it is inherent in this form of processing.

The respect for the essence of the fundamental right to the protection of personal data according to Article 8 (1) Charter requires a sufficient mitigation of this risk. As it is at the joint controllers' discretion to accept the specific methods of verification of a test result, it is also in their purview to mitigate the risk sufficiently. Stipulating such sufficient mitigation, the essence of the fundamental right is respected.

14.3.2. Proportionality of risks with a high risk index and a high likelihood (risk_index=12, likelihood=3)

The six risks contained in this group all concern themselves with the illicit processing of personal data either without a legal basis or with an insufficient legal basis.

Incurring the risks is adequate and necessary: The processing is adequate and necessary to further the pursuit of the legitimate purpose.

The use of the license to process also respects the essence of the fundamental right to the protection of personal data according to Article 8 (1) Charter. In so far as the risks concern the processing without a sufficient legal basis, it is at the joint controllers' discretion to either create a sufficient legal basis or to contain the processing within the limits set by the legal basis. With regard to third parties performing processing activities without a legal basis, the responsibility rests on the joint controllers to exercise adequate supervision or regulatory scrutiny. The controllers are thus able to mitigate the risks. Stipulating such sufficient mitigation, the essence of the fundamental right is respected.

14.3.3. Proportionality of risks with a higher medium risk index and a high likelihood (risk_index=9, likelihood=3)

The seven risks concern themselves with a lack of transparency, inadequate processing or re-identification due to metadata.

Incurring the risks is adequate and necessary: The processing is adequate and necessary to further the pursuit of the legitimate purpose.

The essence of the fundamental right to the protection of personal data according to Article 8 (1) Charter is also respected. The risks may be mitigated by technical or organisational measures or are within the regulatory purview of the joint controllers. In consequence, there is a reasonable expectation of control of the risks, the essence of the fundamental right is respected.

14.3.4. Proportionality of risks with a medium risk index and a medium likelihood (risk_index=8, likelihood=2)

The risks are associated with a medium likelihood. Incurring the risks is adequate and necessary: The processing is adequate and necessary to further the pursuit of the legitimate purpose.

The essence of the fundamental right to the protection of personal data according to Article 8 (1) Charter is respected because the risks can be mitigated by technical and organisational measures as described in the matrix. In consequence, the fundamental right has a reasonable expectation to be protected by the joint controllers as the mitigation may be stipulated.

14.3.5. Proportionality of risks with a low medium risk index and a high or medium likelihood (risk_index=6, likelihood=3 or 2)

The risks are associated with a low medium risk index. They concern themselves with data manipulation and transparency issues as well as linkage attacks.

Incurring the risks is adequate and necessary: The processing is adequate and necessary to further the pursuit of the legitimate purpose.

The essence of the fundamental right to the protection of personal data according to Article 8 (1) Charter is respected. The risks are partially mitigated by technical and organisational measures. In so far as transparency issues and data manipulation are concerned, they are within the purview of the joint controllers and there is a reasonable expectation of control of the risks.

14.3.6. Proportionality of risks with a low risk index and a low or medium likelihood (risk_index<4, likelihood<3)

The risks are associated with a low risk index. Incurring the risks is adequate and necessary: The processing is adequate and necessary to further the pursuit of the legitimate purpose.

The essence of the fundamental right to the protection of personal data according to Article 8 (1) Charter is respected. The risks are partially mitigated by technical and organisational measures. Their impact on the data subject is low, they do not affect the core of the fundamental right to the protection of personal data. Thus, in comparison to the importance of the pursuit of the legitimate purpose and in light of the limited interference with the fundamental right, the essence of the fundamental right is respected.

15. Measures Envisaged to Address the Risks

15.1. General description of measures in place

The processing in the EFGS is going to be performed comprehensively by the EU Commission as processor according to Article 7a (5) Implementing Decision (EU) 2020/1023. The EU Commission is bound by law according to Article 288 (4) sent. 1 TFEU, Regulation (EU) 2018/1725 , and Article 7a, (5) sent. 2 Implementing Decision (EU) 2020/1023 to operate the EFGS securely.

The EU Commission has defined mandatory and legally binding standards regarding IT security according to Article 288 (4) sent. 1 TFEU, Article 14 (4) Commission Decision (EU, Euratom) 2017/46. These mandatory published standards are legally binding, and their application is mandatory.

15.2. Data hosted on DG DIGIT infrastructure

15.2.1. Description

The data will be hosted on infrastructure that is operated by DG DIGIT and hence meets the mandatory security standards for basic operation and monitoring (VM Hosting, OS Operation, Webserver Operation) (see section 11.9.1 above). The service providers SAP and T-Systems are not involved or required in the implementation of the security standards.

15.2.2. Supporting documentation

The relevant supporting documentation for the security measures applied has to be :

☐ Attached

☒Link:Security Rules of the Commission, IT Security Policy, Standards, Guidelines and Technical specifications

15.2.3. Measures adopted

Indicate the type of measures in place by selecting applicable measures and describing them from the following list, add measures if appropriate to the relevant processing operation:

☒Access control

Who has access to the processed data? How the access is controlled and protected? Are accesses registered and how long these traces are stored for?

Description

Security standards applying to all European Commission information systems, Access Control & Authentication security standard.pdf

See section 11.8 of this report.

☒Physical security

How physical access control is carried out regarding the premises accommodating the processing (zoning, escorting of visitors, wearing of passes, locked doors, etc.)? Are warning procedures in place in the event of a break-in? Where paper documents containing data are used during the processing, how they are printed, stored, destroyed and exchanged?

Description

Security standards applying to all European Commission information systems, ST_physical_security.doc

☒Backups

How are backups going to be managed? How is the security of the data at rest implemented?

Description

Security standards applying to all European Commission information systems,Backup security standard.pdf

See section 11.9.3 of this report.

☒Security of IT channels

What is the type of network on which the processing is carried out (isolated, private or Internet)? How is the security insured? What protocol is used?

Description

See section 11.5.1 and 11.5.2 of this report.

☒**Encryption and/or pseudonymisation of personal data**

What are the means implemented for ensuring the confidentiality of data stored (in the database, in flat files, backups, etc.)? Are the data encrypted? How and when?

Description

Security standards applying to all European Commission information systems,ST_crypto.doc

See section 11.4.6 and 11.5 of this report.

☒**Review of security measures**

Are the information security policies and measures reviewed regularily and, where necessary, improved? Once the processing operation ongoing, how often do you plan to review and, if necessary, to improve it?

Description

Security standards applying to all European Commission information systems,ITSRM2 - IT Security Risk Management Methodology.pdf

Security standards applying to all European Commission information systems,IT Vulnerability and Remediation Management security standard.pdf

☒**Personal data breach handling mechanism is in place**

What measures will you employ in case of data breach (i.e. unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data, etc.)? Do you have a specific procedure in place?

Description

Security standards applying to all European Commission information systems,ST_incident_mgt.doc

15.3. Application Operation

15.3.1. Description

Application operation and monitoring is carried out by T-Systems International GmbH, Security Monitoring by Deutsche Telekom Security GmbH. Contracts according to Article 28 GDPR were signed and technical and organisational measures are agreed, including sub-contractors. The authors of the DPIA-report have not reviewed the implementation of the security standards and rely on the correctness of the respective statements concerning their implementation.

15.3.2. Supporting documentation

If applicable, indicate the relevant supporting documentation for the security measures applied:

☐ Attached

☒Link:Security standards applying to all European Commission information systems

15.3.3. Measures adopted

Indicate the type of measures in place by selecting applicable measures and describing them if appropriate to the relevant processing operation:

☒**Access control**

Who has access to the processed data? How the access is controlled and protected? Are accesses registered and how long these traces are stored for?

Description

Security standards applying to all European Commission information systems,Access Control & Authentication security standard.pdf

See sec. 11.8 of this report.

☒**Physical security**

How is physical access control maintained regarding the premises accommodating the processing (zoning, escorting of visitors, wearing of passes, locked doors, etc.)? Are warning procedures in place in the event of a break-in? Where paper documents containing data are used during the processing, in which manner are they printed, stored, destroyed and exchanged?

Description

Security standards applying to all European Commission information systems, ST_physical_security.doc

☒**Backups**

How are backups going to be managed? How is the security of the data at rest implemented?

Description

Security standards applying to all European Commission information systems,Backup security standard.pdf

See section 11.9.3 of this report.

☒**Personal data breach handling mechanism is in place**

What measures will you employ in case of data breach (i.e. unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data, etc.)? Do you have a specific procedure in place?

Description

Security standards applying to all European Commission information systems,ST_incident_mgt.doc

A process will be designed by TSI to report data breaches without undue delay after having become aware of it.

16. Proportionality of the remaining risks vis-à-vis the purposes pursued

The risks remaining after mitigation are required to be proportional vis-à-vis the legitimate purpose that is pursued by the processing.

The processing in the EFGS and compliant subsequent processing activities are in the general interest in order to establish a high level of human health protection according to Article 168 (1) TFEU and to ensure an expedited return to full mobility for the citizens of the European Union according to Articles 20 (2) lit (a), 21 (1) TFEU.

For a remaining risk to be proportional to the legitimate purpose pursued, it needs to be appropriate, necessary and respectful regarding the essence of the fundamental right to the protection of personal data to incur the remaining risks.

In order to determine the appropriateness of the risk, it has to be determined whether incurring the risk allows the realization of the legitimate purpose. The measures leading to the occurrence of the risk are required to further attaining the legitimate purpose effectively.

The necessity of incurring a remaining risk is determined by the test for the existence of other measures that do not carry the remaining risk or carry that risk to a lesser extent.

Whether incurring the remaining risk respects the essence of the fundamental right to the protection of personal data has to be determined by the test if the core of this fundamental right - the sovereignty of the user regarding its personal data - is affected and if that core remains substantially untouched. This may only be the case if the user even after the realization of the risk remains in a position to determine if the user's personal data is processed, by whom it is processed and how it is processed.

The remaining risks according to section 16 of this document observe these criteria and pass the relevant tests.

16.1. Insufficient legal basis

The license to incur a risk of an insufficient legal basis is appropriate since the use of this license furthers the pursuit of the legitimate purpose. The license enables the pursuit of the legitimate purpose, thus furthering the attainment of the legitimate objective.

Incurring the risk is necessary: Without use of the license to incur the risk, the legitimate purpose may not be achieved, less onerous measures are not available.

The use of the license also respects the core of the fundamental right to the protection of personal data. The sovereignty of the user remains untouched. The personal data processed in the EFGS consists of unresolvable pseudonyms concealing the identity of the natural person behind the pseudonyms. The processing is designed to avoid the re-identification of the natural person as much as possible. Even if the risk is realised, the natural person behind the pseudonym remains concealed and unaffected. The data subject is still free to choose which personal data is processed by whom and how, since the processed pseudonyms do not enable any inference regarding the identity or further personal data of the data subject in as much as is possible. Furthermore, the likelihood of realization is very low, and the risk is highly controllable by nature. The averting of the risk is entirely in the hands of the joint controllers.

16.2. Non-transparent processing

The same considerations as in 16.1apply for the risk of non-transparent processing. The license to incur the risk is appropriate and necessary since it enables the pursuit of the legitimate purpose and less onerous measures are not available.

The use of the license respects the core of the fundamental right to the protection of personal data due to the nature of the processed data to be uncorrelated to the identity of the data subject as much as possible. Furthermore, the risk is under the full control of the joint controllers.

16.3. Processing of inaccurate personal data

The same considerations as in 16.1apply for the risk of processing inaccurate personal data. The license to incur the risk is appropriate and necessary since it enables the pursuit of the legitimate purpose and less onerous measures are not available.

The use of the license respects the core of the fundamental right to the protection of personal data due to the nature of the processed data to be uncorrelated to the identity of the data subject as much as possible.

16.4. Processing of redundant personal data

The same considerations as in 16.1apply for the risk of processing of redundant personal data. The license to incur the risk is appropriate and necessary since it enables the pursuit of the legitimate purpose and less onerous measures are not available.

The use of the license respects the core of the fundamental right to the protection of personal data due to the nature of the processed data to be uncorrelated to the identity of the data subject as much as possible.

17. Non-privacy risks

The operation of the EFGS is subject to risks not related to privacy aspects of the data processing. While these risks are not the focus of the considerations of this DPIA, they nevertheless may eventuate.

The non-privacy risks can be summarized as risks to the organisations operating the EFGS and risks resulting from misguided expectations. They are caused by either a leak within the operational framework – divulging information regarding the participants and actors in the EFGS that are confidential –, an event leading to the unavailability of technical or organizational structure governing the EFGS or an access to such structures that render them ineffective. Misguided expectations may be raised due to different adoption rates of the national mobile contact tracing and warning application, resulting in the expectation that the public approval of the sharing of the personal data needs to be ubiquitous throughout the European Union. Such expectations may lead to disappointment if temporary exposure keys are not shared in equal measure.

In the first class of risks, the leaking, tampering with or the destruction of documents and information, i.e. contracts, security tokens such as certificates or the intrusion into communication structures may reveal information regarding the operation of the EFGS that is not public information. Since the EFGS is operated transparently from an organizational and technical point of view, these type of risks concern themselves with economic structures and personal data of the natural persons performing functions within the EFGS.

The second class of risks concerns logging, monitoring and assessment functions that are required to assess the proper functioning of the EFGS. If these risks eventuate, their resolution may require a temporary suspension of the operation of the EFGS.

The third class of risks finally covers the tampering with the logging, monitoring and assessment functions of the EFGS. Since the data generated in these functions could no longer be trusted, the operation of the EFGS would have to be suspended until the required control and trust can be re-established.

All these classes of risk are subject to mitigation by the existing reliable security and governance functions. The EFGS project is subject to the requirements of Commission Decision (EU, Euratom) 2017/46, Commission Decision (EU, Euratom) 2015/444 and Commission Decision (EU, Euratom) 2015/443 establishing an organizational security framework. These risks are therefore considered to be mitigated.

Misguided expectations may be countered by effective awareness raising public relations efforts in order to explain the processes and benefits of the cross-border contact tracing effort.

18. Next Review

This DPIA needs to be reviewed and updated in regular intervals. In order to provide a reasonable, fair and appropriate assessment of the impact of the processing as well as in order to fulfil the warning function of this assessment, it is recommended to reassess the impact every three months.

This regular review does not preclude the necessity to reassess and update the impact of the processing in case of material changes and modifications to any part of the processing.

19. Accessory Documents

Annex 1: Risk Matrix

Annex 2: Design Decisions

20. Appendix

20.1. Glossary

The following glossary contains essential terms for the European Federation Gateway Service (EFGS) data privacy concept.

All legal terms used in the document are written in italics while keeping as much of the original wording of the GDPR as possible and are quoted using scientific citation.

The types of the terms used are defined as follows:

§ Term with a legal meaning or a legal reference

O Term describing organizational aspects

T Term describing technical aspects

→ Reference to the glossary

Term	Type	Description	Refers to
Anonymous data	§	Anonymous data refers to *"information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."* (Recital 26 sentence 4 GDPR)	
Application user	§	*"Person in possession of a smart device who has downloaded and runs an approved contact tracing and warning mobile application"* (Implementing Decision (EU) 2019/1765, Article 1 (1) (g)	
Back-end	T	The back-end is the part of an IT sysem that deals with data processing in the background.	
Bluetooth	T	Bluetooth is a communication standard. It enables the transfer of data from stationary and mobile devices over a short distance.	→ Mobile device
Bluetooth Low Energy (BLE)	T	Bluetooth Low Energy is a communication technique used by mobile devices up to ten meters apart to communicate with each other via Bluetooth.	→ Mobile device → Bluetooth

			→ Rolling proximity identifier
CDN	T	The CDN (Content Delivery Network) provides the diagnosis keys. The mobile devices can download the keys from the CDN at any time. This causes the mobile device to check if there was a contact with an infected user. Furthermore, it provides the evaluation settings together with the diagnosis keys.	→ Diagnosis key → Mobile device
Charter	§	Charter of Fundamental Rights of the European Union.	
Consent	§	*"'Consent' of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."* (Article 4 No. 11 GDPR).	
Contacts	o	Contacts or contact persons are people with whom the user has been close to, potentially resulting in a coronavirus transmission.	→ User → Corona
Contact tracing	§	*"Measures implemented in order to trace persons who have been exposed to a source of a serious cross-border threat to health within the meaning of Article 3(c) of Decision No 1082/2013/EU of the European Parliament and of the Council"* (Implementing Decision (EU) 2020/1023, Article 1 (1) (h)	
Controller	§	*"'Controller' means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law" (Article 4 No. 7 GDPR)*	
Corona	O	Denomination for various terms that are related to the coronavirus or the COVID-19 disease derived from it (e.g., Corona pandemic, Corona tests, Corona-Warn-App). The term Corona will be used in the documents.	

Corona-App	O	National contact tracing and warning mobile application, operated by the participating member states of the EU to reduce spread of the corona virus.	
Corona-Warning-System	O	National Risk notification system	
Countries of interest	§	*"The member State, or member states, where an application user has been in the 14 days prior to the date of upload of the keys and where he has downloaded the approved national contact tracing and warning mobile application and/or has travelled"* (Implementing Decision (EU) 2020/1023, Article 1 (1) (m)	
Country of origin of the keys	§	*"The member state where the back-end server that uploaded the keys to the federation gateway is located"*(Implementing Decision (EU) 2020/1023, Article 1 (1) (n)	
Cross-Border eHealth Information Services	§	*"Existing services that are processed via National Contact Points for eHealth and through a core service platform developed by the Commission for the purpose of cross-border healthcare"* (Implementing Decision (EU) 2019/1765, Article 2 (1) (c)	
Cross-border transmission chains		It refers to the ability of public health authorities to communicate to (as well as receive from) public health authorities in other member states the relevant keys so that other member states can perform exposure risk calculation and exposure alert.	→ Exposure risk calculation → Exposure alert
Diagnosis key	T	The randomly generated device key (random code) of an infected user after verification of their test results	→ Random code → Infected user
Diagnosis key package	T	A diagnosis key package is a collection of diagnosis keys from various infected users that are sent from the CDN to the mobile devices.	→ Diagnosis key → User → CDN → Mobile device
EFGS	O	European Federation Gateway Service	
eHealth Digital Service Infrastructure for	§	*"Infrastructure that enables the provision of Cross-Border eHealth Information Services via national contact points for eHealth and the European core service platform. This*	

Cross-Border eHealth Information Services		*infrastructure includes both generic services, as defined in Article 2(2)(e) of Regulation (EU) No 283/2014, developed by the Member States and a core service platform, as defined in Article 2(2)(d) therein, developed by the Commission"* (Implementing Decision (EU) 2019/1765, Article 2 (1) (d)	
eHealth network	§	*"Voluntary network connecting national authorities responsible for eHealth designated by the Member States and pursuing the objectives laid down in Article 14 of Directive 2011/24/EU"* (Implementing Decision (EU) 2019/1765, Article 2 (1)(a)	
Encounter	O	Encounter of at least two mobile devices which leads to an exchange and storage of short-term, randomly generated Bluetooth IDs (random codes)	→ Random codes → Mobile device
EU-DPR	§	Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC	EU-DPR
Exposure notification API	T	The API used to communicate with the Exposure Notification Framework.	→ Exposure Notification Framework
Exposure Notification Framework	T	The Exposure Notification Framework is part of the operating system or a background process of the mobile devices from Apple and Google. These components are new and are only available if the operating system of the mobile device is up to date. The framework is responsible for most of the generation of keys and their exchange.	→ Operating system → Mobile device
Federation gateway	§	*"Network gateway operated by the Commission through a secure IT tool that receives, stores, and provides a minimum set of personal data between member states' back-end servers for the purpose of ensuring the interoperability of national contact tracing and warning mobile applications"* (Implementing Decision (EU) 2020/1023, Article 1 (1) (j)	
GDPR	§	*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*	GDPR

		data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)	
Governance model	§	*"Set of rules concerning the designation of bodies participating in decision-making processes concerning the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services or other shared European eHealth Services developed in the framework of the eHealth Network, as well as description of those processes."* (Implementing Decision (EU) 2019/1765, Article 2 (1) (f)	
Health authority	O	The health authority/institution is a state or municipal authority under state law and part of the health service. As part of the obligation to report corona infection, the health department usually receives personal information from the management of the laboratory regarding the infected users.	→ Corona → Personal data → User
Infected user	O	A user who has been diagnosed as infected with corona. The data protection concept uses the term "infected user" for readability. The shortening consists in uncertainties in the serological diagnostic procedure.	→ User → Corona
Infection confirmation		The ability of a user to confirm a positive infection diagnosis in the CWA app, irrespective of the member state where the user tested positive. This in order to communicate the relevant keys to the public health authorities.	→ Corona App
iOS	T	iOS is an operating system as well as a software platform developed by Apple. It only runs on devices from Apple.	→ Operating system
Joint Controller	T	two or more controllers jointly determine the purposes and means of processing, Article 7a s.4 Implementing Decision (EU) 2020/1023	
Key	§	*"Unique ephemeral identifier related to an application user reporting to have been infected with SARS-CoV-2, or who may have been exposed to SARS-CoV-2"* (Implementing Decision (EU) 2020/1023, Article 1 (1) (k)	
Log data	§	*"Automatic record of an activity in relation to the exchange of, and access to, data processed through the federation gateway, that show in particular the type of*	→ Federation Gateway

		processing activity, the date and time of the processing activity, and the identifier of the person processing the data." (Implementing Decision (EU) 2020/1023, Article 1 (1) (o)	
Mobile device	T	Mobile devices are cellular gadgets that are equipped either with the Android operating system or the iOS system provided by the manufacturer Apple.	→ Operating system → Android → Ios
National Contact Points for eHealth	§	*"Organizational and technical gateways for the provision of Cross-Border eHealth Information Services under the responsibility of the Member States"* (Implementing Decision (EU) 2019/1765, Article 2 (1) (b)	
National contact tracing and warning mobile application	§	*"Software application approved at national level running on smart devices, in particular smartphones, designed usually for wide-ranging and targeted interaction with web resources, which processes proximity data and other contextual information collected by many sensors found in the smart devices for the purpose of tracing contacts with persons infected with COVID-19 and alerting persons who may have been exposed to COVID-19. These mobile applications are able to detect the presence of other devices using Bluetooth and exchange information with back-end servers by using the internet"* (Implementing Decision (EU) 2020/1023, Article 1 (1) (i)	
Operating System (OS)	T	The OS provides the basic functions for programs on mobile devices. Apple (iOS) and Google (Android) added additional functions for the risk evaluation which are used within the CWA app.	→ Mobile device → iOS → Android → Corona App
Other shared European eHealth Services	§	*"Digital services that may be developed in the framework of the eHealth Network and shared between member states"*(Implementing Decision (EU) 2019/1765, Article 2 (1) (e)	
Personal data	§	*"'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as 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" (Article 4 No. 1 GDPR).	
Processing	§	*"'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"* (Article 4 No. 2 GDPR)	
Processor	§	*"Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."* (Article 4 No. 8 GDPR)	
Pseudonymization	§	*"'Pseudonymization' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"* (Article 4 No. 5 GDPR)	
Pseudonymized processing	T	Personal data processing in a pseudonymized manner	
Purpose	§	This term is colloquially used in this document to define the motivation for a target-oriented activity or behavior. In Article 5 (1) GDPR, the processing of personal data is closely related to the processing purpose. They are to be understood according to the principles of appropriation and storage restriction (among others). They must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*" (Article 5 (1) (e) GDPR)	
Random code	T	The CWA uses two types of random codes: a randomly-generated device key (daily key) that is newly generated on a daily basis, or a short-term random Bluetooth ID (rolling proximity identifier) that is cryptographically derived from the	→ Corona App → Rolling proximity identifier

		randomly-generated device key multiple times per hour and exchanged between adjacent mobile devices.	→ Mobile device
Report type	T	information about with which verification procedure the corona infection of this user was attested, set by the national back-end.	→ user → Back-end
Risk determination	T	Continuous sending and receiving of short-term random Bluetooth IDs (random codes) that are stored in the encounter records. The stored data subsequentially undergoes an exposure verification.	→ Random codes → Encounter
Rolling proximity identifier	T	Term employed by Apple Inc. for "rolling proximity identifier"	→ Rolling proximity identifier
Rolling proximity identifier	T	The rolling proximity identifiers are calculated in the Exposure Notification Framework based on the daily keys. They are exchanged as sending and receiving keys between mobile devices through the Bluetooth Low Energy interface.	→ Exposure Notification Framework → Mobile device → Bluetooth Low Energy
Special categories of personal data	§	*"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."* (Article 9 (1) GDPR)	→ Personal data
Temporary Exposure Key	T	The Temporary Exposure Key is generated on a daily basis by the mobile device in the Exposure Notification Framework. The keys serve as the initial value for the creation of the Rolling proximity identifiers. In later steps of the process, they help in the calculation of an individual exposure risk in case the owner gets infected and decides to warn others by means of their daily key. By doing so, the daily keys become diagnosis keys.	→ Exposure Notification Framework → Mobile Device → Rolling proximity identifier → Diagnosis key
Third party	§	*",Third party' means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and person who, under the direct authority of the controller or processor, are authorized to process personal data."* (Article 4 No. 10 GDPR).	

TFEU	§	*Treaty on the Functioning of the European Union as published in the Official Journal C 326 , 26/10/2012 P. 0001 - 0390*	TFEU
Transmission risk	T	The day-specific risk that an infected user with a diagnostic key shares with another user and that is included in the calculation of the risk score	→ Infected user → Diagnosis key → User
User	T	A person who has installed the CWA app on their mobile device and who has activated its functionalities.	→ Corona App → Mobile device
User consent	T	In this document, the "user consent" data structure is used within the meaning of data protection. Please refer to the definition of "consent" included in this document for more information.	→ Consent → User
Verification of infection	§	*"Method applied for confirming an infection with COVID-19, namely whether this was self-reported by the application user or resulted from confirmation from a national health authority or a laboratory test"* (Implementing Decision (EU) 2020/1023, Article 1 (1) (l)	

20.2. List of abbreviations

Term/Abbreviation	Description
API	Application Programming Interface
CWA	Corona-Warn-App
DB	Data Base
DFC	Data Field Catalogue
DPIA	Data Protection Impact Assessment
EDPB	European Data Protection Board
EFGS	European Federation Gateway Service
EN	Exposure Notification API
ENF	Exposure Notification framework
EU	European Union
GDPR	General Data Protection Regulation
TSI	T-Systems International GmbH