DATA PROTECTION IMPACT ASSESSMENT

Data processing system:

Application "Stop COVID-19"

Controller:

Ministry of Health, Ksaver 200a, 10000 Zagreb

Contact:

zastita.podataka@miz.hr

Zagreb, November 3, 2020.

Version 2.0

Since the SARS-CoV-2 virus began to spread across Europe and the world in early 2020, public and political debates have increasingly focused on a technological solution to the burning problem.

Can the COVID-19 pandemic be contained using an app on a smartphone?

Such a system would automatically record the user's interpersonal contacts and thus be able, in a timely manner and anonymously, to inform those who were in epidemiologically relevant contact with a COVID-19 patient confirmed by the laboratory finding. Then exposed individuals could be effectively informed about the treatment of a potential early stage of infection.

In order to slow the spread of disease COVID-19 among the population in the Republic of Croatia, the Government of the Republic of Croatia and the Ministry of Health have developed an application "Stop COVID19" that informs users that they have been in contact with the person who was subsequently confirmed to be infected with disease COVID-19.

The app is based on a service jointly developed by Google and Apple and uses Bluetooth technology to exchange random anonymous keys between users' smart devices that are in an epidemiologically relevant close contact. These encrypted keys are changed several times during each hour, further guaranteeing the protection of users' privacy.

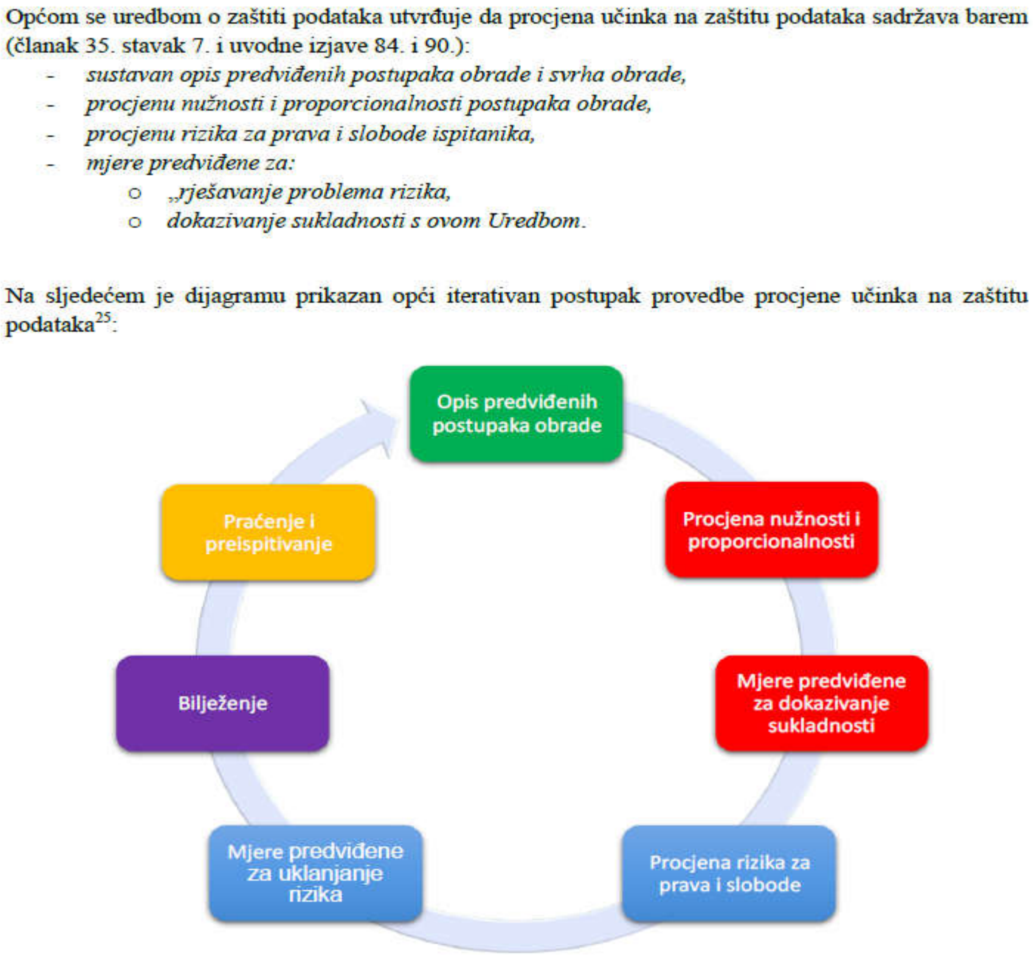
If one of the users subsequently receives a positive laboratory test for COVID-19, he may decide to share this information via the application using a one-time verification code.

In this way the application determines whether the user has been in contact with a COVID-19 positive person and, if so, specifies the date of the contact made and recommends the next steps.

Downloading the app is voluntary, and the users can turn it off whenever they want. The installation and use of the application does not require user registration, nor does any personal data be requested or recorded, nor does the user's geolocation data be collected at any time.

Looking at the planned systems to prevent the spread of COVID-19 across Europe, these are extensive social experiments involving the digital recording of the behavior of individuals under state control. The effectiveness and implications of such applications cannot yet be predicted, and it can be assumed that various versions will be imported and evaluated.

The consequences for data protection, and therefore fundamental rights, will potentially affect individuals, but also society as a whole. For this reason, we consider it relevant to carry out a data protection impact assessment.



Općom se uredbom o zaštiti podataka utvrđuje da procjena učinka na zaštitu podataka sadržava barem (članak 35. stavak 7. i uvodne izjave 84. i 90.):

- *sustavan opis predviđenih postupaka obrade i svrha obrade,*
- *procjenu nužnosti i proporcionalnosti postupaka obrade,*
- *procjenu rizika za prava i slobode ispitanika,*
- *mjere predviđene za:*
    - ○ *„rješavanje problema rizika,*
    - ○ *dokazivanje sukladnosti s ovom Uredbom.*

Na sljedećem je dijagramu prikazan opći iterativan postupak provedbe procjene učinka na zaštitu podataka[25]:

Opis predviđenih postupaka obrade
Procjena nužnosti i proporcionalnosti
Mjere predviđene za dokazivanje sukladnosti
Procjena rizika za prava i slobode
Mjere predviđene za uklanjanje rizika
Bilježenje
Praćenje i preispitivanje

The General Data Protection Regulation establishes a data protection impact assessment has to contain at least (Article 35(7) and recitals 84 and 90):
_systematic description of the envisaged processing operations and their purpose
_assessment of the necessity and proportionality of processing operations,
_risk assessment for the rights and freedoms of the data subject,
_measures provided for:
_risk problem-solving,
_demonstrating compliance with this Regulation

The following diagram shows the general iterative process of carrying out a data protection impact assessment25:

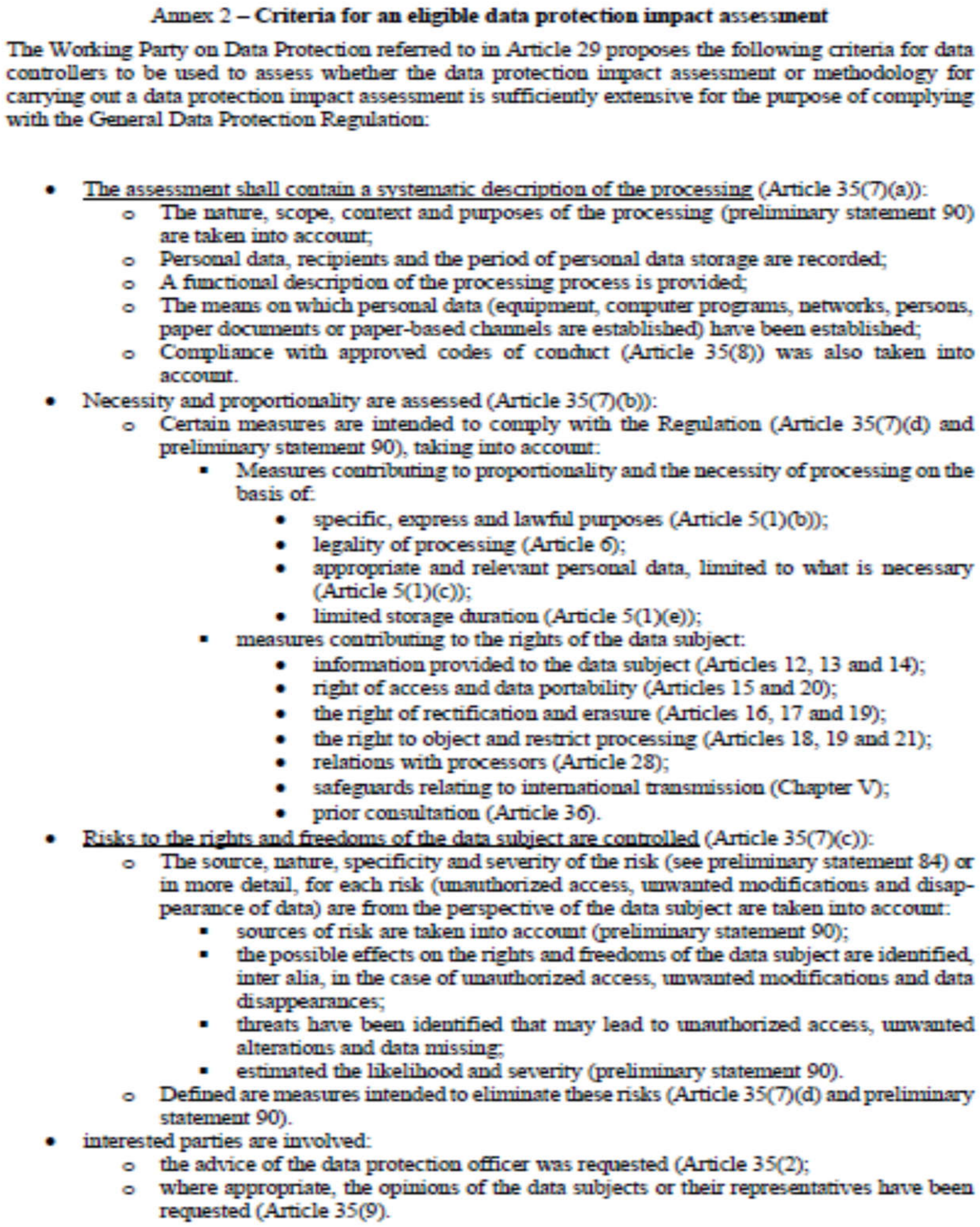
Description of the envisaged processing operations

Monitoring and review
Assessment of necessity and proportionality

Recording
Measures intended to demonstrate conformity

Measures intended to eliminate risks
Risk assessment for rights and freedoms

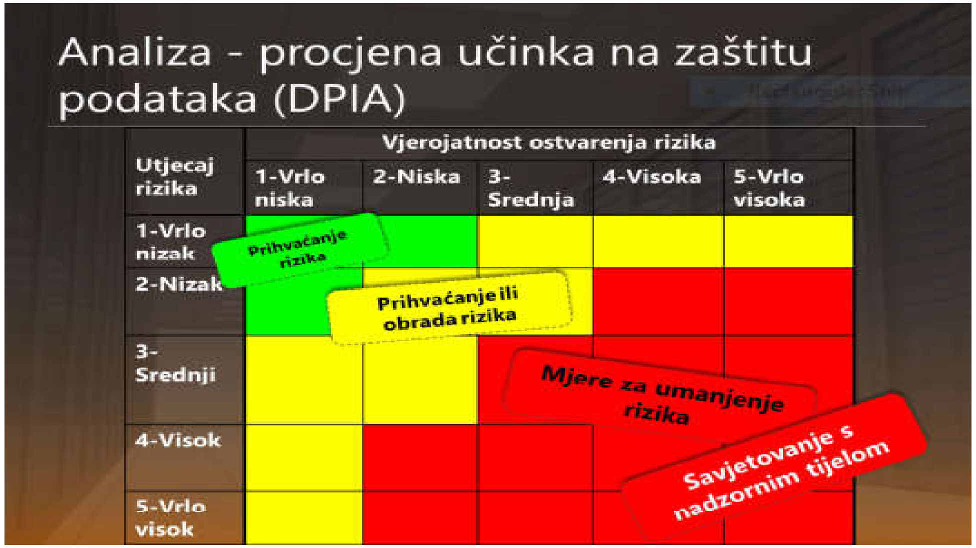
Source: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
Guidance on data protection impact assessment



Annex 2 – Criteria for an eligible data protection impact assessment

The Working Party on Data Protection referred to in Article 29 proposes the following criteria for data controllers to be used to assess whether the data protection impact assessment or methodology for carrying out a data protection impact assessment is sufficiently extensive for the purpose of complying with the General Data Protection Regulation:

- The assessment shall contain a systematic description of the processing (Article 35(7)(a)):
  - The nature, scope, context and purposes of the processing (preliminary statement 90) are taken into account;
  - Personal data, recipients and the period of personal data storage are recorded;
  - A functional description of the processing process is provided;
  - The means on which personal data (equipment, computer programs, networks, persons, paper documents or paper-based channels are established) have been established;
  - Compliance with approved codes of conduct (Article 35(8)) was also taken into account.
- Necessity and proportionality are assessed (Article 35(7)(b)):
  - Certain measures are intended to comply with the Regulation (Article 35(7)(d) and preliminary statement 90), taking into account:
    - Measures contributing to proportionality and the necessity of processing on the basis of:
      - specific, express and lawful purposes (Article 5(1)(b));
      - legality of processing (Article 6);
      - appropriate and relevant personal data, limited to what is necessary (Article 5(1)(c));
      - limited storage duration (Article 5(1)(e));
    - measures contributing to the rights of the data subject:
      - information provided to the data subject (Articles 12, 13 and 14);
      - right of access and data portability (Articles 15 and 20);
      - the right of rectification and erasure (Articles 16, 17 and 19);
      - the right to object and restrict processing (Articles 18, 19 and 21);
      - relations with processors (Article 28);
      - safeguards relating to international transmission (Chapter V);
      - prior consultation (Article 36).
- Risks to the rights and freedoms of the data subject are controlled (Article 35(7)(c)):
  - The source, nature, specificity and severity of the risk (see preliminary statement 84) or in more detail, for each risk (unauthorized access, unwanted modifications and disappearance of data) are from the perspective of the data subject are taken into account:
    - sources of risk are taken into account (preliminary statement 90);
    - the possible effects on the rights and freedoms of the data subject are identified, inter alia, in the case of unauthorized access, unwanted modifications and data disappearances;
    - threats have been identified that may lead to unauthorized access, unwanted alterations and data missing;
    - estimated the likelihood and severity (preliminary statement 90).
  - Defined are measures intended to eliminate these risks (Article 35(7)(d) and preliminary statement 90).
- interested parties are involved:
  - the advice of the data protection officer was requested (Article 35(2);
  - where appropriate, the opinions of the data subjects or their representatives have been requested (Article 35(9).



Analiza - procjena učinka na zaštitu podataka (DPIA)

Utjecaj rizika	Vjerojatnost ostvarenja rizika				
	1-Vrlo niska	2-Niska	3-Srednja	4-Visoka	5-Vrlo visoka
1-Vrlo nizak	🟩	🟩	🟨	🟨	🟨
2-Nizak	🟩	🟨	🟨	🟥	🟥
3-Srednji	🟨	🟨	🟥	🟥	🟥
4-Visok	🟨	🟥	🟥	🟥	🟥
5-Vrlo visok	🟨	🟥	🟥	🟥	🟥

Prihvaćanje rizika

Prihvaćanje ili obrada rizika

Mjere za umanjenje rizika

Savjetovanje s nadzornim tijelom

Analysis - Data Protection Impact Assessment (DPIA)

Risk influence	Probability of the risk realization				
	1 - Very low	2 - Low	3 - Middle	4 - High	5 - Very high
1 - Very low	Risk acception				
2 - Low		Risk acception or processing			
3 - Middle			Risk mitigation measures		
4 - High				Consultation with the supervisory authority	
5 - Very high					

	Instructions and questions for setting up a context for DPIA implementation	Reply/Description	Is it recognised in relation to the above description/response, which risk and if it is, describe it	Probability of the risk realization	Risk influence	Risk acception or processing	Risk mitigation measure
Information about the Controller	*Indicate who the Controller or Joint controller is*	Ministry of Health of the Republic of Croatia, Ksaver 200a, Zagreb	n/p	n/p	n/p	n/p	n/p
Data Protection Officer (DPO)	*Provide the address/contact of the data protection officer of the Controller*	zastita.podataka@miz.hr	n/p	n/p	n/p	n/p	n/p
Data on the Processor	*Specify who the Processor is*	APIS IT d.o.o., Paljetkova 18, 10001 Zagreb	n/p	n/p	n/p	n/p	n/p
Justification of the need to implement DPIA	*In general (high-level description, not detailed description) describe what will be achieved by the project and what functionality the application includes. Summarise the reason for conducting DPIA. Provide references to other relevant project documentation containing other details with a description of the project.*	The aim is to improve the health treatment of users who have been undoubtedly exposed to COVID-19, and to increase the public's sense of security in the pandemic era. The project involves the application of a completely new technology with a new way of processing data, and the purpose is to achieve improved health processing of users, which is the reason for establishing the context for the implementation of DPIA. The application includes the "proximity" key exchange functionality (which are anonymous) that give the possibility, if confirmed to be infected, for the user to send their infected keys to the server so that the server can inform other users of the application of potential exposure in the Republic of Croatia but also users in other European countries which exchange anonymous keys through the European Federated Gateway service	n/p	n/p	n/p	n/p	n/p
	Is the application use mandatory?	Installing and using the app is entirely voluntary. Users decide independently whether to download the installation to their mobile device, how they will use it and when to remove the app from their mobile device. Users decide for themselves whether to enable the exchange of anonymous keys through the European Federated Gateway service.		2	3	Risk processing	Communication plans of the National Headquaters, the Ministry of Health and Croatian institute of Public Health on current epidemiological measures should also contain precise information on the use of the mobile application.
	Describe the nature of 'processing'; what data will be collected, how it will be used, stored and deleted. Whether the data will also be exchanged with other organisations and if so, specify them. What type of processing will occur and may be related to risks related to the protection of personal data/privacy?	Anonymous key information and date of contact with other devices are collected. It will be used to notify other users of the app about a potential contact with the infected person who sent their infected keys. The app only remembers the keys for the previous 14 days, while older keys are deleted. The keys of COVID-19 positive persons, who so choose themselves, will potentially be exchanged with the Ministry of Health of the Republic of Croatia and Croatian institute of Public Health and other countries that use the same method of exchange of keys. Information about anonymous keys will be exchanged through the European Federated Gateway Service only in the case when the user gives his consent after installing the application.	n/p	1	1	Risk acception	
	What types/types of data does the processing cover and does it include and the processing of specific categories of data (see Article 9 GDPR) or data of minors?	Anonymous keys for contacts and infected persons and the contact date of the two users. At this time, none of this is considered personal information because it is in no way possible to link anonymous keys to a person. The app can also be used by minors, but the system does not check or determine it (who they are, how old they are, etc.)	n/p	1	1	Risk acception	
	Describe the scope of the 'processing': the amount of data (estimates of the number of persons and or any other appropriate assessment), which geographical area covers (HR only or?) *How long the data will be used, describe the time dimension of the processing.*	For the app to be as efficient as it is, at least 60% of the population needs to install it. This is not necessarily the number of real people who will want to use the app, but is the recent experience of an expert. The geographical area covers the entire territory of Croatia, and once interoperability is established with other EU Member States using the same Google/Apple services, key exchanges with servers in those countries will also be achieved. The data will be used during a pandemic with the possibility of shutting down the application in case of a possible health system strain or because of the pandemic end	n/p	1	1	Risk acception	

	Instructions and questions for setting up a context for DPIA implementation	Reply/Description	Is it recognised in relation to the above description/response, which risk and if it is, describe it	Probability of the risk realization	Risk influence	Risk acception or processing	Risk mitigation measure
Description of the context and envisaged processing operations	*Describe the nature of the relationship between the person using the application (data subjects) and the controller (Ministry of Health?) What level of control does respondents who use the app have over their own data? Are there previous examples of such processing that should be taken care or flaws related to the security of such intended processing, is it the application of new technology or a completely new way of processing data?*	The Ministry of Health and APIS IT cannot find out who the users are because there is no list or register of application users. The only information that the user voluntarily enters into the application is the verification code, generated by the competent healthcare professional, to enable the transmission of exposure notices to the infection. The user does not enter any other information and may remove the app from the device at any time.	n/p	1	1	Risk acception	
	Is the protection of basic rights secured, since this application does not have the ability to intervene in the processing, i.e. the revocation of incorrect notices?	There is no practical possibility of intervention in data processing.	There is no way after someone has been notified that he has been in contact with someone, to delete that contact because it is "not correct". That is, there is no possibility of "recalling" incorrect notifications because it is not recorded somewhere with us on the base, but rather that the app and google services do it independently. It should be intervened probably in the user's cell phone, which is more than impossible.	1	5	Risk acception	
	What is the current maturity of the technology to be used and is there a public concern that needs to be addressed?	The technology is in the early stages of testing, but there is no particular concern as the same methods are used or are planned to be used by most EU members and other countries that choose to rely on Google/Apple exposure notification services.	n/p	1	1	Risk acception	
	Will any (if any) approved code of conduct or certification related to this processing/application be used?	Yes, if mechanisms for the evaluation and accreditation of national applications at EU level are available. The Processor, APIS IT, is ISO 27001 certified.	n/p	1	1	Risk acception	
	Describe the purpose of the processing, what is to be achieved, what are the benefits of the processing for the Controller and beyond, what is the intended effect on the data subjects who will use the application?	The processing aims to notify users of the app who have been exposed to an infected key sent by the app user positive for the COVID-19 test. It is on the user's conscience whether they want to send their infected keys, but it is not mandatory! The benefit of this processing for the user is the mutual anonymous information of other users about the potential exposure to the infection. The effect for users is a sense of security while using an app that can contact them in case they have been exposed to the infection. The Controller has the benefit of pre-isolating users so as not to further spread the infection, which in the users themselves assumes responsibility and solidarity because they use the app on a voluntary basis, and all the keys are anonymous and randomly generated.	n/p	1	1	Risk acception	
	Indicate whether and when any additional consultations will be carried out with relevant participants and/or the public, if necessary. If not necessary, write down the justification.	The Department of Health will inform the public in due time about the voluntary, anonymity and safety of using the app.	n/p	1	2	Risk acception	
	Is there a need for consultation/engagement of information system security experts or some other technical experts?	The Ministry of Health has included the Croatian Information Systems Security Bureau in the final phase of the project and has carried out a vulnerability check on the services needed for the operation of the application, in order to protect against cyber threats. The eHealth Network security architecture used to exchange data between the national system and the European Federated Gateway service.	Croatian Information Systems Security Bureau conducted a vulnerability check of the API services required for the operation of the COVID-19 disease exposure notification application, which reported us on 26. 6. 2020., we quote the section: "The web service is essentially simple and has only a couple of API destinations (endpoint) and we have not been able to find any significant defects."	2	4	Risk processing	CERT ZSIS is ongoing for further checks and monitoring of cyber-threat capabilities and swift action.
	Are personal data, such as computer equipment, programs, and other resources, established?	Although the keys exchanged through the app on the mobile device do not fall into the personal data category, all means used to operate the application have been identified.	n/p	n/p	n/p	n/p	n/p

	Instructions and questions for setting up a context for DPIA implementation	Reply/Description	Is it recognised in relation to the above description/response, which risk and if it is, describe it	Probability of the risk realization	Risk influence	Risk acceptance or processing	Risk mitigation measure
Assessment of necessity and proportionality	*Describe the legal basis for processing (legality - what legal basis is used and assess whether a legal basis is properly determined) and the proportionality of processing operations with purpose and legal basis: is there a different way to achieve the same outcome?*	Keys exchanged via the application on the mobile device do not fall into the category of personal data. The application is downloaded by the user voluntarily, and when downloaded to the mobile device, he gives his consent for cross-border interoperability. The legal basis is the necessity to perform a task of public interest.	The legal basis for the processing of personal data are: - Art.6. st.1 (a) - for cross-border interoperability - Art.6. st.1 (e), - Art.9. st.2 (i) and (h) The prerequisites for this are that the processing of personal data falls within the legal conduct of the competent authority in accordance with Art.6 GDPR, the processing of personal data is necessary and in accordance with further provisions of the GDPR and legal regulations.	1	1	Risk acceptance	
	Do we have a specification/description proving that the processing is proportionate to the legal basis (adequate, relevant and limited only to the necessary purposes of processing, that we will not infringe the rights and freedoms of the application user?	The app is limited to the necessary information only and uses the Google/Apple service - a service that uses the mobile operating system (Android or iOS) locally for the app. The documentation is publicly available here, in the Methods section: https://static.googleusercontent.com/media/www.google.com/en//covid19/exposurenotifications/pdfs/Android-Exposure-Notification-API-documentation-v1.3.2.pdf Other descriptions that can be proven are part of the project documentation.	n/p	1	1	Risk acceptance	
Measures intended to demonstrate conformity	*How is it ensured that data is limited to what is necessary in relation to the purposes for which it is processed?*	By collecting only anonymous keys, the date of contact (to determine when the contact was and to be notified to the user who is infected). Other data is not collected!	n/p	1	1	Prihvaćanje rizika	
	How will it be proven that the data is kept only as long as is provided for by the legal basis/purpose of the processing?	By examining the anonymous key database from the processor. Also, by examining the publicly published description of the application's work and architecture.	n/p	1	1	Risk acceptance	
	How will it be proven that the data is used solely for lawful purposes and not by another? (logos, something else?)	Logos	n/p	1	1	Risk acceptance	
	How will it be ensured that any further processing of the data will not be used for other purposes before proper verification is this ok?	There is no other purpose, there are keys and dates that cannot be interpreted by the server independently, but the processing of the match of the contact with the infected key occurs exclusively on the user's cell phone.	n/p	1	1	Risk acceptance	
	How is it ensured that Processors are obliged to comply with and comply?	The Contractor's contractual obligation, implemented all necessary GDPR procedures, protocols and other legislation.	n/p	1	1	Risk acceptance	
	What processing information will be disclosed to the respondents and how will it be communicated to the respondents? (data subject's rights - GDPR)	Before installing an app or later in the app itself, the user has the option to read the Privacy Policy, Terms of Use, Accessibility Statement and program components used. All information will also be available through Koronavirus.hr - Official Government website for timely and accurate information on coronavirus	n/p	1	1	Risk acceptance	
Other issues with which risks can be identified (technical - IT, process and organizational, others)	*Is there a need for rules to ensure corrections and/or accuracy of personal data? I.e. is there a need for some "data quality" rules?*	None because the system does not store any personal data except automatically generated and anonymized key identifiers.	n/p	1	1	Risk acceptance	
	How do we ensure data security - confidentiality, integrity and availability? How do we know someone didn't change records, access them for no purpose and sent them around? How did we secure ourselves from destruction, accidental or deliberate?	Confidentiality, integrity and availability is ensured in accordance with application provider (Processor) database creation standards (backups, etc.). How do we know that someone didn't change records: Logs in the database, creating periodic replicas/dump bases, limiting the authority on the base production. Destruction insurance.	n/p	1	1	Risk acceptance	
	The monitoring system processes personal data concerning health status.	The process consists of processing anonimous "proximity" key on smartphones, transferring that data to the server after a diagnosis of infection, and eventually distributing it to all other smartphones to notify possible contacts with infected users. All data on your smartphone is personal data related to the device user.	Since only COVID-19 users have the option, if they so choose to, to transfer data (their keys for the last 14 days) to the server, the data transmitted constitutes data related to health status, and the processing of such data is subject to the GDPR.	1	1	Risk acceptance	

	Instructions and questions for setting up a context for DPIA implementation	Reply/Description	Is it recognised in relation to the above description/response, which risk and if it is, describe it	Probability of the risk realization	Risk influence	Risk acception or processing	Risk mitigation measure
	Is it possible to de-anonymise users and how is it provided?	De-anonymisation of the users is not possible by implementing legal, technical and organisational measures.	Reference to a natural person is effectively and irreversibly separate from the processed data by a multidimensional approach, so that the data obtained is anonymous. The application of legal, technical and organisational measures ensures the efficient and irreversible separation of data in practice resulting in non-identification data indicating disease exposure, which are stored on the server and distributed to other applications.	1	1	Risk acception	