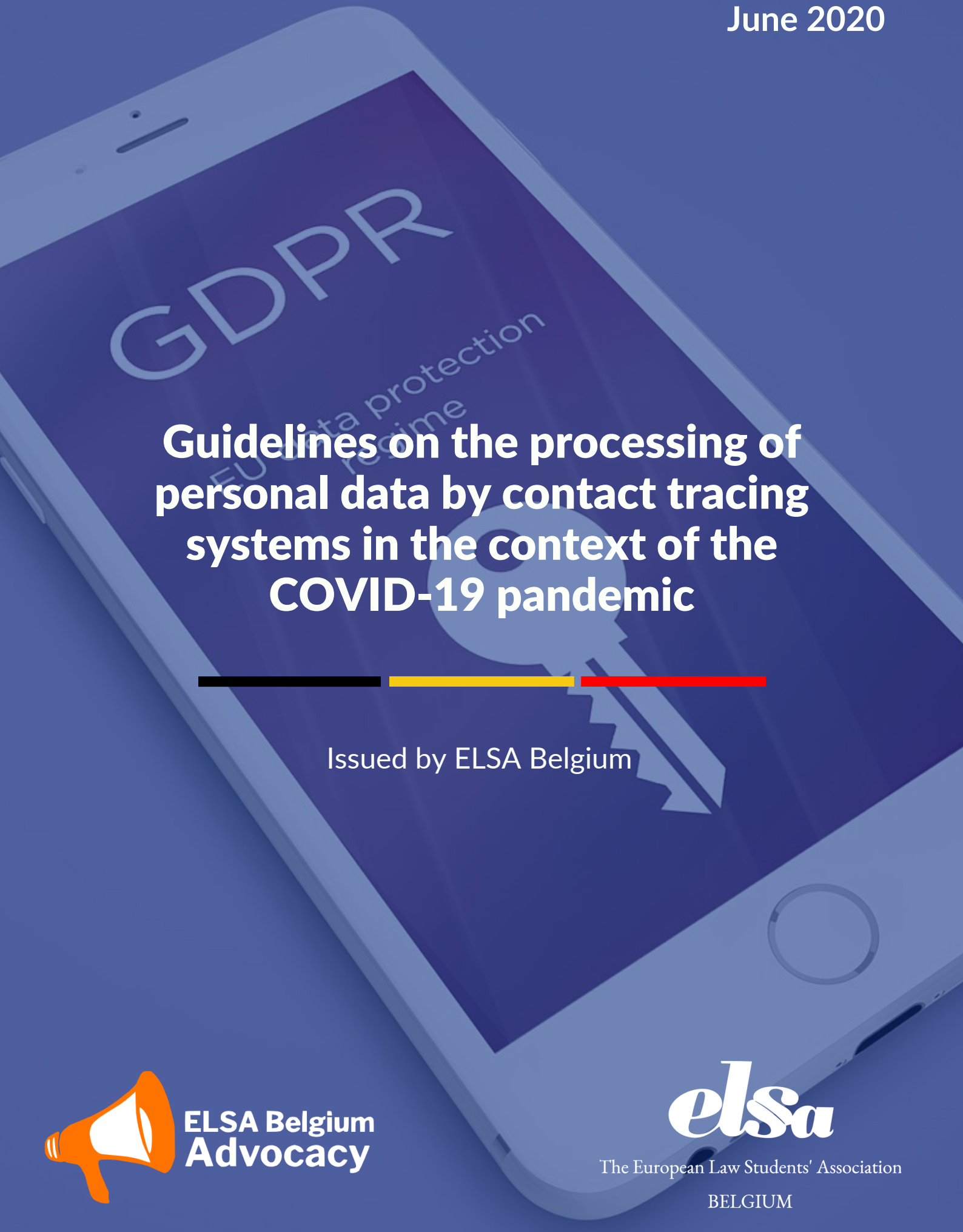
June 2020

Guidelines on the processing of personal data by contact tracing systems in the context of the COVID-19 pandemic

Issued by ELSA Belgium



ELSA Belgium Advocacy

The European Law Students' Association
BELGIUM

Guidelines on the processing of personal data by contact tracing systems in the context of the COVID-19 pandemic

Research Team: Viktor Francq, Lucas Pinelli, Maria Enescu, Tomislav Rachev and William-Alexandre Toublanc.

Managing Team: Apolline Baudoux, Brandon Cheliotis, Lucas Pinelli and Viktor Francq.

June 2020

TABLE OF CONTENT

DECLARATION OF INTENT

Due to the recent outbreak of COVID-19, Belgium, as many other States, entered a large lockdown. The evolution of the situation progressively allowed for a loosening thereof and the country is now slowly reopening itself. This return to a normal life comes with a series of challenges that States have to respond to. Amongst them is the control of the spread of the virus, which is linked to some form of control of the contacts within the population.

As an answer to those challenges, States are developing different contact-tracing systems. They consist of ways to inform people that they have been in contact with infected persons and, therefore, that they face a risk of contagion themselves. In Belgium, two kinds of systems have been discussed: tracing apps and call centers.

Understanding the gravity of the current situation and thankful for what the Belgian State is doing in order to improve the situation of the Belgian people, ELSA Belgium is willing to participate in this debate in order to help public authorities finding a good and tempered solution when it comes to those tracing systems. As the biggest law-students and young lawyers association in Belgium and part of the biggest law-students and young lawyers association in the world, we have construed an objective opinion on the matter, based on the position taken by different superior bodies[1]. Based on those researches, we have tried to build the best possible solution from a legal point of view.

The present Guidelines are the result of this whole process. We respectfully submit them to the different Belgian authorities in charge of organising the above-mentioned tracing systems with the views of contributing to the national effort of dealing with the crisis.

Aiming at acting as a third party specialised in such matters, ELSA Belgium is open to help with further contributions on the matter.

For those reasons, we would like to submit the following Guidelines on Tracing Systems to the Belgian Federal State, the Flemish Region, the Walloon Region and the Brussels-Capital Region.

Respectfully yours,

ELSA Belgium

Apolline Baudoux, Brandon Cheliotis, Yannick Fadeur, Lucas Pinelli, Viktor Francq, Aude Valizadeh, Eva Madessis and Gao Xing

On the basis of the contributions of Viktor Francq, Lucas Pinelli, Maria Enescu, Tomislav Rachev and William-Alexandre Toublanc.

[1] European Data Protection Board, European Data Protection Supervisor, European Commission, European Parliament, Council of Europe, Belgian Data Protection Authority

GUIDELINES

ELSA Belgium

Considering that Belgium has been suffering from the recent outbreak of coronavirus; that the Belgian has already or is currently organising tracing systems in order to allow for some control of the spread of the virus while progressively putting an end to the lockdown; that those measures are necessary in order to ensure the Public Good and the health of the population as a whole;

Considering that those tracing systems, as needed as they might be, present some risks for the rights and freedoms of the people in their quality of mass-processing of sensible data by a public authority; that, as such, they require a special attention and a very thorough assessment when being developed; that their creation undoubtedly wins to be the result of a common effort ;

Considering that many authorities have expressed their views on the matter; that those opinions have the legal authority required to be considered objective legal assessments;

Considering that ELSA Belgium is willing to advocate for its values of defence of human rights, contribution to legal education, encouraging social responsibility, human dignity and cultural diversity and to take part to the legal aspects of that debate; that it constitutes an apolitical third party that only bases its considerations on objective legal knowledge;

Considering that the implementation of contact-tracing systems by the Belgian State is taking two directions; that it firstly consists of a call centers system that is actually a default system in Belgium when it comes to dealing with epidemics, that it consists of organisms managed by the Regions (Flanders, Brussels-Capital and Wallonia) who can access a central database storing contact information of infected people (who are themselves collected directly by medical staff) to call them in order to ask for the list of their recent physical contacts, which are themselves called in order to inform them that they might be infected;

Considering that the second system is that of tracing apps; that such applications aim to be downloaded on smartphones, which issue temporary specific anonymised keys; that those keys are then constantly exchanged with other users of tracing apps who happen to be nearby and stored in the receiving phones so that, if declared infected, the person can turn their keys into a « sick » number in order for the app to inform all the people met that they might be infected;

Stressing out that the legal framework of the tracing systems shall reflect the reality thereof; that this is a matter of trust on which the efficiency of those systems rely in line with the prevalence of rule of law in our country; that such prevalence requires the final and complete legal instruments implementing the legal systems to be mandatorily submitted to the DPA for approval; that those principles are constitute fundamental basis of our democracy;

Having studied and debated the different positions taken on the matter;

Has issued the following guidelines.

I. As to the use of tracing systems

The first question to address is whether any of those processings – tracing apps and call centers system – are actually permitted and suitable, which is the case only if they are considered necessary and proportionate with regard to their objective with respect to Article 5.1 c) of the General Data Protection Regulation.

Those objectives, which are further detailed below, mainly consist of controlling the spread of the virus within the population by informing people who have been in contact with infected persons. They also aim at conducting research about the virus presently and in the future. Both processings must, therefore, be the least intrusive and the most efficient in order to reach those purposes.

It is clear that tracing apps, as proposed in the projects of Royal Decrees that were submitted in Belgium, could be considered as the most efficient solution if they were used by the whole population. It would allow for complete information for all the people and for a full overview of the spreading characteristics of COVID-19 on the whole Belgian population. However, this consists of a rather intrusive procedure, since it requires a non-stop real-time tracing of those who would use the apps. Furthermore, it can only reach its full efficiency if adopted by a sufficient rate of the people. Otherwise, it misses its point, since it is considered that they only reach full efficiency if they are used by around 60% of the population.

Call centers, on the other hand, might consist of a broader processing when it comes to their scope (see below). However, it is completely impossible for them to process the contact data without some form of collaboration of the data subject, as a result of their manual and non real-time nature. They might be considered the most protective system from a comparative perspective, as well as the best established. However, their efficiency is at first stance way below that of the app as they present a certain number of imprecisions (linked to human failure or absence of constant follow-up such as the one that is offered by the apps).

Our assessment of both systems consequently leads to the conclusion that they offer different qualities, one bringing more efficiency and the other one being less intrusive. However, none of them seems sufficient in order to fulfill the above-mentioned purposes while offering a minimalistic processing.

Therefore, in order to fulfill the objectives sought while offering complete compliance with the principles of the GDPR, we plead for the parallel use of both systems in a fully-integrated coherent strategy. Such an organisation would be based on the free use of applications by individuals (*see basis of the processing down below*) as a substitute for manual contact tracing. If activated early enough before any declaration of infection (e.g.: two weeks, which is the estimated longest incubation period of the virus), they offer a very high level of efficiency and accuracy which would make it unnecessary to exercise a human-based follow-up by Regional call centers. After the cure, they also ensure correct control of the further evolution of the patients' contacts during the time where they might still be contagious.

In order for call centers to offer a similar level of efficiency, they shall permit a further follow-up of the person during the time where they would still be infectious. This means that the person shall be called many times and would be asked to share all the contacts that they have had more than once, which is obviously a very heavy processing.

Therefore, we believe that tracing apps should be encouraged as much as we can while letting people have full freedom of choice. It is therefore needed to let them have a second option if they do not want to make use of the apps. This is where call centers take place, with the condition to exercise a further follow-up until a defined period, while app users would not have to submit to such a procedure as long as they downloaded the app long enough before they are declared infected in order for that tracing system to be efficient (around 2 weeks). This use of apps might also be encouraged by positive incentives, which can in no possible way disadvantage people who decided to submit themselves to a processing handled by the call centers. This can be the case of the distribution of tokens offering reductions in restaurants or shops (which can also be considered as a positive consumption incentive in order to help the economy). Such an organisation is likely to constitute a fully integrated system with optimal efficiency.

Finally, in order to promote the use of apps amongst weaker parts of the population, there shall be created an obligation for medical staff to present the use thereof to infected people to let them choose which system suits them best.

II. As to the framework of each tracing system

1) Basis of the processing

Contact tracing is a needed step in order to fight COVID-19 in an efficient way by controlling its spread and learning from it. Therefore, it can be considered a public interest to develop systems aiming at reaching those purposes. Such public interest constitutes a valid basis of processing with respect to Article 6.1 e) of the GDPR.

However, in order to be coherent with the full framework that we have presented above, both systems cannot be put into places mandatorily. This was stressed by nearly all institutions that issued an opinion about tracing apps. Therefore, in line with what they have advised, we consider that any data processing made by tracing apps must be based on consent as understood under Article 6.1 a) of the GDPR. Only manual contact tracings of data subjects who have not downloaded the app a sufficient time before the infected diagnosis is issued shall be based on public interest and, therefore, be made mandatory.

Such a public interest, however, only applies to the processing of data needed in order to control the spread of the virus and to issue statistics about it (see hereunder). If any further processing of non-anonymised data is made for research purposes, it shall be based on consent as well. This would be the case for name databases used in order to contact people consenting to take part in experiences on the virus.

2) Purposes of the processing

The previous points have already briefly discussed the matter of the purposes of tracing processings. It is now time to define them clearly and restrictively.

The general objectives of contract tracing systems are 1) controlling the spread of the virus and 2) gathering data needed in order to conduct research about COVID-19.

The first objective can be reached differently by each processing method.

- When it comes to the apps, this purpose is fulfilled by confirming contaminations in the app, keeping an anonymised history of contacts that the infected had with other people (*see below*) and informing the people met that they were in contact with an infected person. No other concrete action is needed in order to reach the set goal.
- As to call centers, such purpose is made possible by asking the medical staff to enter a series of information about their patients into a database, which is then used by the Regions in order to contact the infected. They are then asked the contact details of the people they remember to have met recently, who are themselves contacted in order to inform them of their situation.

When it comes to the second objective – namely, allowing for scientific research –, it is fulfilled either by anonymising the collected data in order to use it as a statistical and research object or by using individual cases that might be called upon in order to further investigate their specific case. However, this second option is only possible for initially non-anonymised data (*which shall not be the case of applications, see below*). It can, therefore, only be applied to processings based on call centers.

It is extremely important to underline that such research purpose is only fulfilled if the data is widely shared with a large number of laboratories and scientists. Otherwise, it does not seem possible to consider that such processing is truly aiming at ensuring a Public Interest, which is the larger basis of the whole tracing system. This means that all statistical data shall be shared with the different research bodies, including data processed by the app on the basis of consent. Indeed, considering that the consensual processing of data by applications is itself a substitute to the processing conducted by callcenters on the basis of a Public Interest, the creation of a monopolistic concentration of app-collected research data would constitute a violation of data protection regulations at force by the whole system, as well as a potential breach of competition law. Such consequences would also harm the general principles of fairness and responsibility that scientific research relies on.

From our perspective, no other objectives justify further processing. Therefore, the principle of minimisation requires the scope thereof to be based solely on those two purposes.

3) Scope of the processing

Regarding the scope of the contact tracing apps, we believe that only **anonymised temporary keys** (under the aspect of numbers) shall be generated and processed. We are aware that no anonymisation technique is fully reliable at the moment, but anonymisation grants the highest level of protection and drastically reduces the risk of re-identification. Also, these keys should be temporary and thus regularly renewed, for compensating for the shortcomings of the anonymization technique used, increasing the level of protection.

Of course, in order for the app to be efficient and to attain its goal, the **status of being infected** shall be processed, with the appropriate safeguards for the privacy of the infected person in order to avoid re-identification. These safeguards should be strong enough, as the status of being infected can be regarded as "health-related personal data", falling under the scope of Article 9 of the GDPR as being a special category of personal data. If the app provides for the functionality of the person adding the symptoms themselves, that person might only be considered as "potentially infected". Also, the processing of symptoms-related data shall have the same

regime. The certified update of the status to "infected" shall only be performed by or under the supervision of health authorities.

Furthermore, **proximity data** are necessary for attaining the purpose of fighting against the COVID-19 pandemic. They consist of the proximity history (approximate area) and time period (morning, afternoon,…) of contact between two devices that use the app. No location or mobility data shall be processed. Also, no unnecessary data such as the civil status, communication identifiers, equipment directory items, messages, call logs, location data, device identifiers will be collected. This way, the principle of data minimization will be observed.

Concerning the manual contact tracing, performed via call centers in Belgium, it is worth mentioning that it involves a higher degree of personal data processing, for both the infected person and for the people this person came in contact with. Indeed, for the infected subject, data such as their **name, gender, phone number, address and profession** shall be processed. The name, phone number and address shall be processed for the purpose of reaching them. Data such as their gender and profession shall be collected only for research and statistical purposes, after being anonymised and aggregated. In addition to this, inevitably, their **status of being infected** and the **evolution of the person's condition** will be processed. Data regarding the **collectivity** the person is part of might also be relevant, in order to identify the competent call center. Furthermore, data about the people the infected came in contact with will also be processed, in the form of their **names, phone numbers and address**, with the purpose of reaching them and informing them about being in contact with an officially infected person and indicating the procedure to follow.

4) General remarks about the processing

First of all, in order to ensure the efficiency of the app, the population shall be encouraged to use of **labeled apps (see section 7)**, despite the fact that there might be developed various private apps. The apps, in order to be efficient, have to be used by at least 60-70% of the population. In order to attain this threshold, the use of private apps that are not interconnected with the official ones shall be discouraged. The use of a non-labeled app will not only decrease the efficiency of the official one, but will also pose certain increased risks for the users, such as feeble data security, data breaches, data misuse or abuse by unauthorised parties.

Secondly, we recommend that **app developers shall make the app's source code public** at least a week before the app is made accessible to the public, in order to allow for the study thereof. Two possibilities stem from this idea. On the one hand, the source code could be published so that every citizen would be able to review it if they wish to do so. This would increase the level of transparency in relation to the population. However, it can unfortunately ignite studies performed by non-specialists and the dissemination of fake news to the population. On the other hand, the source code can be made accessible only to the state. In this case, the citizens might argue that the measure is not fully transparent and that the state has full discretionary power in reviewing it. Nonetheless, this will counter the aforementioned drawback regarding the dissemination of fake news about the source code. However, we consider the publishing of the source code necessary with regard to the needs for transparency in the matter.

Thirdly, among the other principles enshrined in the GDPR (such as data minimization and storage limitation, data security, lawfulness of the processing etc.), we consider that particular attention shall be devoted to the principle of **transparency**. The measure shall be fully transparent and the citizens shall be clearly explained to: what data is being collected through the

app, what purposes will this data be used for, the data storage time and conditions, the liability and accountability of the controller and the processor, who the processors are, who the processors are or will be, a free access to the Data Protection Impact Analysis, etc. By ensuring a very high level of transparency, people will be encouraged and motivated to embrace and use the app, which will increase its overall efficiency and the spread of the virus should be diminished. Transparency is of paramount importance in the current circumstances. People are reluctant and fearful as this extraordinary situation is unprecedented, so they do not have a previous example on how to react and how to approach the situation. Additionally, people are becoming more and more aware of the fact that they have more rights than ever before. However, not all of them are fully aware of what exactly these rights are and how to exercise them. Therefore, transparency is vital in order to address these concerns.

5) Duration

As to the duration of the processing, it shall be determined with consideration for the set purposes. All information shall be kept as long as needed to reach those and no longer than that. It is also worth highlighting that this only has regards to data allowing for identification as anonymised data can be kept as long as wished.

Therefore, all data shall be kept as long as needed in order to control the spread of the pandemic. From an individual point of view, this means until the end of the infectious period, which is not precisely known but whose duration is at least two weeks long after the cure. This shall, then, be considered the normal length of all processings, including the infectious status recorded on the app. Indeed, although many institutions advised the infected status to be deleted immediately from the app, it seems like it is actually not sufficient in order to reach the purpose since the person is still likely to be in contact with other people, who shall be informed thereof.

However, considerations for discrimination prevention order to foresee some time period between the time an infected person is in contact with other people and the moment the latter are notified so. A reasonable period would be a day.
The only exception to this duration shall be non-anonymised data processed for research purposes, given that the person consented thereto. In that case, the processing shall last as long as the person did not withdraw their consent or at least until the end of the pandemic (*see deletion*).

6) Security of the data

As far as data security is concerned, all relevant aspects must be taken into account - data storage, protection against unauthorized access and data corruption as well as the mandatory securisation of the transmission. Before looking into the relevant measures to be taken, it is important to consider what model of automatic tracing is put into place.

So far two approaches have established themselves - a centralized and decentralized one. While we acknowledge the fact that many countries have opted for a decentralized system in which contact-matching takes place locally on devices, we recommend a centralized system, locating the contact matching on a centrally controlled computer server, which we consider better suited to fulfill its purpose, namely tracing and interrupting the infection chain. The difference is that in such a system, not only the anonymised identifiers of diagnosed people are sent to the central

database, but also their proximity history, thus enabling the national agency to track the infection rate, as well as the number of potentially infected people, exposed to the virus. It shall be noted that identification of the potentially infected people would be impossible as the proximity history only comprises the anonymised keys of the people with whom contact has been registered.

However, such a centralised system implies additional privacy risks, as more data is being transmitted between the device and the central server. Assuming that these risks can be minimised through the application of state-of-the-art cryptographic techniques, we believe that the benefits of the centralised approach outweigh the drawbacks.

To ensure sufficient data security, all app providers must implement the necessary measures to securely store the processed data on the device and protect it from unauthorised access. Its transmission between the devices and the central server must be subject to end-to-end encryption.

As to the central server, it is crucial that European law is applicable to its operation. Therefore it must be located within the borders of the EEA. A list of those who access the data on the server must be logged and kept for 10 years in order to allow for the exercise of possible criminal or civil actions.

Full transparency must be ensured about the use of the data and its concentration within the databases, therefore the code of the apps must be open-source and available to anyone that wants to contribute to its quality or test its security.

With regard to manual tracing, both Sciensano, federal Public Health authority, and the call-center authorities shall be considered as controllers in order to face the duties of the controller under GDPR, which include, amongst other things, concluding confidentiality agreements with their agents and supervising them as well as conducting a specific DPIA.

Finally, the different databases, including any database that would not be related to contact tracing processings, must be completely isolated from one another in order to avoid cross-checks that would compromise the anonymisation of the data. The respective data from the automatic and the manual tracing should be kept in different servers, as well as by different processors if doable, in order to increase security.

7) Security of the data: aspects of the organisation of tracing applications

In order to encourage the refinement and sophistication of tracing apps as well as to ascertain a free competition among (potential) app developers, it shall be allowed for several applications to be developed. Furthermore, it shall be possible for a Public application to be developed and/or for the State to acquire an existing app operating in the market.

However, the implementation of such tools in the Belgian framework pursues a reason of Public interest, namely the protection of Public Health, and as such requires strong safeguards to be guaranteed in order to be recognized by the competent Belgian authority.

In this regard, we recommend the creation of a label to be issued by the Belgian Data Protection Authority for the applications to legitimately operate in Belgium.

The label shall at least require the following criteria to be fulfilled by the candidate applications:

- a sufficient degree of securisation.
- the application shall be subject to control by the competent Belgian authority.
- the data collected by the application shall be transmitted to Sciensano's database in order to ascertain the consistency of the whole system.
- the application shall guarantee interoperability both with other applications labeled in Belgium and tracing applications recognised in other European countries.
- the application's source code shall be made public before the application is available.
- the application shall be submitted to a panel of experts for analysis before being officially published.

The fulfillment of the criteria settled out by the Belgian authorities shall be sufficient for an application to be granted the label.

Furthermore, considering that the development of non-labeled apps might undermine the efficiency of the system hereof created for reasons of public interest, it must be assessed whether an exclusion from the Belgian market of non-labeled apps is necessary and therefore may comply with European provisions regarding the freedom to provide services.

Indeed, the creation of such a label relies on reasons of public health and the protection of consumers' sensible data. This exclusion might be necessary to avoid loads of sensible data to be shared with applications without having minimal certainties with regards to their securisation nor to their involvement in the tracing system created and aiming at avoiding the further spread of the Covid-19 disease. In addition, the conditions for obtaining the label are limited to maintaining a consistent framework for tracing applications in order to control the spread of Covid-19.

Therefore, should such an assessment conclude to the need and the legality of limiting the amount of tracing apps to the labeled ones, the label shall be made as a condition to lawfully operate in Belgium.

8) Deletion

As the whole system of tracing is to be temporary, and without impacting the right to further process anonymised data which do not fall under GDPR, technical measures shall be implemented in order to enable the automatic deactivation of the application and the deletion of the data at the end of the pandemic. The official end of the pandemic shall be determined by law in order to avoid any interpretation issues in this regard. In addition, towards the settled end date of the pandemic, notifications to prompt users to disable or completely remove these apps from their phone might be considered.

Similarly, consent being at the core of the system, when data have been disclosed to third parties for research purposes, the data subjects shall explicitly confirm their consent at the aforementioned end of the pandemic for their non-anonymised data to be kept and processed for research purposes linked to the pandemic.

9) Exercise of the rights

When the consent of the user is required to use the application, the latter must be provided with all legal information. Moreover, a complete and detailed information about the actual conduct of the processing shall be displayed, fully and easily accessible online. Information includes but is not limited to the right for the data subject to withdraw his consent and specific information relating the centralized system of processing and storage in Sciensano's database, such as the purposes of the processing, the duration of the processing and the storage as well as the Regional authorities to whom the data might be transferred.

When contacted by call centers in the context of manual contact tracing, the data subject shall be provided information about the data collected, the legal basis and purposes of the processing as well as the duration of the processing and the storage. In the case of processing of non-anonymised data for research purposes - where the processing relies on consent - the (confirmation of) consent of the data subject shall further be asked via email containing complete and detailed information about the conduct of processing as well as the rights of the subject and their exercise by the latter.

Irrespective of the collection system (app or call center), information about the exercise of rights, particularly the rights to access, rectification and deletion, must be granted.

Furthermore, a system allowing the data subjects to easily exercise their rights shall be implemented.

10) Data Protection Impact Assessment

According to article 35(1) of GDPR, it is mandatory for all controllers to realise a Data Protection Impact Assessment (DPIA) taking into account "the nature, scope, context and purposes of the processing" when this processing "is likely to result in a high risk to the rights and freedoms of natural persons".

In the framework delimited by Belgian law, we wish each DPIA to be controlled by the Belgian Data Protection Authority. Administrative control is possible according to the law creating a DPA[2] before the launch of the app or the settlement of the call center. In these two situations, a DPIA is mandatory, when looking at the concerns of the Belgian DPA in its opinions 42/2020 and 43/2020.

In case Sciensano is qualified as sole controller, the three regions must be regarded as processors. Nevertheless, and in line with the opinion delivered by the Belgian DPA, all three Regions (Wallonia, Flanders and Bruxelles-Capitale) have to be considered as controllers with regard to call centers when it comes to the sharing of information between Sciensano and the Regions, since they are responsible for gathering information on infected or potentially exposed people.

[2] "Loi du 3 décembre 2017 portant création de l'Autorité de protection des données/'Wet van 3 December 2017 tot oprichting van de Gegevensbeschermingsautoriteit', such as up to date on the 3rd of June 2020.

11) Control of the processings

On the basis of the law of 3 December 2017 creating the Data Protection Authority and more specifically its Articles 58 and 60[3], it should be reminded that any citizen who is the owner of the collected data is entitled to make a complaint to the Belgian DPA.

As to any judicial control by the Court of Justice of the European Union, according to the European Treaties, the access of citizens to the Court is only possible via the use of Article 267 TFEU (preliminary reference). This access is submitted to the existence of a pending case at the national level and the question sent by the national court or tribunal to the CJEU. This question must deal with the interpretation of EU Law, primary or secondary law.

We insist in the access to an administrative control by the Belgian DPA in line with the aforementioned law (Article 58) and then to the guaranteed right to have access to a court or tribunal on the basis of Article 6 of the European Convention of Human Rights (ECHR) and Article 47(1) of the Charter of Fundamental Rights of the European Union (CFREU) with respect of Belgian law.

The interpretation of Belgian law in line with EU secondary law offers the ability for the plaintiffs to ask any judge to send a preliminary question to the CJEU in order to interpret EU law, and more specifically the GDPR. We invite as a result the national courts and tribunals, under Article 267, paragraphs 2 or 3 TFEU, to make preliminary rulings to the CJEU if necessary and to ask for the application of Article 105 of the Rules of Procedure of the Court of Justice (Expedited procedure).

12) Data Protection Officers

Article 37(1)(a) of GDPR provides that "The controller and the processor shall designate a data protection officer in any case where […] the processing is carried out by a public authority or body". It is further provided in subparagraph (b) that "The controller and the processor shall designate a data protection officer in any case where […] *the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale*".[4]

Consequently, the competent authorities and Sciensano must appoint a Data Protection Officer (DPO). The first mentioned subparagraph shall be applied in the case the Belgian Federal Government decides to settle a centralised system when setting a "coronavirus app" as well as to any public callcenters systems, while the second subparagraph is applicable when the processor is not a public entity.

This obligation is applicable to and private entities in charge of processing of data, namely the app developers or private entities who might be in charge of contacting people in each region.

[3] 'Loi du 3 décembre 2017 portant création de l'Autorité de protection des données'/'Wet van 30 JULI 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens', aforementioned.
[4] Emphasis made by the authors

13) Transfers of data inside and outside the EEA

The French Data Protection Authority (the CNIL) has adopted on 25 May 2020 an opinion on the French project of a decree on the "StopCovid" app based on a centralised system[5]. In paragraph 30 of its opinion, the CNIL took note that the app will communicate between the smartphones the identity of people exposed to the SARS-CoV-2 virus, and not people who are effectively contaminated by this virus.[6] The CNIL also underlined that there will be no registered connection between effectively infected people and people who might be exposed to the SARS-CoV-2 virus. In other words, there will be no difference between a potential exposure and an effective exposure to the virus for the application. Moreover, private apps cannot make this distinction and won't be allowed to transfer to the competent authorities whether concerned people are effectively infected or potentially exposed.

In line with the opinions expressed by the Belgian DPA, the impossibility to draw a line between effectively infected people and people exposed to the SARS-CoV-2 is respectful to the protection of personal data. In our opinion, this can go further in the idea that the communication of the possible exposition to the SARS-CoV-2 of a person cannot be done in real time, but a significant period of time has to be observed.

In case the Belgian authorities adopt a centralised system for the implementation of the app, the central server shall be administered by Sciensano but the anonymised data regarding the number of diagnosed as well as potentially infected people shall be shared with the responsible Regional authorities. When it comes to sharing data with employers, it shall only be permitted only if this is required in order to exercise their profession, e.g. medical staff or retirement home employees.

As to the installation of the app, it must be highlighted that the use of "captchas"[7] in order to ensure that the user is a human being can be a way to send personal data outside the EU. It must be explained to the users of the application that personal data are going to this private entity and the competent public authorities should anticipate that transfer of data outside the EU to be in conformity with Article 49 GDPR. A proposal to avoid the use of reCAPTCHA in the future could be to use the identity card as a way to identify as a person and not as a computer.

14) European cooperation

Currently, member States of the European Union are not sharing a common approach for the settlement of a system regarding the apps in order to tackle the pandemic. Nevertheless, and taking into consideration the opinion 42/2020 of the APD, we can find some guidelines for the development of an app. The common features must be an interoperability in protocols, with an open source code, and an integrated approach on the matter. However, we obviously do not consider that the enhanced cooperation provided in Article 326 and following articles in the TFEU is suitable because of the procedure enshrined in Article 329 TFEU, considering its heavy and time-consuming nature.

[5] CNIL, Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid » (demande d'avis n°20008032), https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2020-056-25-mai-2020-avis-projet-decret-application-stopcovid.pdf , consulted on 1 June 2020.

[6] CNIL, Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid », mentioned, para. 30, consulted on 1 June 2020.

[7] CAPTCHA is the acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart" and is a type of challenge–response test used in computing to determine whether or not the user is human. "reCAPTCHA", a famous implementation of CAPTCHA online, is owned by Google

However, we recommend competent Belgian authorities to be in favour and to promote any initiative inside or outside the EU legal framework in order to foster European cooperation in the creation of a European or a common database, a European label for apps against the dissemination of SARS-CoV-2 and a European application in order to fight against Covid-19.

RECOMMENDATIONS

I. As to the use of tracing systems

- Being a more efficient and less broad tracing system, applications shall be favoured;
- Only being fully efficient if used by a sufficient percentage of the population, they shall be encouraged by positive incentives such as tokens offering reductions in weakened industries and commerces;
- Being more intrusive, they shall be coupled with a second tracing system which consists of call centers;
- The choice of getting one's data processed by call centers must not be discouraged in any way (absence of sanction or negative incentives); in this event, collaboration shall be prompted;
- In order to offer sufficient efficiency, those call centers must realise some follow-up with infected people during the period of time where they are still considered potentially infectious;
- It shall be mandatory for medical staff to present both tracing systems as well as their respective advantages and disadvantages in order for people to make an enlightened choice.

II. As to the framework of each tracing system

1) Basis of the processing

- All processings made by an application shall be based on consent;
- Processings organised by callcenters shall be based on public interest;
- The previous point must be understood as applying only to infected people who would not have downloaded a tracing app long enough before they are declared infected (2-3 weeks);
- Further non-anonymised processings organised by call centers with regard to scientific research must be based on consent.

2) Purposes of the processing

- Contact tracing apps shall only pursue the purpose of gathering an anonymised historic of contacts who could be informed if a person that they met is declared infected;
- Call centers processings shall only aim at using data introduced by medical staff in order to contact infected people, collect a list of contact information of the people they have been close to in the previous weeks and contacting those people in order to inform them about their situation;
- All information must be anonymised in order to conduct statistical researches;
- Data processed for research purposes must be widely shared with all scientists and laboratories in order to be in line with the general purpose of Public Interest underlying the whole system;
- Data collected by call centers or shared with them can be used for research purposes in a non-anonymised format if the data subject agreed thereto.

3) Scope of the processing

- The processing in the context of contact tracing apps shall only include: **anonymised temporary keys that are regularly renewed, the status of being infected and proximity data (for the definition of each notion, see the related text)**
- The processing in the context of manual contact tracing via call centers shall only include: **name, gender, phone number, address and profession (for the infected person) and name, phone numbers and address (for the people the infected person came in contact with).**

4) General remarks about the processing

- The use of labeled apps shall be encouraged;
- The app developers shall make the source code public prior to the release of the app;
- The principles enshrined in the GDPR relating to the processing shall be fully observed;
- Particular attention shall be devoted to the principle of transparency.

5) Duration

- All data shall be kept up until three weeks after the cure, which includes the status of infected collected by a tracing app;
- The sharing of the information related to contacts with infected people shall be shared after a reasonable (one day) period of time rather time in real-time;

- Non-anonymised data aiming to conduct researches collected on the basis of consent shall be kept as long as consent is not withdrawn or until the end of the pandemic at least;
- No duration limit is to be set for anonymised data.

6) Security of the data

The following measures shall be implemented

- State-of-the-art cryptographic techniques
- End-to-end encryption during transmission
- Open-source development of the applications code
- Isolation of the contact tracing processings from other available databases
- Separation of manual and automatic tracing data on different servers
- Supervision and regular audits of the measures by independent insitutions (the most important being the Belgian DPA).

7) Security of the data: aspects of the organisation of tracing applications

- It shall be possible for several apps to operate in Belgium;
- A label fixing the minimal features and characteristics the apps should contain shall be created to improve the legitimacy of labeled apps;
- It should be assessed whether such a label might be made as a condition to operate in Belgium.

8) Deletion

- The official end date of the pandemic shall be determined by law;
- The apps shall be automatically deactivated at the end of the pandemic;
- When data are shared for research purpose the consent of the data subjects shall be sought at the end of the pandemic to possibly keep and further process those data.

9) Exercise of rights

- A system allowing the data subjects to easily exercise their rights shall be implemented;
- Information about the exercise of rights, particularly the rights to access, rectification and deletion, must be granted to every citizen;

- The app user shall be provided with all legal information at the download;
- A complete and detailed information must further be provided online;
- People contacted by call centers shall be granted information about the data collected, the legal basis and purposes of the processing as well as the duration of the processing and the storage;
- When the processing relies on consent sought through telecommunication services, the confirmation of the data subject's consent shall further be asked via email containing complete and detailed information.

10) Data Protection Impact Assessment

- The regions and Sciensano must be considered as controllers;
- Both Regions and Sciensano must realise a DPIA each as a consequence.

11) Control of the processings

- Judicial control at national level must be done in compliance with the ECHR and the CFREU;
- Reminding the possibility given to citizens, as data owner, to launch an administrative control before the Belgian DPA;
- Administrative control before the Belgian DPA must be guaranteed on the basis of the law settling the DPA;
- Reminding to the national courts and tribunals in the meaning of Article 267 TFEU their capacity to ask for an expedited procedure when making a preliminary reference to the CJEU.

12) Data Protection Officers

- Sciensano and the Regions shall appoint a DPO for each of them;
- In the case Regions would appoint private entities as processors in charge of managing the call centers, such entities shall appoint a DPO;
- In any case, app developers shall appoint a DP.

13) Transfers of data inside and outside the EEA

- Sciensano should be appointed as administrator of the central server of the app if a centralised system is adopted;
- The sharing of data with employers must be permitted only if this is strictly necessary for the exercise of their job;
- Data of infected people shall be shared with the responsible regional authorities;

- To find another way to allow the identification of users as individuals by circumventing in the future reCAPTCHA, in order to avoid the transfer of personal data outside the EU and the EEA;
- Not to make a distinction between effectively infected people and potentially exposed people in the app;
- Not to make a distinction between effective exposure and potential exposure to the virus when informing individuals about the exposition and in the app;
- To avoid by any means the direct communication to individuals about the effective or potential exposition to the virus when informing about their exposure to SARS-CoV-2.

14) European cooperation

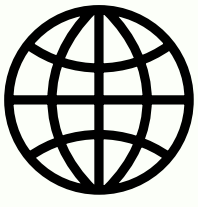
- Support any European initiative in order to promote European cooperation in the creation of a common database, a European label for apps fighting against SARS-CoV-2 or the creation of such app.

For any inquiry do not hesitate to contact us

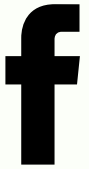
Lucas Pinelli: marketing@be.elsa.org

Viktor Francq: dpo@be.elsa.org

ELSA Belgium: info@be.elsa.org

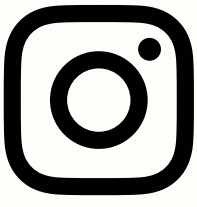


wwww.elsa-belgium.org



/ELSABelgium

/elsa-belgium



@elsa_belgium

"A just world in which there is respect for **human dignity** and **cultural diversity**"

The European Law Students' Association

BELGIUM

ELSA Belgium is composed by: ELSA Antwerpen, ELSA Brussel, ELSA Brussels, ELSA Gent, ELSA Hasselt, ELSA Leuven, ELSA Liège, ELSA Louvain-la-Neuve and ELSA Saint-Louis