noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
AUSTRIA

Ad hoc Paper (V0.3)
SARS-CoV-2 Tracking under GDPR

In the wake of the Corona crisis, many governments and non-governmental institutions consider the usage of "contact tracking apps" to fight the pandemic. They float different ideas how these systems shall look like (see examples here). While reviewing some of those ideas, *noyb* has prepared this *ad hoc* paper on legal requirements for virus tracking apps.

While this paper can give a general and superficial overview of the minimal requirements of the GDPR and possible compliance strategies, it naturally remains abstract and needs to be adapted to any specific tracking project. We feel that compliance with baseline privacy protections is crucial for the acceptance of any such tracking system by the public.

This paper is not a policy document and does not make any political assessment of different tracking approaches. It also does not attempt to assess which processing operations would be necessary from a medical or statistical perspective.

Max Schrems
Chairperson, noyb.eu

➔ We intend to update this paper over the next days and weeks. Please check for the latest version of this paper on noyb.eu.
➔ Major changes compared to version 0.2 of this document are indicated by a pink line → on the right edge of each paragraph.

1. SCOPE OF THIS PAPER (TRACKING APPS)

This paper is focused on known technical methods to tracking infections of individuals with SARS-CoV-2. These approaches focus on interactions between individuals where such interaction happens in a sufficiently close physical proximity and long enough for the virus to be transmitted – but between individuals that are not intimate enough to inform each other about their infection status without the use of a digital tracking system.

Realistic scenarios are e.g. encounters with co-travelers on a train or bus or longer interactions in stores, restaurants and alike. In contrast, the tracking of briefly passing stranger on the

street (as the interaction is usually not intense enough) or the tracking of co-workers or family members (as they are known to the infected person anyways) seem to be of limited benefit.

This paper does not cover the use of personal data for statistical purposes or policy assessments (like mobile phone data analysed for movement statistics) or the use of personal data for the surveillance of quarantined persons.

Preliminary scientific papers (see for example here) have indicated a very strong reduction of the spread of SARS-CoV-2, if the window between infections and dissemination of the virus can be narrowed through an app. This paper is therefore based on the *preliminary assumption* that the use of contact tracing apps can be an appropriate, proportionate and effective approach to limit or prevent the spread of SARA-CoV-2.

Any compulsory implementation of such measures need to be based on a wider factual assessment that proofs that such measures are effective to make them proportionate (also compared to other measures) under Article 7, 8 and 52 CFR.

2. KNOWN TECHNICAL APPROACHES

Currently, two approaches are debated to track possible infections with SARS-CoV-2. There may be other approaches not (yet) covered by this paper.

2.1. Tracking via mobile network data

Different media reports and political debates have focused on the use of mobile operator data to fight SARS-CoV-2. As far as known to *noyb*, location tracking based on mobile phone networks is not accurate enough (accuracy of only 50 Meters or more) to get relevant information about the interaction between two persons in most realistic scenarios.

> *For example: When two users are on the same train or in the same building, network data will unlikely be able to differentiate between the train carts or rooms of the building.*

Given the current state of technology, personalised tracking of possible exposed persons based on network data, will hardly be technically feasible, especially within buildings. Given the lack of accuracy, it is highly likely, that such an approach would lead to too many notifications and "information overload".

2.2. Locally installed tracking apps

The other approach is based on locally installed smart phone apps. These apps can access more precise positioning data and allow communication between phones and thereby log the interactions between people.

There are different technological approaches to generate and exchange the necessary interaction information (like ultrasound, Bluetooth, WiFi, NFC signaling and/or GPS tracking). Some of these technologies function in buildings or tunnels, whereas some do not allow tracking in such places.

In most projects, Bluetooth Low Energy (BLE) is used to transmit IDs, without reducing the battery life of a smart phone. This technology is limited by operating systems and available data packet sizes. The transmitted information is limited to about 23 bit, which makes a direct exchange of many forms of modern encryption or key exchanges impossible. In addition, Apple's iOS limits the use of BLE for applications that are operating in the background.

The further use of the generated interaction information may come in many shapes and forms, including local storage and cloud storage, as well as different deletion routines, encryption and pseudonymisation approaches. Some system designs may follow a more federated (peer-to-peer) approach; others may follow a more centralized approach.

This paper focuses on the approach using smartphone apps, instead of mobile network data, which appears to currently be the most realistic and efficient approach.

3. USE OF GENERATED TRACKING DATA

The interference with the fundamental rights of the individual depends on the consequences of the processing of personal data. So far, the following approaches seem to be envisioned:

3.1. Different steps and processing operations

Most concepts foresee different steps and processing operations for (A) the ongoing tracking of personal data ("*capturing phase*") and (B) the use of data in case of a necessary warning about the interaction with a SARS-CoV-2 positive person ("*incident*"). Applications may allow notifying multiple types of incidents (such as a suspected infection, a confirmed infection or a correction of a false notification that was previously transmitted).

Different legal analysis may apply to these different situations and processing purposes. These processing operations may be even performed by different controllers (see below).

Additional functions (like "data donations" for combatting SARS-CoV-2, self-assessment functions and other information) may be seen as separate processing operations, which are not the focus of this paper.

3.2. Consequences of incidents

The acceptance and possible behavioral change of users (like avoiding tests to avoid the consequences of a positive outcome) widely depends on the legal and practical consequences of the use of any such application:

- **Information of persons**

Some approaches focuses on the attempt to pro-actively inform persons that have interacted with a SARS-CoV-2 positive person, so that these individuals can act accordingly (like requesting a test, self-quarantine, etc). It leaves each individual with the freedom to take self-determined measures – or to even ignore the information that was provided.

- **Identification, test and/or isolation of positive cases**

Other approaches focused on the attempt to identify, test and quarantine persons that have interacted with a SARS-CoV-2 positive person as quickly as possible.

This is obviously a much more serious interference with the individuals' freedoms and is likely to collide with a wide range of fundamental rights (such as the freedom of movement, freedom to conduct a business and freedom to privacy and family life) that follow the processing of personal data. The interference is, however, limited to specific individuals. In such cases, the public interest may override the rights of the individual, as foreseen in existing laws that allow for a mandatory quarantine.

In practical terms, some users may be deterred if the use of a tracking application may lead to the limitation of their freedoms.

- **Identification, test and/or isolation via a combination with national laws**

In certain jurisdictions, even apps that only aim at informing an exposed person may indirectly trigger duties of the exposed person to be tested or isolate.

> *For example: A criminal law or tort law may treat inaction by an informed exposed person as negligence or even intent to spread the virus further or to infect a person.*

It is therefore necessary to assess possible legal consequences of a mere notification, as this notification could be viewed as a "fact" that triggers legal consequences. In many jurisdictions, case law exists on the negligent transmission of other infectious diseases like HIV or Hepatitis.

- **Limitation of the freedom of movement ("app duty")**

According to certain (unverified) reports, some countries seemed to take the reverse approach and allow freedom of movement *only* to persons that use an application.

A variation of this approach could be that the use of an app would become a *de facto* requirement to take part in public life, for example because businesses would require customers to use a tracking app to continue using their services.

This follows an "*infected unless proven healthy*" approach and leads to a very severe interference with a wider range of fundamental rights.

At the same time, this is the approach that many European governments have *de facto* taken when declaring a national lock-down for all residents of a country or areas without further differentiation between individuals. While different forms of tracking interactions could be seen as proportionate to fight SARS-CoV-2, one has to take into account that a "lock-down" may not only interfere with the right to data protection but with other fundamental rights (like the freedom of movement, the freedom to conduct a business or the freedom of assembly).

Exceptions for persons that are (temporarily) not able to use forms of tracking (see below at 6.5) would be necessary to avoid illegal discrimination and arbitrary regulations.

4. LEGAL ANALYSIS UNDER GDPR

4.1. Controller(s)

Systems may be based on a centralised architecture, where a governmental entity or private company (such as a health care provider) qualifies as the “controller”.

In the alternative, a system may be based on a network of end-users (“peer to peer”) where each user may (depending on the design of a system) qualify as the “controller” for a local processing operation, such as an automated “contact book”.

Such processing could (in limited situations and strict technical implementations) even be considered to fall under the “household exemption”, which includes the “holding of addresses” (Recital 18 GDPR). A local “interaction protocol” or “contact book” could (in certain cases) be interpreted as a “household activity”. In such limited situations, the local processing of such data would not fall under the regulations of the GDPR, which may allow for more flexibility in the design of a “peer to peer” system.

A combination of different (joint) controllers for different parts of the processing operations may be parts of an overall system.

For example: When an overall system consists of a centralised notification system and local tracking of interactions, the user could be the controller of the local contact book and a health care provider could be the controller of the notification system..

4.2. Personal data

As the aim of any such processing activity is the tracking and/or information of a specific infected person or the information of people who have had personal encounters with an infected person, the necessary data about interactions, locations and alike usually constitutes personal data.

By definition, data that allows the identification or the singling out of an app user by the respective controller and/or other app users cannot qualify as anonymous and must be seen as personal data (Article 4(1) GDPR). Given that the only purpose of a “contract tracing” app is to trace an individual exposed person, it seems unthinkable that such a system could be designed with only truly “anonymous” data. Therefore, the GDPR usually applies to the processing of such personal data.

4.2.1. Special categories of data

In most cases, the processing operations are aimed at transferring specific information about the infection with SARS-CoV-2, which clearly constitutes data about a person's health. These data are treated as a “special category” of data, the processing of which is subject to stricter rules under the GDPR.

For the purposes of this paper, it is therefore assumed that most processed data must be treated as a “special category” under Article 9(1) GDPR.

4.2.2. Pseudonymous data

Certain elements of any tracking system can (and according to data security and data protection by design principles must) be based on pseudonymous data (such as hashes, random IDs and alike). Such data still falls under the GDPR and all relevant protections, but may be a required from a data security perspective (Article 32 GDPR). The use of well-chosen pseudonyms usually leads to a lower potential for misuse and interference with the right to data protection.

4.2.3. Encrypted data

Other elements of any tracking system can (and according to data security and data protection by design principles must) be based on encrypted data.

Such data still falls under the GDPR, even when data may not be identifiable for certain holders of information (for example when tracking data about others is stored locally in an encrypted format, with a third party having the decryption key).

Proper and intelligent encryption is at the same time a crucial element to comply with the requirements of the GDPR, like data minimisation (see below) and data security (Article 32).

4.3. Legal basis for processing

Any processing operation needs to have a legal basis under the GDPR. A controller has to rely on one or more legal bases for the processing of personal data, and has to make it clear to the users which legal basis is underlying each processing operation, bearing in mind that there may be different legal bases for different processing operations. Overall, the GDPR offers multiple legal bases that may apply to the processing of SARS-CoV-2 tracking information.

4.3.1. Consent

As with any processing operation, the data subject can consent to the use of personal data. This may be the preferred approach for most processing operations, given the sensitivity of the data and the severe interference with the right to data protection.

Special attention must be given to consent being “freely given”, “specific”, “explicit” (or “unambiguous”) and “informed”.

In the employment context, the insurance context or in the case of government measures, consent can usually not be deemed freely given. It may lead to a conflict between the GDPR assessment of the controller and the factual situation for the data subject, if governments, insurances or employers require the data subject to use a contract tracing app, or to use the notification function of an app.

> *For example: When a private app provider bases the processing of personal data on consent, but governmental regulation makes the use of an app a condition to leave the house, the consent cannot be considered as “freely given” consent.*

Consent should ideally be given when installing an application or for each interaction with another user of an app.

The app (or any framework that the app is using) may allow defining the conditions under which a user consents to the use of data. A user may only consent to specific purposes, to a

certain duration and alike. Such limited consent could function as an additional layer of legal protection, when technical protections are not available.

In most realistic scenarios, it seems that the tracking of interactions with other people in the capturing phase, as well as any notification in the case of an "incident", can be based on the consent by the person that installed the application and/or triggered the notification.

Tracking of other users that have not installed an app (like when a system cannot differentiate between IDs of smart phones that installed the app and those who have not), would have to be based on another legal basis.

4.3.2. Vital interests

Recital 46 GDPR explicitly mentions "*monitoring epidemics and their spread*" as a "vital interest" of the data subject or a third party. It can therefore be assumed that processing of data for such purposes is a "vital interest" of the data subject or a third party.

Article 6(1)(d) GDPR ("vital interests") does not apply to special categories of data. Consequently, this legal provision only allows processing of data that does not constitute a special category under Article 9 GDPR.

> *For example: The collection of contact data in a "contact list" (e.g. Bluetooth identifiers during the "capturing phase") does usually not reveal any special category of data (like health information), but is necessary to notify a person in the case of an "incident". The collection of such information may possibly be based on Article 6(1)(d) GDPR.*

As Article 9(2)(c) GDPR requires that special categories of data may only be used for a "vital interest" if, in addition to the requirements in Article 6(1)(d), the data subject is "*physically or legally incapable of giving consent*", it seems unlikely that it could be a suitable legal basis for processing special categories of data, once an incident occurs – unless a patient is becoming critically ill in a very short period of time.

> *For example: Consent or another legal basis under Article 9(2) GDPR seems to be necessary for the notification of other users about an "incident" as this constitutes data concerning health of the infected person and potentially the exposed person.*

Whenever processing for the combat of SARS-CoV-2 constitutes a "vital interest", the question if processing can also be based on a "legitimate interest" under Article 6(1)(f) GDPR should not arise. In other circumstances the usual balancing of interests under Article 6(1)(f) GDPR has to be exercised (e.g. for the use of data for purposes of data security or fraud prevention).

4.3.3. Union or Member State laws

Article 9(2)(i) GDPR foresees that Union or Member State law can allow or require processing in the case of "*serious cross-border threats to health*". SARS-CoV-2 clearly fulfills this definition. The clause at the same time requires "*suitable and specific measures to safeguard the rights and freedoms of the data subject*".

While Article 9(2)(i) seems to the be *lex specialis* for most processing operations during the SARS-CoV-2 crisis, Article 9(2)(g), (h), and (j) GDPR may also allow the Member States to pass

national laws that require the processing of special categories of personal data for reasons of substantial public interest, certain medical and health care purposes or research and statistical purposes. Any such national law has to provide specific and suitable measures to safeguard the rights and freedoms of data subjects. This means in essence that such national legislative measures are only allowed to restrict the fundamental rights of privacy and data protection where it is suitable, necessary and reasonable to achieve the aim.

There may be existing national laws (such as laws on infectious diseases) or newly created legal measures for the fight against SARS-CoV-2. This paper does not assess the compliance of any particular existing or proposed national legislation in Member States with GDPR.

- **Legal basis to process personal data ("permission")**

A law may *allow* certain processing of data, while leaving it up to the controller if they wish to process personal data (like a general permission to use personal data for tracking).

- **Duty to process and/or provide personal data ("duty")**

In many cases, laws will *require* certain processing of personal data (such as reporting duties for infectious diseases). This may influence the design of a tracking system.

> *For example: A system may be designed to either include a "reporting" function, or to the contrary, it may be designed so that information duties do not apply to the individual user because the data is encrypted or pseudonymised to an extent that a user cannot possibly fall under a duty to report an infected person – which would otherwise apply under national law.*

A deeper analysis of specific laws is beyond the scope of this paper, but seems to be crucial to avoid unintended consequences or surprising legal duties of the users of an app.

4.4. Purpose limitation

The principle of purpose limitation is the "backbone" of any data protection analysis, since further compliance with the GDPR provisions will be assessed against the specific purposes identified and communicated by the controller of a processing.

Purposes must be specific enough to allow a good understanding of any data usage. Hence, the "prevention of further SARS-CoV-2 infections" is for example not specific enough. Examples for relevant purposes may include:

- retaining interaction information for SARS-CoV-2 tracking,
- the information of persons about SARS-CoV-2 exposure,
- the information of health authorities about SARS-CoV-2 exposures or
- verification (e.g. towards a third party) that there are no known exposures of the user.

The exact actual and precise purpose(s) will depend on the functionalities of the application or tracking system. There may be numerous purposed for each function of an app.

4.4.1. Secondary use

Under certain conditions, the GDPR may allow the secondary use of personal data for other purposes that were not originally envisioned (for example under Article 6(4) GDPR).

It is however necessary that foreseeable purposes (like research and statistics) are included in the original list of purposes (Article 13(1)(c) GDPR). The processing of data for such purposes must usually be made optional and must usually be based on the consent of the user. If it is based on other legal bases, the user must be informed properly and - in cases of processing based on legitimate interest - be provided with the option to "opt-out".

It is generally possible to allow users to "donate" their personal data for useful, but unnecessary processing operations (such as statistics or research). Given fight against SARS-CoV-2 it is also highly likely that users will opt-in to such secondary use.

4.5. Data minimisation

4.5.1. General principle

The general principle of data minimisation should ensure that only the minimum amount of information is processed that is necessary for the purpose. This does not mean that the collection of information has to be limited to an extent that the purpose cannot be fulfilled anymore. Any information that is necessary for the purpose of the processing operation can be processed. If the processing operation may not provide sufficiently accurate data, it is necessary to process the relevant data to achieve sufficient accuracy.

Examples of data that may be relevant (depending on the system):

- Date and time of an interaction
- Location of an interaction
- Duration of an interaction
- Identifier of the person that the user interacted with
- Data to verify the accuracy of a reported infraction (prevention of misuse)

Examples of data that may not be relevant (depending on the system):

- Data about persons that do not participate in a tracking system
- Device identifiers or tracking information that is not relevant from a medical perspective
- Exact timestamps, locations and alike, if less specific information (for example only the date instead of the exact timestamp) is sufficient.

4.5.2. System design on a "need to know basis"

Any tracking system needs multiple actors (ideally the majority of the public) to jointly share and process personal data. Only an utmost limitation of available data for each individual actor can lead to an overall system that is in any way complaint with the fundamental rights to data protection and privacy. This may be implemented through a stringent "need to know" approach, where access to data is strictly limited to the persons and entities that need to process the data, with adequate technical measure to implement such a policy. This approach may be limited by technical and organizational constraints.

> *For example: The logic that decides if a person is notified (for example based on distance, duration and time of the contact) could be running on the device of the infected person, the central administration or the exposed person. Different data must then be stored and sent.*

4.5.2.1. Data that is available to the central administrator

There may be certain data ("account information") that a central administrator may need to verify the individual app user's identity. Controllers who act as central administrators may seek to limit such data, or only require further information on the user's identity in certain situations (e.g. when a user reports an incident or requires medical assistance). Even in such situations, alternatives that limit the personal data that is stored at a central administration could be used.

> *For example: To ensure that only verified positive cases can be reported, a centralised notification system could require a code/token, that is distributed to each person that was tested positive for the virus. This could verify the accuracy of a reported infection, without the need for a centralized account.*

Other information, such as the use of statistics, should be based on anonymous data.

4.5.2.2. Data that is available to the normal user ("capturing operation")

The app user, who does not have any function as a central administrator, appears not to require access to any personal information of other individuals during the capturing operation of a tracking system. Depending on defend design and privacy choices, such data may be stored locally or in a centralized system.

The identification data that is provided by the device of the persons the app user has been in contact with, may be pseudonymised or encrypted before or after it is shared with the app user, which should ensure that users cannot access each other's personal information. Identifiers can also be rotated on a regular basis, to increase the number of identifiers assigned to each user. This limits the possibilities to track a person using identifiers.

The local contact list may be fully shielded from the user that collects the information. Data that is not or no longer necessary for the user should be automatically deleted, for example when the potential incubation period of the virus has passed.

4.5.2.3. Data that is available to the infected person ("incident")

If a person is known to be infected ("incident"), that person should ideally not have to do more than reporting that fact in a verifiable way. To avoid false notifications, some form of approval/review could be ensured (for example a confirmation of a health care professional that conducted the SARS-CoV-2 test or a code/token that is handed out).

The infected person does not need to know which exposed persons will be informed.

A trusted third party (for example a health care provider or government entity) could take care of the decryption, review and analysis of the collected data and trigger the notification of exposed third parties.

4.5.2.4. Data that is available to the exposed person ("incident")

If a person reports an infected, the exposed person may only be notified about the fact that he/she was exposed. Such information may be sent via a centralised communication service or through a "peer to peer" system. In certain setups, the local app may download a list of IDs

of infected persons to then match them against the local contact book of a user. In other setups the infected person reports the IDs of the exposed persons, which are in turn notified.

Additional information (such as date, time, distance and location) may be relevant to understand how severe the exposure was or how long symptoms can realistically be expected. Such additional information may, however, interfere with the right to privacy of the infected person, as it may reveal the identity of the infected person.

To balance these conflicting interests, it may be possible to provide such information in a format that is abstract enough (for example only the day of the infection and rough duration of the exposure or an "exposure score") to provide the relevant information, while also ensuring the anonymity of the infected person as far as possible.

4.5.2.5. Data that is available to public authorities / health care providers

Depending on national legislation or the design of the system, data may need to be provided to public authorities or health care providers. The design may deliberately not process such information, to circumvent such information duties (for example to strengthen the trust of users in the anonymity of the system).

Whenever possible, statistical data or data relevant to research should be based on an "opt in" consent, to ensure that users can "donate" their information if they wish, but may also use the core functionality of the app without the further use of any personal data.

4.6. Accuracy of data

Especially when it comes to such a sensitive matter as the infection with a highly contagious virus or the exposure to a virus, the accuracy and quality of data is of utmost importance.

It would be counterproductive and even negating the purpose of the processing activity, if users get either false or too many (irrelevant) notifications about a possible exposure ("information overload"), or too few or delayed notifications. Some examples that may be considered to ensure that accurate data is provided:

- *Special focus needs to be put on an accurate technical analysis of the interaction between two individuals and any possible logic or algorithm that decides which exposed individuals need to be informed. A decision about which person needs to be informed could for example be based on proximity, timeframes (times at which a patient was likely more/less infectious), duration of interactions, or if the encounter happened within a building, during transit or outside (e.g. based on GPS locations). Such an analysis of the raw data may only be done in the case of a confirmed "incident", or already during the capturing phase or a combination thereof.*
- *Equally, a system needs to provide accurate enough information to the exposed person, to enable it to take the relevant steps. Options may range from a mere binary information (exposed/not exposed), an "exposure score" or contextual information like day, duration, location and proximity.*
- *Finally, it seems important that users cannot single-handedly provide inaccurate information (like self-reporting as positive/negative without an independent verification).*

While the accuracy of information from a medical perspective must be assessed jointly with medical experts, a duty to provide accurate information also results from Article 5 GDPR.

It is important to review the possible legal consequences of a notice that a user was exposed. In some countries, this information may trigger serious legal consequence, which may not be intended by the developer of the app and is also subject to certain limitations under the GDPR (see point 4.9. below).

4.7. Storage limitation

The principle of storage limitation requires that personal data may not be kept for longer than necessary. Timelines must be based on medical relevance (like infection times) as well as realistic durations for administrative steps that may need to be taken.

> *For example: Data may be kept for realistic infection times and realistic SARS-CoV-2 test times, to ensure that data is not deleted before a positive test result is available, but also not kept for longer than absolutely necessary.*

It is imperative that data is deleted as soon as it cannot fulfill the relevant purposes anymore.

4.8. Data security

Any such tracking system would be a prime target for many actors, if only to test if the security of the architecture. Attackers may develop their own applications that interact with a system or other apps, but provide false data or collect data for illicit purposes. Given the sensitivity of the processed data, but also the need for public trust in a SARS-CoV-2 tracking system, data security has to be at the heart of any proposed system, while at the same time be "appropriate" (Article 32 GDPR) compared to these risks and the consequences of misuse.

4.9. Automated Decision Making & Profiling

Most approaches on tracking apps have in common that decisions are taken on the basis of the data collected and processed through the app, with the support of algorithms assessing the situation (for example assessing a "relevant exposure" or an "exposure score").

As a rule, decisions solely based on automated decision-making are not allowed under the GDPR, when such decisions have an impact on the legal status of individuals, or when they can significantly affect them in a similar way (Article 22 (1) GDPR).

While a government controller may be able to take such measures, a private controller itself may not be able to take such a decision. However, even private controllers may *de facto* form such decisions in combination with other legal obligations ("split decision"). This may be the case, for example, when certain actions or restrictions are taken or imposed if a person is informed about their SARS-CoV-2 status or a possible exposure.

> *For example: A national law may require that a person that becomes aware of an exposure must self-quarantine for 14 days. An employee may need to inform his employer about a possible exposure any may not be able to work for a certain time. A user may violate a national criminal law or tort law, if he or she does not take the necessary steps to ensure that he or she does not further spread the virus.*

No matter if indirect or direct, such decisions are prohibited as a rule. Only three exceptions to this prohibition can be envisaged: (i) when EU or national law allows it, (ii) when it is

necessary for entering into or performance of a contract or (iii) when the users have given their explicit consent.

If special categories of data (the so-called "'sensitive data'") are processed in the context of automated decision-making, only two exceptions apply: (i) when the individuals have given their explicit consent, or (ii) when the processing is necessary for reasons of public interests, on the basis of EU or national law.

In cases, where automated decision-making is allowed, suitable measures must be adopted to safeguard the rights, freedoms and legitimate interest of the persons whose data are processed. It also means that a human, able to explain and influence the decision, must always be involved in the process. In other words, there must always be a "human behind the machine" who is acting on behalf of the controller and can explain and oversee the decision, taking into consideration all relevant data. This will allow correcting possible errors in the process, which can lead to incorrect classification, unlawful discrimination or other negative impact on the individual or assessment based on wrong assumptions.

The nature and the safeguards put in place, the impact on the rights of the people and the existence of any human involvement should all be mentioned in the Data Protection Impact assessment to be performed according to Article 35 (1) and (3) GDPR.

These safeguards must also be communicated to the individuals, together with a complete information about the automated decision-making. They should always be in a position to understand the rationale behind a decision affecting them, before but also after the decision is taken, putting them in a position to contest it.

Finally, where the processing involves profiling, the individuals should be fully informed about the existence of the profiling and its purpose (e.g. to predict the spread of contagious diseases within a specific category of a population). Profiling is a further processing of data and has to fully comply with all the requirements of the GDPR.

5. DATA PROTECTION BY DESIGN

Any tracking system that is meant to gain widespread acceptance by the society must be built with privacy protections in mind. This should go beyond the letter of the law in Article 25 GDPR and should include a wider attempt to design a privacy friendly architecture.

5.1. Local storage

Many technical solutions rely on the local storage of interaction information (“self-tracking”).

This can give the individual user factual power over the data, as the data physically remains in the hand of the user. It should be ensured that the data is stored in a secure way and neither accessible by the operating system nor other applications on the user’s phone.

Local storage also means that the data of other tracked persons may be used by the device owner. Mitigation strategies may include encryption or pseudonymisation of such information before it is transmitted or stored on the local device.

5.2. Encryption (public/private keys)

Especially in situations where potentially millions of users process personal data on each other, strong encryption may ensure that data can be shared while preventing that each recipient can misuse and disclose such data.

Asymmetric cryptography is especially suitable to achieve this aim. Key exchanges may for example be based on a peer-to-peer basis or on a trusted institution.

5.3. "Two-person" rule

As a further precaution, the use of personal data (especially in the case of an infection) can be based on the “two person” rule, meaning that two actors (for example the infected person and a health care professional) must enter a key to trigger a processing operation like the decryption of data or the notification of exposed persons.

5.4. Pseudonymisation

Whenever anonymous or encrypted processing of information is not possible, pseudonyms must be used to obfuscate the personal data that is processed.

Pseudonymous data is not privileged under the relevant rules within the GDPR and must be treated as normal “personal data”.

5.5. Independent verification

To ensure the accuracy of personal data that is shared through a system, forms of independent verification may be introduced. A system must for example ensure that users cannot enter false information and trigger inaccurate notifications.

5.6. Third party services

Developers regularly use third party services, plug-ins and SDKs. Such elements often require third country data transfers. While this *can* be compliant with the GDPR, the mere mentioning that third parties have access to (some) personal data may lead to rejection by users. Typical examples are third party cloud hosting, SDKs for bug tracking or functions of the operating system to show notifications to the users.

Design choices between usability and privacy may be left to user preferences, when allowing them to “opt in” to additional functions.

5.7. (Conflicting) Rights under GDPR and other laws

Users may exercise their rights as data subjects against the relevant controller. This may conflict with the interests of other users (for example when an infected person wants to know who the recipients of the notification are, see Article 15(1) GDPR).

Users may also refrain from (properly) using certain applications or systems, when national laws require the controller to report data to governmental entities.

A strict “need to know” basis may enable the controller to handle such requests by invoking national laws and/or Article 11(2) GDPR.

6. OTHER ISSUES

While not directly linked to a legal analysis under GDPR, the following points seemed worth mentioning in any *ad hoc* paper on SARS-CoV-2 tracking approaches:

6.1. Sufficient acceptance

Any SARS-CoV-2 tracking system is heavily dependent on the acceptance of a large portion of any society. Good privacy and data protection practices are surely a precondition for broad acceptance of any tracking system by the public.

6.2. Interoperability

Especially (competing) private initiatives may consider certain interoperability with other applications or systems when designing a SARS-CoV-2 tracking system. This may also require certain additional processing activities, e.g. for sharing data between applications or between devices. Interoperability may consequently also require different legal bases for processing under Article 6 and 9 GDPR. Furthermore, the principles of data protection by design must be adhered to, when developing interoperable technical solutions.

6.3. Social pressure

While social pressure may be desirable for anyone that initiates a SARS-CoV-2 tracking system, as this may be a key factor for the use of any system, a freely given consent to a tracking system may not be possible if it is *de facto* impossible to not use it (for example if private entities make the provision of services dependent on the use of an app). The same applies in an employment context, where the consent of an employee is deemed not to be freely given.

6.4. Behavioral changes

Dependent on the legal and technical interplay, surveillance and tracking measures may also lead to behavior that undermines the tracking effort.

> *For example: If a SARS-CoV-2 test leads to quarantine measures, overly broad information about the health status to third parties, discrimination and alike, some people may try to avoid testing. If the information through an app leads to the duty to be tested, people may avoid using the app.*

Such behavioral changes and possible evasion tactics need to be considered in an app design.

6.5. Limited access to technology

It cannot be assumed that every person has access to a modern smart phone, which is fully operational and charged. Subscribers also regularly exceed their data limits.

Others may use alternative operating systems (like Blackberry or “open” Android derivatives) or traditional mobile phones. Some users may not use Google or Apple accounts, which are necessary to download applications from their respective app platforms.

Children usually do not have mobile phones at all. Especially elderly (and therefore vulnerable) people may not have a mobile phone at all or may not use smart phones. Mobile phones that

are designed for elderly people may not use an iOS or Android operating system and cannot run external applications. Many such phones are in essence only “feature phones”.

6.6. Open source & independent verification

Implementation as open source software, as well as other forms of independent verification, can be crucial elements to ensure high quality and trust in any tracking system. This can be independent of the licensing model (for example when the code is published, but the copyright stays with an entity to ensure the proper use of the code).

Open licenses may allow sharing technology among countries and developers – especially for lesser-developed regions or countries that are too small to operate their own tracking system.

6.7. Nudging as a softer way to ensure adoption of a system

Different forms of “nudging” could be used to encourage the use of an app, for example:

- Clear and transparent communication about the functioning of the app
- A frictionless testing routine that is linked to the use of the app
- Sending direct links to each phone with the link to the installation page
- A bonus by the mobile phone operator for anyone that installed the app
- Discounts by shops, restaurants and services for app users
- Encouragement through “badges” that can be shared on social networks
- Including apps in announcements that must be posted by employers, shops or on public transport
- Invitations to install an app by schools, universities, employers, public transport or clubs
- Engaging trusted role models (“influencer”) to promote the app
- “Invites a friend” option

6.8. Other processing operations

Apps may process additional relevant information (like the information that a user had a negative test on SARS-CoV-2, information about mere symptoms and alike) and allow users to share additional information for research, public health and statistics (“donate your data”).

Apps should ensure that such different functions are usable independent of the core tracking function, as it is highly likely that a vast majority of users would “opt in” to additional processing for the public good, but such processing may deter others from using the core functionality of the app. The GDPR would also not allow “bundled” consent” to functions that can be separated.

CONTACT & FEEDBACK

We are very much looking forward to improve this paper further. Should you have any feedback on this ad hoc paper, or need further support when developing any system or app that is aimed at combating SARS-CoV-2, do not hesitate to contact our legal team at info@noyb.eu.