# Considerations arising from the letter to parliament on the introduction of ‘CoronaMelder’


## Message to Parliament

In April, the Rathenau Instituut sent the House of Representatives five considerations for the parliamentary discussion on the coronavirus crisis, which also included consideration for the coronavirus apps that had been announced at the time[1]. In response to this letter to parliament on the national introduction of ‘CoronaMelder’[2], we hereby provide additional considerations.

The five considerations we highlighted earlier were:

1. Strengthen the public health infrastructure.
2. Assess the use of coronavirus apps as part of public health: not as the core of the solution, but as one policy option.
3. Take the time to carefully examine the coronavirus apps, paying attention to all relevant aspects.
4. Develop knowledge about the coronavirus apps, and other policy options, so as to guide international and European policy development.

---

[1] https://www.rathenau.nl/nl/digitale-samenleving/de-coronacrisis-vraagt-om-zorgvuldig-handelen-en-democratisch-debat

[2] https://www.rijksoverheid.nl/documenten/kamerstukken/2020/07/16/kamerbrief-over-landelijke-introductie-coronamelder

5. Act in such a way that citizens maintain confidence in the approach to the coronavirus crisis.

These considerations remain important. To combat the coronavirus, the public health infrastructure must be adequately equipped. The infringement of citizens' rights associated with the introduction of CoronaMelder is only justified if it is demonstrably necessary and if the integration into the public health infrastructure is effective. Adequate capacity at the GGD (Municipal Health Service) for source- and contact tracing and adequate test capacity are of primary importance.

By means of this letter, we provide you with additional considerations on six issues:
1. Fragmented provision of information;
2. Justification and proportionality;
3. Dependence on, and preference for, Google and Apple;
4. Medical data;
5. Risk of profiling and stigmatisation;
6. Complaints, objections, rebuttal, harm and redress.

**1. Fragmented provision of information**

The information provided to the House is very fragmented. The letter from the minister and the numerous recommendations are pieces of an incomplete puzzle.

The House of Representatives can ask the Cabinet to help the political and social debate by starting with an explanation based on the existing legislation and the current powers of the minister and the GGD, and then indicating how CoronaMelder contributes to this.

**2. Justification and proportionality**

Given the CoronaMelder reliability of 70-75%[3], in combination with the reliability of coronavirus tests and the risk of inaccuracies in the reporting process[4], the question is whether the introduction of the app will be adequately effective and therefore proportionate. Due to the lack of a clear explanation regarding proportionality, it is now also unclear when the use will no longer be proportional and when the app will be terminated.

The European Convention on Human Rights (ECHR) states that there shall be no interference by a public authority with the exercise of rights of citizens, such as their privacy rights, except such as is in accordance with the law and is necessary in a

[3] https://www.rijksoverheid.nl/documenten/rapporten/2020/06/08/veldtest-bluetooth-validatie-covid-19-notificatie-app

[4] https://www.rijksoverheid.nl/documenten/rapporten/2020/07/07/gegevensbeschermingseffectbeoordeling-dpia-covid-19-notificatie-app

democratic society in the interests of, for example, the protection of health or for the protection of the rights and freedoms of others.

The House of Representatives can ask the Cabinet how the announced legislation regarding the coronavirus app meets the quality requirements set by national and international legislation, such as the ECHR.

The House of Representatives can ask the Cabinet to determine a date on which the use of the app will be terminated, or to indicate the criteria that will lead to the termination.

**3. Dependence on, and preference for, Google and Apple**

With the possible introduction of CoronaMelder, the government will enter into a far-reaching relationship of dependency with the private parties Google and Apple with regard to its public health infrastructure. As the Digital Support for Combating COVID-19 advisory committee has already conveyed (Advice 2: Use of Google and Apple APIs), clear and binding agreements with them are essential.

For example, Google and Apple do not currently provide a complete insight into the source code of the API they offer, and it is uncertain whether the partially disclosed source code is the same as the code actually found on users' phones. The independent monitoring of security aspects and control of improper processing of personal data are therefore impossible.

Furthermore, Google and Apple now unilaterally determine the terms of use and are free, at any point in the future, to change those terms of use or the behaviour of the API.

Currently, for example, even though it is not necessary from a technical point of view, the Google Play Store and registration of a Google account are both conditional requirements when it comes to using the CoronaMelder on Android systems. Users with other Android systems or, for example, various Huawei phones on which the Google Play Store is not available, are therefore excluded.

In short, the Cabinet strengthens the competitive advantage of Google and Apple, while it is impossible to determine whether their API is a Trojan horse.

In the Netherlands, the introduction of the Electronic Patient Record and the application of artificial intelligence (AI) in healthcare has been handled with great care. To date, the work on the challenges that this entails are still ongoing. The House of Representatives must ensure that these private parties cannot gain access to medical or other sensitive data via this app without strict guarantees regarding privacy.

The House of Representatives can ask the Cabinet how it will manage the risks arising from the dependencies on Google and Apple.

**4. Medical data**

The Data & Privacy Impact Assessment (DPIA) notes that if the GGD discovers a (possible) infection, there will be a treatment relationship between an infected citizen and the GGD. Once this data becomes part of the treatment relationship, it is protected by medical confidentiality. The relevant data is then part of the medical record, and the current laws and regulations regarding this are applied. For example, in cases where the infection data is used for research for the sake of (insights into) public health.

Furthermore, app users, in their capacity as patients, have different rights with regards to the data in their medical record. For example, as a general rule, the patient must give their permission for their data to be used further by those other than the treating GGD healthcare professional. It is currently unclear as to how the app ensures that medical confidentiality is respected and that users are informed about this. In the documents provided thus far, hardly any attention has been paid to the medical nature of the data and the applicable rules.

The House of Representatives can ask the Cabinet whether the app meets all the requirements for processing medical data.

**5. Risk of profiling and stigmatisation**

The DPIA focuses solely on the GDPR aspects of the app itself and the data processed in it. A DPIA should also assess the risks of profiling, but in the current document the risks of profiling have not been taken into account.

The app functions, for example, within the operating systems of Google and Apple. It is therefore possible for these companies to combine the (telemetric) data of users with other data about users who are already known to them, and thus build profiles.

Users and non-users of the app can also be stigmatised. People may be asked if they are using the app and this can be determined by a scanner without their knowledge. In all kinds of situations, there is the risk of stigmatisation, discrimination and exclusion, whereby users can be harmed, their choices can be influenced or, for example, they can be denied access to important places, products, services or treatments.

The threat posed by profiling and stigmatisation can be long-term. After all, profiles can continue to exist for a long time, even if the app and the data used in it are temporary.

Furthermore, the 'Ethical analysis of the COVID-19 notification app in addition to the GGD source- and contact tracing' states that further measures are needed in order to

prevent improper use, including the stigmatisation of users and non-users. However, the ethical analysis does not yet pay attention to the risks associated with profiling.

It is unclear whether citizens will be asked for permission for data to be used anonymously. With the existing Corona Check app[5], the app builder (a private party) asks, for example, for permission to use data in order to improve certain 'services'. However, anonymising does not mean that profiling is not possible. Even if the data is destroyed or anonymised, person-sensitive information may continue to exist and (groups of) citizens may be subject to disadvantage or harm. Based on information received from the COVID Radar, for example, the LUMC hospital in Leiden, the Netherlands, conveys which postcode areas in the city of Leiden have a greater risk of contamination. This can stigmatise a particular neighbourhood.

The House of Representatives can ask the Cabinet whether parties other than those mentioned in the DPIA request access to data, and if so, for what purpose.

The House of Representatives can ask the Cabinet what measures it is taking to counter the threat posed by profiling and stigmatisation, not only looking at the app, but also at the entire broad context of its use or non-use.

**6. Complaints, objections, rebuttal, harm and redress**

The documents sent by the minister to the House of Representatives only deal with the data subjects' rights insofar as personal data is involved. However, there may be circumstances in which no personal data is processed, but a citizen nevertheless wants to submit a complaint or objection, wants to invoke a rebuttal or has been subject to harm. Part of this falls within the domain of the GGD, in the context of the treatment relationship, but in other situations it is unclear. For example, with regards to complaints about the app.

The House of Representatives can ask the Cabinet how rights that do not arise from the GDPR are implemented.

[5] https://decoronacheck.nl/