Summary: COVID-19 outbreak and data protection

The COVID19 outbreak will require some public health measures, which are under the responsibility of the competent national authorities, notably public health authorities, such as contact tracing. These authorities may ask EUIs to disclose information (including personal data) to them, which they then have to process in line with the applicable legislation.

These competent national authorities fulfil their task based on their mandates established by law (i.e. 6(1)(e) + 9(2)(i) GDPR for lawfulness of processing on their end). Disclosures in line with their mandates would seem to be justified under Article 9(1)(a) of Regulation (EU) 2018/1725.

There are three steps to consider here:

1. Why can competent national authorities collect and request information, including personal data?
2. Can EUIs disclose that information?
3. What happens afterwards?

While EUIs themselves are entitled to take some measures to protect their staff, they have to stay within the remit of their role as employers. This means that they should not try take over tasks that are properly in the remit of the competent national (public health) authorities. Therefore, we recommend you to remind your EUI management of the data protection principles and the remit of their role.

You may want to consider the following:

4. Precautionary measures to be taken by EUI administration?
5. What is the role of your EUI's medical service here?

Finally, you will find further references to guidance by national DPAs and further reading at the end of this document.

1. Why can competent national authorities collect and request information, including personal data?

What is the basis for national competent (public health) authorities doing contact tracing, disease surveillance and similar activities?

Their tasks are laid down by law and within that mandate, these authorities are entitled to obtain certain information (see Articles 6(1)(e), 6(3), 9(2)(i) GDPR quoted below, emphasis added):

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

[…]

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

[…]

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

Article 9

Processing of special categories of personal data

1. Processing of […] data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

[…]

(i) **processing is necessary for reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, **on the basis of Union or Member State law** which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

Such disclosures are not a derogation from the rules of GDPR or a situation of force majeure, but use cases explicitly foreseen in it.

For further explanation, see also recital 54 GDPR:

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. […]. Such processing of data concerning health for

reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

2. Can EUIs disclose information to competent national (public health) authorities?

Regulation 2018/1725 has specific rules on disclosure of information to recipients other than EUIs. Requests that are within the mandate of competent national public health authorities can be assumed to fulfil these requirements (emphasis added):

Article 9

Transmissions of personal data to recipients established in the Union other than Union institutions and bodies

1. Without prejudice to Articles 4 to 6 and 10, personal data shall only be transmitted to recipients established in the Union other than Union institutions and bodies if:

(a) the recipient establishes that the data are **necessary for the performance of a task carried out** in the public interest or in the exercise of official authority vested in the recipient; or

[…]

Disclosures fulfilling this requirement will be lawful.

EUIs should ascertain that the requester in fact has that authority and document disclosures made for accountability purposes.

3. What happens afterwards?

Competent national authorities to which EUIs have disclosed information, including personal data, have to process them in line with the applicable legislation. This means GDPR and the legal acts assigning these tasks to competent authorities apply to their further processing.

The competent authorities are separate controllers from the EUIs here. Retention periods, data subject rights etc. follow the procedures adopted by the competent authorities. The relevant national DPA supervises their compliance with GDPR.

4. Precautionary measures to be taken by EUI administration?

While EUIs can of course take reasonable precautionary measures, the general principles of necessity and proportionality still apply when exercising their duty of care for staff.

EUIs are accountable for necessity and proportionality. EUIs should limit their processing to what is necessary. If in doubt, check with your DPO.

As with any processing of personal data, the EUIs are accountable for applying adequate security measures for the protection of the confidentiality of the information and shall apply encryption or pseudonymisation techniques whenever needed. Especially, due care has to be taken for the protection of the electronic transmission of sensitive information.

To give some practical examples, an EUI may think that it would be good to know where staff intend to go while on leave (to not approve leave meant for going to certain areas and to know where people have been before returning). However, you can get basically the same effect by instructing staff to check whether the place they have been has changed status and to stay at home if it has been declared a risk zone in the meantime. Also in times of crisis, think of data protection by design: do you need that information? Can you get the same effect collecting less information?

Other measures are clearly disproportionate: e.g. obliging all staff to regularly disclose detailed health status information to their employer's medical service. **Such updates are for the treating physician only**, not for the employer.

Of course, there are plenty of precautionary measures that do not lead to this kind of additional processing: providing hand sanitiser, encouraging telework etc.

As always, purpose limitation applies. Personal data collected for these specific purposes should not be used for another purpose. Nothing can be made public without the consent of the data subjects, unless disclosure to e.g. public health authorities is required by law.

5. What is the role of your EUI's medical service here?

Your medical service is well-placed to provide guidance on preventive measures internally. However, keep in mind that your EUI's medical is not the primary care provider for your staff. Staff (suspected of being) infected of course have to cooperate with their care provider and competent national (public health) authorities**. Following the evolution of the case is the task of the treating physician.** If another EUI provides medical services to you under a SLA or similar, the same applies. It may make sense to have a reminder to the medical service providing these services to your EUI.

6. Further references

Some national DPAs have published guidance on data protection aspects of public health responses to COVID-19:

- Denmark: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/hvordan-er-det-med-gdpr-og-coronavirus/

- Ireland: https://dataprotection.ie/en/news-media/blogs/data-protection-and-covid-19
- Italy: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9282117
- France: https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles
- The Netherlands : https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/mijn-zieke-werknemer#mag-ik-mijn-werknemers-controleren-op-corona-7633
- Luxemburg: https://cnpd.public.lu/fr/actualites/national/2020/03/coronavirus.html

For general information on public health surveillance, see also:

- WHO Guidelines on ethical issues in public health surveillance https://www.who.int/ethics/publications/public-health-asurveillance/en/