
Hughes Hubbard & Reed

The EDPB and the CNIL Release Guidance on Processing Personal Data in the Workplace during the COVID-19 Outbreak

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

Attorney advertising. Readers are advised that prior results do not guarantee a similar outcome. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. For information regarding the selection process of awards, please visit <https://www.hugheshubbard.com/legal-notice-methodologies>.

April 20, 2020 - Over the last few weeks, organizations in France and across the EU have been implementing measures to ensure business continuity and safeguard employment while applying the general rules on processing personal data in the context of the covid-19 outbreak.

The European Data Protection Board (EDPB) and the French Data Protection Authority (CNIL) have released practical guidance for employers on how to implement GDPR-compliant measures. The EDPB plans to issue additional guidance later this week on teleworking and the CNIL plans to update its guidance according to current events.

Guidance from the EDPB

- **Overall guidance**

The EDPB recommends relying on GDPR core principles (lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality), and emphasizes it is important to adopt adequate security measures and confidentiality policies ensuring that personal data is not disclosed to unauthorized parties and to document measures implemented “to manage the current emergency and the underlying decision-making process [for GDPR compliance]”.

To find out whether or not they are entitled to request health information from employees (and visitors at the end of the health emergency period in France) or to perform medical check-ups on employees, the EDPB specifically recommends employers only process personal data that is necessary to fulfill their duties and organize work in line with national legislation, in accordance with the GDPR principles of proportionality and data minimization.

- **Lawfulness of the processing**

The EDPB indicated that the GDPR enables employers to process personal data, including health data, in the context of epidemics without the need to obtain the consent of the data subject and notably that:

- the legal base of the processing is the necessity of:
 - . complying with a legal obligation when the processing is necessary for the employer to comply with the law (such as obligations relating to health and safety in the workplace) (Article 6 of the GDPR), and
 - . protecting vital interests when the processing is necessary to protect someone's life (Article 6 of the GDPR), and;
- the exception to the prohibition to process health data being the necessity of processing such data for reasons of public interest in the area of public health (such as the control of diseases and other threats to health) (Article 9 of the GDPR).

Guidance from the CNIL

On April 17, 2020, the CNIL published a statement on its website concerning the impact of the covid-19 outbreak on its audits and sanctions procedure.

With regard to its investigation procedure, it states that during the health emergency period:

- only those situations whose seriousness requires urgent investigations will be subject to inspections, including online inspections;
- organizations have extended time limits to respond to requests for additional information following an investigation;
- the deadlines for complying with a formal notice have been suspended until June 24, 2020, for formal notice whose deadline had not expired by March 12, 2020, and the starting point for taking measures to ensure compliance has been postponed until June 24, 2020, for formal notices sent after March 12, 2020.

As for sanctions proceedings, the CNIL has specified that organizations that had been expected to provide their observations during the period between March 12 and June 24, 2020, now have until August 24, 2020 to provide their observations and comments.

Nevertheless, the CNIL has pointed out that all of these deadlines may be tightened, while taking into account the constraints relating to the current health emergency, when the interests it is responsible for protecting justify such action (for example, in the event of a serious violation of the rights of individuals or the legal framework in force or to ensure that such violations cease).

- **Measures to limit the spread of the virus**

The CNIL indicates that employers may:

- invite employees to report any suspicions directly to the employer or to the health authorities and, to this end, set up dedicated information channels and, in the event of a report, record the date, the identity of the person suspected of being exposed to the virus and the organizational measures taken,
- promote remote working methods and encourage the use of the occupational health service,
- communicate to the health authorities, upon request, information related to the nature of the exposure;

and they may not:

- collect data beyond management of suspected exposure to the virus,

- collect, in a systematic and generalized way or through surveys or individual requests, data relating to searches for possible symptoms presented by the employee or his or her relatives (in particular through compulsory body temperature readings or medical questionnaires).

The CNIL also recalled that employees are required to inform their employer in cases of suspicion of contact with the virus.

- **Measures to enable home and remote working**

The CNIL recommends employers to:

- secure the IT system by communicating a security charter for remote working with the minimum rules to be respected,
- measure the risks involved and take the necessary measures to remedy them if the introduction of remote working requires a change in management rules such as authorizations,
- equip all workstations with a firewall, antivirus software and a tool for blocking access to malicious sites at the very least, and
- implement a VPN network with two-factor authentication processes to avoid direct exposure of services on the Internet.

For employers whose services are on the Internet, the CNIL recommends (1) using protocols that guarantee confidentiality and authentication of recipient servers, (2) using the most recent versions of protocol, (3) applying the latest security patches (by regularly consulting the CERT-FR news bulletin), (4) implementing two-factor authentication mechanisms on remotely accessible services to prevent intrusions (by regularly consulting access logs for remotely accessible services) to detect suspicious behavior, (5) and not making unsecured server interfaces directly accessible.

- **Videoconferencing tools**

The CNIL recommends that users:

- before downloading:
 - . use only those applications that ensure confidentiality of data, do not use the data for other purposes, and ensure compliance with the GDPR rules and protect privacy,
 - . read the terms of use carefully,
 - . check the implementation by the publisher of security measures such as end-to-end encryption of the communication,
 - . secure Wi-Fi with a complex password by activating WPA2 or WPA3 encryption,
 - . make sure the antivirus and firewall are up to date, and;
- when registering for the service:
 - . limit the amount of information provided at registration,
 - . use a nickname, a dedicated email address and a password different from those used on other online services, and;
- when using the service:
 - . look at the privacy settings,
 - . close the application, microphone and webcam after use.

Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak, March 16, 2020; Statement by the EDPB on the processing of personal data in the context of the COVID-19 outbreak. Adopted on March 19, 2020; Coronavirus (covid 19): les rappels de la CNIL sur la collecte de données personnelles, March 26,

2020; Les conseils de la CNIL pour mettre en place le télétravail, April 1, 2020; Covid-19: les conseils de la CNIL pour utiliser les outils de visioconférence, April 9, 2020.

[Click here to go to our COVID-19 Resource Center for more advisories, articles and other content related to the coronavirus pandemic.](#)

Related People



Stefan Naumann



Elsa Malaty

Related Areas of Focus

[Data Privacy & Cybersecurity](#)