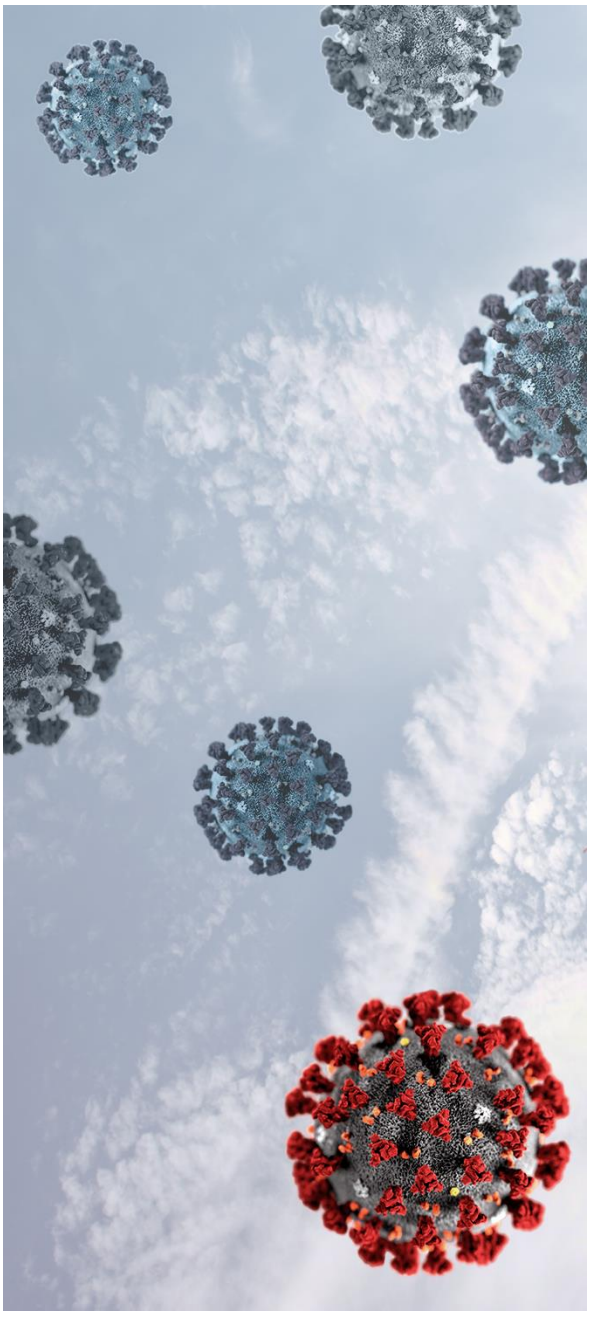
CUATRECASAS

COVID-19: New developments in data protection

Newsletter | Portugal

May 20, 2020



- CNPD guidelines on remote work monitoring
- CNPD guidelines on disclosing information on people infected with COVID-19
- CNPD guidelines on collecting workers' health data
- CNPD guidelines on using remote teaching technologies
- CNPD guidelines on collecting students' health data
- CEPD guidelines on using location data and contact tracing tools in the COVID-19 outbreak
- Cybersecurity best practices for remote working published by the Portuguese National Cybersecurity Center

I. CNPD guidelines on remote work monitoring

With the lockdown and social distancing measures, working remote has become the norm.

Under regular circumstances, the work tools used by remote workers belong to their employer. Workers must follow the rules for use and operation of the work instruments made available to them and can only use them to do their work, unless otherwise agreed.

However, the exceptional nature of the current situation has prevented employers from making technological resources available to most of their workers, so the tools they use often belong to them.

Regardless of who owns the work tools in remote work, the employer retains the right to manage and monitor work. However, given that this system does not regulate remote monitoring, the Portuguese National Data Protection Authority (CNPD) states that "*the general rule prohibiting the use of remote means of surveillance to monitor workers' professional performance fully applies to remote work.*" This conclusion arises from applying the principles of proportionality and minimization of personal data.

The CNPD emphasizes that technological solutions to monitor workers' performance are not allowed, including "*any software that, other than monitoring working and inactive time, registers the Internet sites viewed, the location of the terminal in real time, the use of peripheral devices (mouse and keyboard), captures images of the work environment, watches and records when an application is accessed, monitors the document that is being worked on, and records the time spent on each task.*"

In the CNPD's view, these tools collect too many of the workers' personal data, making it possible to monitor work much more closely than allowed in face-to-face work at the employer's facilities. This data collection and processing breaches the principle of minimizing personal data.

However, the CNPD states that the employer can exercise its right to monitor the worker's activity in other ways, e.g., setting targets, establishing mandatory periodical reporting or scheduling video calls.

The working time recording solutions must be limited to reproducing the record taken when the work is done at the employer's facilities (i.e., recording the start and end of working hours and the lunch break). As these tools are not available, it is legitimate, on an exceptional basis, for employers to make it mandatory to send emails, SMS messages, or any other means that makes it possible, in addition to monitoring the worker's availability and working hours, proving that the maximum working hours allowed by law were not exceeded.

II. CNPD guidelines on disclosing information on people infected with COVID-19

The health authorities daily disclose and make available information on the total number of suspected and confirmed COVID-19 cases, as well as on recoveries and deaths in Portugal.

The data published by the Directorate General for Health ("DGS") is for municipal councils, which publish information on their territories for the peace of mind of the population.

Regarding these publications, the CNPD has received complaints from individuals whose identification and personal contact data, including that of children, has been published on the local authorities' websites and social media, after confirmation of their COVID-19 diagnosis.

The CNPD has informed that local authorities are not entitled to publish health data identifying the individuals concerned.

"*This information is subject to a specially protected legal system, as it belongs to a personal data category that can generate or foster stigmatization and discrimination toward the data subjects.*" Even though local authorities argue that health data must be known and disclosed to guarantee the health and civil protection of the population, this data processing requires regulation allowing it and specifically establishing the data subjects' rights and interests. Such legal provision does not exist.

Another legitimate basis for this data processing is the data subjects' consent, which, however, can be hardly verified in this context. In fact, given the vulnerable situation of those infected by the virus and their dependency on the public authorities, the conditions for them to give their free consent are not there.

The CNPD states that "*such public disclosure will always be regarded as disproportionate because of the negative impact that it has on the lives of infected people - some of whom, we must repeat, are children - excessively restricting their fundamental rights. It cannot be stated that the benefit directly generated by such disclosure, if any, cannot be achieved by other means that are less intrusive and harmful to privacy.*"

Likewise, health data cannot be published, even if the patients are not identified, when the small number of cases in a specific territory makes it possible, because of the size of its population, to identify the infected individuals.

Local authorities must thus refrain from adopting initiatives that involve collecting and disclosing people's personal data when they do not have a legal basis to do it or when they do not follow the national health authority's guidelines.

III. CNPD guidelines on collecting workers' health data

Employers have adopted measures to prevent infection among their workers, e.g., collecting and recording data on the health and personal life of those susceptible to infection by the virus, such as the workers' bodily temperature.

The CNPD states that "*personal data pertaining to health are sensitive data disclosing aspects of the worker's personal life that need not or should not be known by the employer as they may generate or foster discrimination.*" This data category is subject to a specially reinforced data protection scheme, by which the employer does not know and cannot directly record or collect workers' health data.

Although this exceptional situation has caused deep changes in the work context and in the employer-worker relationship, the need to prevent infection by the virus is not in itself a legitimate basis for the employer to adopt just any measure.

Infection prevention may justify the intensification of hygiene and the adoption of organizational measures pertaining to the distribution of workers' space and physical protection. However, "*it does not justify any actions that, under Portuguese law, can only be performed by the health authorities, or by the worker in a self-monitoring process.*"

The CNPD states that employers cannot take and record their workers' body temperature or any other information pertaining to their health and potentially risky behavior.

However, a health care professional in the field of occupational medicine can assess the workers' health condition by getting information on their health and personal life through worker-completed questionnaires.

In response to the publication of these Guidelines, the Assembly of the Portuguese Republic sent a parliamentary request to the CNPD for clarification. In its answer, the CNPD restated its position on taking workers' temperature and emphasized the following:

- Processing of health data in employment relationship, based on the worker's consent, is incompatible with the fundamental right to the protection of data and privacy established in the Constitution of the Portuguese Republic and the European Union Charter of Fundamental Rights.
- Section 13-C of Decree Law 10-A/2020 of March 13, amended by Decree Law 20/2020 of May 1, establishing the possibility for employers to take their workers' bodily temperature, does not establish adequate measures to protect the data subjects' rights, freedoms, and guarantees that the General Data Protection Regulation ("GDPR") requires Member States to provide.
- Processing health data based on the public interest as established in Section 9.1.i) and h) of the GDPR (approved by Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016) must be preceded by a national or EU law determining the legal

conditions for processing and establishing adequate measures for the protection of the data subjects' rights and freedoms.

IV. CNPD guidelines on using remote teaching technologies

The CNPD has published guidelines aimed at all the parties involved in processing data taken in schools, be they teachers, students, parents, or guardians, as well as the entities acting as data controllers and their subcontractors.

The CNPD specifies a long list of personal data processed by remote learning technologies: recording all voice and image of all the involved and of third parties, images of the inside of the room, data included in shared documents and in verbal statements made in video calls, as well as information included in messaging and forums.

As regards teaching platforms, data on platform use (metadata) are collected or can be collected, e.g., the time spent on the platform, the number of courses taken, whether the student has passed, as well as personal data inferred from these: intellectual ability, learning difficulties, personality traits, health data associated with intellectual abilities and concentration.

According to the CNPD, the use of these platforms entails various risks, in particular:

- Undue use of the data collected by the platforms, either by the data controllers or by their subcontracts, in particular, providers of cloud computation services;
- Lack of transparency in data storage within the potential subcontracting of cloud computation service providers, resulting on the data subjects loss of control;
- Discrimination based on profiles or assessments, in particular through the making of automated decisions by learning analytics systems that examine student performance;
- Use of comnunication platforms that do not guarantee the security of communications, or incorrect settings resulting in unauthorized disclosure or access;
- Lack of confidentiality when sharing computers;
- Loss of responsibility of schools and platforms, in the absence of a clear attribution of responsibilities in use of these technologies;
- Remote surveillance to monitor teachers' professional performance (see the above Guidelines on remote work monitoring); and
- Unfeasibility of the exercise of rights by data subjects regarding the platforms.

To mitigate these risks, the CNPD recommends that suitable measures for the technologies employed be applied, in particular:

- Adoption of each remote learning platform must be preceded by an assessment of its impact on data protection so as to properly identify the risks to privacy and enable the adoption of measures to mitigate these risks. The assessment can be conducted by the entities that provide and manage the platforms;
- Teachers must be duly informed regarding the use of the platforms. In particular, they must be able to identify the suitable settings to ensure that their use does not pose any risks to the users' privacy, focusing especially on students; and
- Whenever possible, using technologies that involve the least exposure possible for the data subjects and their family environment (e.g., discussion forums as opposed to a video call).

The use of any performance analysis algorithm (learning analytics) must always be carefully considered and implemented in a manner that is fair and transparent for data subjects, and only if the conditions for the lawfulness of that processing are met.

It should be emphasized that no educational establishment can impose the use of a specific artificial intelligence technology on its students. Such use requires free, specific, and informed consent by the students or, if they are minors, by their parents or guardians.

Data subjects must be given clear information about the use of analysis algorithms, in particular when they involve automated decisions. The data subject's right to human involvement in that process must always be guaranteed.

V. CNPD guidelines on collecting students' health data

With schools reopening and classes restarting, many schools have started to take their students' temperature when entering their facilities.

In line with the various public statements on the processing of health data in the COVID-19 pandemic, the CNPD provides that educational establishments, in their capacity as data controllers, must meet the strict requirements for collection of health data (sensitive data).

The CNPD also states that the reopening of schools, under Decree Law 20-H/2020 of May 14, does not require taking students' bodily temperature, inasmuch as there are no guidelines from the Directorate General for Health on the need or usefulness of doing so.

The CNPD emphasizes the need to follow the general principles for data processing, in particular the existence of an adequate legal basis for the processing, as follows:

- Educational establishments must prove that there is a legal basis, under articles 5 and 9 GDPR, for the processing of sensitive data. Merely invoking third parties' legitimate interests will not suffice, given that the point is to prove that these legitimate interests prevail over the rights of the data subjects, in particular of minors.

- Based on the arguments above, public schools cannot claim that the processing is required for exercising public interest functions as stated in article 9.1.e).

- The CNPD finds that "*consent from the students or* their guardians *can only be the basis of the processing if there is no threat or communication that the students' refusal to have their temperature taken will have the negative consequence of the student being prevented from entering a classroom, and thus from receiving the teaching required for their preparation for assessment*."

- The lawfulness of the processing cannot be based on school regulations, as the autonomy of schools does not allow the restriction of rights, freedoms, and guarantees without a qualifying legal act, in particular the right to the protection of personal data and privacy protected by the Constitution of the Portuguese Republic and the GDPR.

- Even if the school can prove that there is a legal basis, the data controllers must prove that the processing is necessary, to the extent that it is the least intrusive regarding the data subjects' rights in comparison to other available options.

VI. CEPD guidelines on using location data and contact tracing tools in the COVID-19 outbreak

According to the European Union Commissioned for Health, Stella Kyriakides, the fight against the COVID-19 pandemic through digital applications will follow the "global gold standard," namely the European values and legislation protecting fundamental rights, in particular privacy and data protection.

The European Data Protection Board ("EDPB") issued Guideline 4/2020 on the use of location data and contact tracing tools in the COVID-19 outbreak on April 21, 2020.

The guideline is intended to clarify "*the conditions and principles for the proportionate use of location data and contact tracing tools, for two specific purposes:*

- *using location data to support the response to the pandemic by modelling the spread of the virus to assess the overall effectiveness of confinement measures; and*

- *contact tracing, which aims to notify individuals that they have been in close proximity of someone who is eventually confirmed to be a carrier of the virus, in order to break the chains of infection as early as possible.*

The EDPB points out that it has already positioned itself regarding the processing of geolocation data collected by electronic communication service providers, stating that such data must be previously anonymized.

Processing location data directly collected from users' devices will only be lawful if the users' previous consent is given, or when processing is strictly necessary for the information society service explicitly requested by the user (e.g., use of a mobile app).

The EDPB considers the concept of data anonymization, its legal and technical implications, and concludes that "*Many options for effective anonymisation exist, but with a caveat. Data cannot be anonymised on their own, meaning that only datasets as a whole may or may not be made anonymous. Any intervention on a single data pattern (by means of encryption or any other mathematical transformation) can at best be considered a pseudonymisation.*"

The EDPB also emphasizes that systematic, large-scale monitoring of location and contact between individuals "*can only be legitimised by relying on the voluntary adoption by the users for each of the respective purposes*." Thus, imposing the use of this technology on citizens is not considered lawful. The EDPB states that these apps should operate within a logic of privacy by default, in compliance with the principle of limitation of purpose and data minimization.

The parties involved should also consider that there may be a legitimate basis for data processing that overrides consent, such as the public interest sought by public authorities, as provided in European and Member State legislation.

Finally, the EDPB underlines that "*procedures and processes including respective algorithms implemented by the contact tracing apps should work under the strict supervision of qualified personnel to limit the occurrence of any false positives and negatives. In particular, the task of providing advice on next steps should not be based solely on automated processing*."

The EDPB has also provided a number of technical recommendations and guidelines for developing apps that comply with the principle of privacy by default.

VII. Cybersecurity best practices for working remote published by the Portuguese National Cybersecurity Center

The Portuguese National Cybersecurity Center published its "Cybersecurity best practices for working remote," which should be considered by organizations and companies whose workers are working remotely.

https://www.cncs.gov.pt/recursos/boas-praticas/

Contact

Cuatrecasas, Gonçalves Pereira & Associados,
Sociedade de Advogados, SP, RL
Sociedade profissional de responsabilidade limitada

Lisbon
Praça Marquês de Pombal, 2 (e 1-8º) I 1250-160 Lisbon I Portugal
Tel. (351) 21 355 3800 I Fax (351) 21 353 2362
cuatrecasasportugal@cuatrecasas.com I www.cuatrecasas.com

Oporto
Avenida da Boavista, 3265 - 5.1 I 4100-137 Oporto I Portugal
Tel. (351) 22 616 6920 I Fax (351) 22 616 6949
cuatrecasasporto@cuatrecasas.com I www.cuatrecasas.com

Cuatrecasas has set up a Coronavirus Task Force, a multidisciplinary team that constantly analyzes the situation emerging from the COVID-19 pandemic. For further information on the contents of this document, please contact our Task Force by email at TFcoronavirusPT@cuatrecasas.com or through your usual contact at Cuatrecasas. You can read our publications or attend our webinars on our *website*.

Information about the processing of your personal data.

Data Controller: Cuatrecasas, Gonçalves Pereira & Associados, Sociedade de Advogados, SP, RL ("Cuatrecasas Portugal").

Purposes: management of the use of the website, of the applications and/or of your relationship with Cuatrecasas Portugal, including the sending of information on legislative news and events promoted by Cuatrecasas Portugal.
Legitimacy: the legitimate interest of Cuatrecasas Portugal and/or, where applicable, the consent of the data subject.
Recipients: third parties to whom Cuatrecasas Portugal is contractually or legally obliged to communicate data, as well as to companies in its group.
Rights: access, rectify, erase, object to, request the portability of your data and/or restrict its processing, as described in the additional information. For more detailed information on how we process your data, please go to our data protection policy.

If you have any questions about how we process your data, or if you do not wish to continue receiving communications from Cuatrecasas Portugal, please send a message to the following email address data.protection.officer@cuatrecasas.com.