COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Joint Statement

on the right to data protection in the context of the COVID-19 pandemic

by Alessandra Pierucci, Chair of the Committee of Convention 108

and

Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe

Strasbourg, 30 March 2020

The COVID-19 pandemic (more commonly known as Coronavirus) poses unprecedented threats and challenges for individuals, and countries around the world. The need to stop its spread and cure those who are suffering is a prominent goal shared by nations globally.

The efforts deployed by the World Health Organisation, other international organisations, governments, health-care institutions and their staff as well as businesses to prevent an even larger scale propagation of the virus, to save people, and protect the society are limitless and should be strongly supported.

States have to address the threat resulting from the COVID-19 pandemic in respect of democracy, rule of law and human rights, including the rights to privacy and data protection.

In the effort of curbing the number of new contaminations, governments have had to resort to extraordinary measures, including the declaration of a state of emergency in many cases. While the alarming public health situation of those countries has justified the introduction of specific regimes, it should be stressed that, during those limited periods, the exercise of human rights, as enshrined in several international (such as the International Covenant on Civil and Political Rights and the European Convention on Human Rights) and national instruments is applicable and cannot be suspended but only derogated or restricted by law, to the extent strictly required by the exigencies of the situation while respecting the essence of the fundamental rights and freedoms.

General data protection principles and rules

When it comes to the right to data protection, it should first of all be noted that Convention 108, as well as the modernised "Convention 108+", set forth high standards for the protection of personal data which are compatible and reconcilable with other fundamental rights and relevant public interests.

It is important to recall that data protection can in no manner be an obstacle to saving lives and that the applicable principles always allow for a balancing of the interests at stake.

In accordance with Convention 108+ it is crucial, that even in particularly difficult situations, data protection principles are respected and therefore it is ensured that data subjects are made aware of the processing of personal data related to them; processing of personal data is carried out only if necessary and proportionate to the explicit, specified and legitimate purpose pursued; an impact assessment is carried out before the processing is started; privacy by design is ensured and appropriate measures are adopted to protect the security of data, in particular when related to special categories of data such as health related data; data subjects are entitled to exercise their rights.

One of the main data protection principles provided for by Convention 108+ is the principle of lawfulness, according to which processing of data can be carried out either on the basis of the data subject's consent or some other legitimate basis laid down by law. It should be noted that, as explicitly provided by the Explanatory Report to Convention 108+, such legitimate basis notably encompasses data processing necessary for the vital interests of individuals, and data processing carried out on the basis of grounds of public interest, such as in the case of monitoring of life-threatening epidemic.

The right to data protection for instance does not prevent public health authorities to share the list of health professionals (names and contact details) with entities tasked with the distribution of FFP2 masks. Neither can the right to data protection be claimed to be incompatible with epidemiologic monitoring, stressing that anonymised data is not covered by data protection requirements. The use of aggregate location information to signal gatherings infringing confinement requirements or to indicate movements of persons traveling away from a severely touched area (in terms of number of COVID-19 positive persons) would thus not be prevented by data protection requirements.

Furthermore, "Convention 108+" acknowledges the need to allow some exceptions and restrictions in the name of pressing objectives of public interest and individuals' vital interests. Nevertheless, restrictions to its principles and rights must respond to very clear requirements, even during the state of emergency, to ensure the persisting respect of the rule of law and fundamental rights.

According to Convention 108+ (see Article 11) exceptions shall be "*provided for by law, respect the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society*".

Where restrictions are being applied, those measures have to be taken solely on a provisional basis and only for a period of time explicitly limited to the state of emergency. It is also crucial that specific safeguards are put in place and that reassurances are given that full protection are afforded to personal data once the state of emergency is lifted. This should include concrete measures and procedures regarding the return to "normal" data processing regimes, with special attention to data bases containing health-related data or other special categories of data and/or to those created for the purpose of tracking, following, and profiling individuals, whose processing was performed during the state of emergency.

Data protection authorities are invited to carefully assess the measures taken by state authorities against those conditions.

Processing of health-related data

Provided that the primacy of the human being and the adoption of professional standards are guiding values in the field of health treatment, the processing of health-related data shall guarantee respect for the rights and fundamental freedoms of every individual, in particular the rights to privacy and to protection of personal data. Recommendation CM/Rec(2019)2 regarding health-related data provides specific guidelines in this regard. Its provisions on the sharing of data between health professionals and between health and other sectors should, in particular, guide the practices of professionals concerned.

Communication to the public by health and government authorities should remain a priority to be in a capacity to protect, inform and advise the public. Nonetheless, during such communications, the publication of sensitive data (such as the health-related data) of specific individuals should be avoided and it is recommended that the processing of such data is only done, if additional technical and organisational measures that are complementing those applied to non-sensitive data are put in place.

Large-scale data processing

Since massive data and data bases are generated, seizing the benefits of data processing techniques and technologies such as Big Data or Artificial Intelligence, that data should be processed in such environments in a way that respects human dignity and data protection. The respective guidance developed by the Committee of Convention 108 in the context of Big Data and Artificial Intelligence can be useful tools for developers as well as governments to shape those processing in a way that safeguards against voluntary misuse or unintended negative consequences, including the discrimination of individuals or groups of individuals.

Transparency and "explainability" of analytics or AI solutions, a precautionary approach and a risk management strategy (including the risk of re-identification in the case of anonymised data), a focus on data quality and minimisation, and the role of human oversight are some of the key points to take into account in the development of innovative solutions to fight against COVID-19.

Data processing by employers

Employers are facing difficulties in maintaining their business or activity while protecting the public and their staff, very often having their employees teleworking. This practice however should not lead to the monitoring of employees, including by video means; non-intrusive measures are to be thought when organising the work and working conditions.

In the given circumstances, employers may have to process personal or sensitive data that they usually do not process (such as health-related data); therefore it should be recalled that when doing so, they should respect the principles of necessity, proportionality and accountability and should also be guided by principles designed to minimise any risks that such processing might pose to employees' rights and fundamental freedoms, in particular their right to privacy as elaborated in Recommendation CM/Rec(2015)5 on the processing of personal data in the context of employment. In particular, employers should not process personal data beyond what is necessary to the identification of potentially exposed employees.

If they are required by law to disclose certain data to state authorities for public health reasons, they are invited to do so in strict compliance with the underlying legal basis, with a view to take the necessary measure to return to "normal" processing (including permanent deletion) once the state of emergency regime is no longer applicable.

Mobile, computer data

Telecommunication companies, online platforms and internet service providers are also actively involved in the fight against the spread of COVID-19 and are increasingly required to share subscriber data, personal information they collect and other types of information with public authorities to notably contribute to epidemic surveillance, including the analysis of spatial data to determine the location of possibly infected people. Similarly, private and public bodies can develop IT solutions for epidemic surveillance.

Large-scale personal data processing can only be performed when, on the basis of scientific evidence, the potential public health benefits of such digital epidemic surveillance (e.g. contact tracking), including their accuracy, override the benefits of other alternative solutions which would be less intrusive.

The development of these surveillance solutions should be based on a prior assessment of the likely impact of the intended data processing on the rights and fundamental freedoms of data subjects, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

In light of the precautionary and proportionality principles, pre-tests in various "sandboxes" should also be recommended, as is currently the case with various possible medications being tested in clinical trials.

While real-time information on the spread of the virus can be instrumental in isolating it, it must be stressed that the least intrusive solutions should always be preferred.

Data processing in educational systems

Schools and universities are deploying all possible efforts to increase distance learning skills and resources, with professors and teachers themselves facing the challenge of being isolated. When considering the technical solutions aimed at ensuring the continuity of the educational work, data protection-oriented standard configurations should be preferred, for instance regarding the default settings, so that the usage of applications and software does not infringe the rights of the data subjects (data protection by default) and to avoid processing more data than necessary to achieve the legitimate purpose of ensuring educational continuity.

It is also of primary importance that a proper legal basis is chosen (including the approval by parents or legal guardian where necessary) and that parents benefit from a maximum of transparency regarding the processing of their children's data.

Additional guidelines[1] regarding the processing of personal data in the context of education are currently being elaborated by the Committee of Convention 108 and will serve for practitioners and decision makers.

* *
*

While people are facing difficult and threatening times, while the situation evolves rapidly and governments take measures to protect the population, they must do so without putting societies at greater risk on the longer term.

It is only with unity and solidarity, in full respect of the rule of law, human rights and democracy that we will overcome this unprecedented situation.

[1] Draft Guidelines: Children's Data Protection in Education Systems