EDPB KEEPS POSITION ON THE PROCESSING OF PERSONAL DATA IN THE CONTEXT OF THE COVID-19 EMERGENCE

SERGIO GUIDA

Independent Researcher, Sr.Data/Information Governance Mgr.

Key-words: ePrivacy - GDPR - geolocalizzazione - sensitive data

Category: Legal Area

Prohibition of entry into the EU from outside the Union for at least 30 day; the Stability and Growth Pact's rules that seem to be heading towards a long suspension; those on state aid that will be reviewed to give flexibility to member countries in the war on the coronavirus: Covid-19 has crossed European borders not even a month ago, coming to Italy arrogantly, and has already changed the connotations of the Union.

While governments, public and private organisations throughout Europe are taking measures to contain and mitigate COVID-19, the processing of different types of personal data could be heavily involved.

So the European Data Protection Board (EDPB) reminds that efforts to use geolocation data to carry out contact-tracing – indeed in the same way that some countries controversially plans to - would currently be unlawful under the ePrivacy Directive. But in certain circumstances, including matters of national and public security, member states are titled to introduce new laws that would override their existing interpretations of the directive.

In the statement, we read: "The national laws implementing the ePrivacy Directive provide for the principle that the location data can only be used by the operator when they are made anonymous, or with the consent of the individuals".

"The public authorities should first aim for the processing of location data in an anonymous way (i.e. processing data aggregated in a way that it cannot be reversed to personal data). This could enable to generate reports on the concentration of mobile devices at a certain location ("cartography")."

In practice, to identify groups of people who were breaking self-isolation rules law enforcement agencies could use aggregated location data, based on individuals' proximity to cell towers, but they

couldn’t use the data to find people who had come into close contact with those who had later tested positive.

The statement continues: “When it is not possible to only process anonymous data, Art. 15 of the ePrivacy Directive enables the member states to introduce legislative measures pursuing national security and public security.

“This emergency legislation is possible under the condition that it constitutes a necessary, appropriate and proportionate measure within a democratic society. If such measures are introduced, a Member State is obliged to put in place adequate safeguards, such as granting individuals the right to a judicial remedy.”

Substantially the ePrivacy directive tends to follow a pro-privacy agenda, like EU data legislation in general and similarly, it could be allowed to member states to maintain sovereignty when it comes to issues of national security.

About the GDPR, it “provides for the legal grounds to enable the employers and the competent public health authorities to process personal data in the context of epidemics, without the need to obtain the consent of the data subject.”

Andrea Jelinek, EDPB’s chair, affirms: “Data protection rules (such as GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. However, I would like to underline that, even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects. Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data.”

So, apparently, the EDPB statement’s main purpose is to remind that GDPR protections cannot simply be swept away even during a public health crisis.

“This is a warning to governments, health authorities and employers that while they can process biometric and health data without consent, this must be done proportionately, lawfully, and with safeguards in place.”

Not remarkably, in both the ePrivacy Directive and the GDPR it is emphasized that any exceptions to the general safeguards can only take place by respecting some precise fundamental precautions, among which proportionality stands out.

Effectively, starting from the fact that the huge data processing capacity allowed by technology causes a significant impact on each individual citizen's life and in line with the 2017 Necessity Toolkit, which had delimited the scope of the concept of the need for limitations to fundamental rights, the EDPS adopted in December 2019 new «Proportionality guidelines». Those rules further define the content and purpose of the rights guaranteed by the Basic Charter and by the GDPR,

developing a deep legal analysis aimed at creating a real proportionality test and practical tools to help assess the compliance of proposed EU measures that would impact the fundamental rights to privacy and the protection of personal data.

One last point: the phase of "proportionality in the strict sense" examines the effects of the legislative act, comparing and weighing the benefits deriving from the pursuit of the objective to which the legislator aims and the costs, that is, the sacrifices that it imposes on others rights and interests at stake. It is the most delicate evaluation already normally, that's why in practice the risk that the necessary serenity of judgment may be affected by the urgency to use as soon as possible pervasive but effective technological tools to limit so contagious pandemics as COVID-19 must be carefully weighed.

Source: European Data Protection Board (EDPB).

Link: https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en