Data crossing borders

Christopher Kuner 2020-04-15T16:21:16

The coronavirus pandemic presents challenges at both national and global levels. Countries are currently focusing their efforts on threats to their own economies and social systems. However, international cooperation and consideration of cross-border issues are crucial to containing and ultimately overcoming the virus.

Some countries outside Europe (such as Israel and South Korea) have implemented measures involving the collection, processing, and transfer of personal data to fight the spread of coronavirus, and both the European Union and many Member States have indicated an interest in doing the same. Such measures often require that data be shared across national borders, such as by establishing data sharing platforms for research data and enabling the worldwide tracking of mobile phone users.

The cross-border sharing of personal data raises questions under the EU General Data Protection Regulation 2016/679 (the GDPR), which is the main EU legislation dealing with data protection and has had influence around the world. The GDPR requires a legal basis for the transfer of personal data to third countries, which also applies to measures taken to fight the pandemic.

Many academics, data protection authorities (DPAs), and public bodies have opined on privacy issues related to coronavirus, but have thus far devoted less attention to questions about the transborder sharing and transfer of personal data. For example, guidance published by DPAs (such as the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EPDS)) focus mainly on issues of national significance (such as those arising under national employment law) or on technical questions (such as the use of mobile applications for contact tracing).

There are many issues relevant to the global sharing of personal data to combat coronavirus, only two of which will be dealt with here. The first question is whether EU data protection law is flexible enough to allow the international sharing of personal data to fight the pandemic. Secondly, data protection law has traditionally been shaped by pivotal events in history (think of the effect that the reaction to the terrorist attacks of 11 September 2001 had on data protection law), and one can ask what implications the crisis will have on the future development of data transfer regulation.

Global data sharing under the GDPR

The GDPR provides three possible legal bases for data transfers, namely 1) formal adequacy decisions of the European Commission covering third countries or international organisations (Article 45); 2) appropriate safeguards (such as protections provided for by contractual clauses, or legally-binding instruments between public authorities) (Article 46); or 3) derogations for specific situations

(Article 49). The first two categories are likely to be of more limited use in the present crisis, at least in the short term, and will not be discussed further (for a discussion of adequacy decisions and coronavirus, see here).

Applying the derogations is the easiest way to provide a legal basis for data transfers, as long as the conditions for their use are fulfilled. The two derogations most relevant to fighting the pandemic are when the data transfer is necessary for important reasons of public interest (Article 49(1)(d) GDPR) or when it is necessary to protect the vital interests of the data subject or of other persons (Article 49(1)(f) GDPR). The recitals to the GDPR confirm that these derogations can cover situations such as the monitoring of epidemics and their spread (Recital 46) or contact tracing for contagious diseases (Recital 112).

These derogations are designed to be used under restrictive conditions. For example, the public interest derogation is only available with regard to an interest recognized by EU or Member State law (Article 49(4) GDPR). Moreover, as the CJEU has held several times (e.g., *Schrems*, Case C-362/14, para. 92), derogations from data protection rights must be interpreted restrictively, which has led the DPAs to imply that the derogations may only be used when the transfers they cover are "occasional" and "non-repetitive" (see EDPB Guidelines 2/18, pp. 4-5). Such restrictions could create uncertainties about whether these derogations are available on an ongoing basis, which could limit their use. For example, transfers for purposes such as medical research, or those to humanitarian organisations providing aid to vulnerable individuals, may by their nature need to be continual and repetitive, since combatting the virus is an ongoing activity that will likely continue until a vaccine is developed and implemented around the world, which could take several years.

However, it is submitted that the derogations do provide sufficient flexibility to allow such data transfers. "Combatting serious cross-border threats to health" is an interest recognized by EU law at the constitutional level (see Article 168(1) TFEU), indicating that it should fall under the "public interest" derogation. Furthermore, as the EDPB recognizes in its guidance cited above (see p. 5), the terms "occasional" and "non-repetitive" do not appear in the text of the GDPR dealing with these two derogations. The CJEU has also emphasized that necessity is the crucial factor for determining whether a derogation may be used (i.e., limitation of its use to situations where there is a close connection between the derogation and the situation to which it is to be applied), not whether the transfer is occasional or non-repetitive. Particularly relevant in this regard is *Opinion 1/15* (paras. 179-180), where the CJEU upheld a provision of a proposed international agreement between the EU and Canada allowing the transfer of airline passenger (PNR) data to the Canadian authorities in cases where the transfer was necessary, "in exceptional cases", to protect the vital interests of data subjects (including because of "a significant public health risk"), since transfers would be limited to exceptional situations and there was a strict necessity requirement for them (the Court went on to invalidate the proposed agreement, but on other grounds). Necessity does exist in the present situation, given that cross-border data transfers are crucial to the very nature of the data processing activities designed to combat the virus.

However, widespread use of these derogations should only be allowed when the strict necessity requirement is satisfied, which should be determined under an evidence-based standard, i.e., whether under medical or scientific standards the transfer is necessary to find a solution for the pandemic. Any other approach would risk watering down the standards of the GDPR and making the derogations of Article 49 into the rule.

The GDPR also contains some unexplored possibilities upon which data transfers could be based. For example, Article 46(2) GDPR allows data transfers under approved codes of conduct and certification mechanisms based on binding and enforceable commitments, but thus far no such arrangements have been approved by the EDPB. The present crisis provides an opportunity for public authorities, NGOs, humanitarian organisations, medical research institutes, and others to propose a code of conduct and/or certification mechanism to provide protection for global data sharing to combat coronavirus; hopefully the parties could then work together with the DPAs to fast-track its approval. Such an initiative could make a significant contribution to protecting personal data transferred globally.

The future of data transfer regulation

Examining the issues from a broader perspective, one can ask what the long-term implications of the pandemic will be for the regulation of data transfers and global data sharing. While it is too soon to say for sure, two major trends can already be discerned.

First of all, there will be increased pressure to allow global data sharing for important reasons of public interest, in particular for the transfer of health-related and medical data to combat the virus, which will require development of a conception of the global public interest. DPAs around the world have accepted the need for increased global data sharing to combat the pandemic, but will have to perform a difficult balancing act so as to be seen not to hamper the fight against the virus, while at the same time ensuring that data protection and privacy rights are respected. The pressure the DPAs are under to allow global data sharing can be seen in the statement of 17 March made by the Global Privacy Assembly (an international group of DPAs), which contains the surprising assertion that “data protection authorities stand ready to help facilitate swift and safe data sharing to fight COVID-19” (one does not normally think of the facilitation of data sharing as being among the tasks of DPAs).

In considering the path to recognition of the global public interest in the context of data protection, one can either be pessimistic when considering how some governments (such as that of Hungary) have been willing to ignore key values like legality and proportionality in the fight against coronavirus, or optimistic if one regards an international catastrophe like a pandemic as the crucible in which countries can forge a conception of the global public interest. The EU and its Member States could make a valuable contribution in this regard by demonstrating that they are capable of “digital solidarity”, i.e., by moving towards EU-wide solutions

to combat the virus, such as the EDPS has called for (indeed, the Commission has proposed such a "common Union toolbox").

A second global trend is the rise in nationalism that has accompanied the spread of the virus, which may have an effect on the regulation of data transfers as well. While nationalism is often malign, it may also reflect a change in attitudes towards globalisation. Examples include the massive increase since the pandemic in restrictions implemented by countries around the world on the export of goods, and government initiatives to have certain types of sensitive goods (such as medical equipment) produced domestically. The growth in global data flows in recent decades has been accompanied by an increase in international trade, and measures to liberalize data flows have gone hand in hand with the removal of trade restrictions (e.g., para. 1(1) of the Commission's adequacy decision for Japan, and the Commission's 2017 communication on "Exchanging and Protecting Personal Data in a Globalised World"). Thus, the liberalization of data flows will likely suffer if the free trade in goods is restricted. This may lead to a rise in so-called "data nationalism", such as incentives or even requirements that databases be stored locally (so-called data localization). The regulation of data transfers could thus become less about granting sufficient protection for the processing of personal data transferred abroad, and more about prioritizing the storage of data locally.

Data must be crossing borders – and must be protected while doing so

As governments, regulators, and individuals grapple with the pandemic, it is important that data protection and privacy be built into the solutions that they develop, including mechanisms to protect data shared across borders. DPAs should make issues of global data sharing a key component of guidance they issue, and together with data controllers they should explore the use of novel mechanisms to provide protection for data transfers. This will also require countries to begin developing a conception of the global public interest. All of this is necessary both to ensure that personal data can flow across national borders to combat common global threats, and to protect the values of legality that form the basis of democratic societies.
