COVID-19
Questions & Answers
Coronavirus emergency vs. GDPR security standards

10 April 2020

In view of the challenges posed by the Coronavirus pandemic, MedTech Europe endeavours to support its members, in particular providing information and guidance on crucial questions related to the present situation.

This Q&A discusses questions relating to GDPR compliance. While it is not to be treated as guidance or legal advice, it will hopefully serve as a useful point of reference.

It has been drafted by Vassilis Karantounias, Senior Counsel at CMS Brussels (EU Law Office), with the support of Cynthia O'Donoghue, Partner at ReedSmith London, and Olivier Proust, Partner at Fieldfisher Brussels as well as the MedTech Europe Data Protection Committee.

Disclaimer

While MedTech Europe considers *the information herein to be reliable it makes no warranty or representation as to its accuracy, completeness or correctness. The document is intended for informational purposes only and should not be construed as legal advice for any particular facts or circumstances. MedTech Europe is not responsible for any damage or loss incurred by any of its members or any third party acting based on the contents of this document. MedTech Europe reserves the right to change or amend it at any time without notice.*

1. Is personal data protection under the GDPR given priority over other fundamental rights? What is its relation to human health?

No, personal data protection is not given priority over other fundamental rights according to the GDPR. The GDPR respects all fundamental rights and observes the freedoms and principles recognized in the Charter of Fundamental Rights of the European Union ("Charter").[1]

In addition to the rights to privacy and personal data protection,[2] the Charter establishes the rights to life and the physical and mental integrity of the person,[3] and furthermore it grants the status of fundamental right *inter*

[1] Recitals 2 and 4, Article 1 (2) GDPR.
[2] Articles 7 and 8 Charter.
[3] Articles 2 and 3 Charter.

alia to the access to health care and medical treatment.[4] Accordingly, a high level of human health protection is required in all of the EU's policies.[5]

In that context, the GDPR not only effectuates the right to personal data protection but also helps to realise and reinforce other fundamental rights. Therefore, the right to the protection of personal data must be balanced against other fundamental rights, such as health care, medical treatment and health security, in accordance with the principle of proportionality.[6] For instance, the GDPR recognizes that health-related personal data which merit higher protection, are nevertheless to be processed when fundamental rights (other than the right to personal data protection) are at stake, in particular where it is in the public interest to do so, such as for health security, the prevention or control of communicable diseases and other serious threats to health.[7]

2. Do exceptional circumstances, such as the COVID-19 outbreak and the measures taken in the fight against this pandemic, excuse non-compliance with the GDPR? If not, are they nevertheless relevant?

No, exceptional circumstances, such as the COVID-19 outbreak and the measures in the fight against it, may, in principle, not serve as an excuse for non-compliance with the GDPR. Having said that, they may indeed be relevant from a GDPR perspective, in several ways. For instance:

- They fall within the ambit of the legal bases laid down in the GDPR for the processing of relevant personal data.[8]
- They may justify the adoption of EU or Member State legislative measures restricting the scope of certain rights and obligations under the GDPR.[9]
- They may form part of the *nature, scope, context and purposes of processing* and have an impact on *the risks of varying likelihood and severity for the rights and freedoms* of individuals. They are, therefore, legally significant under the risk-based approach (hence, amongst others, the scalability of controller's obligations), enshrined in several provisions of the GDPR, such as on controller's accountability, the principle of data protection by design and by default, and data security.[10]

---

[4] Article 35 Charter.
[5] Ibid.
[6] Recital 4 GDPR. In the same vein, see article 8 (2) of the European Convention on Human Rights; and, for instance, European Court of Human Rights, Avilkina and Others v. Russia, judgment of 6 June 2013, application no. 1585/09, para. 45: "*The Court reiterates that the protection of personal data, including medical information, is of fundamental importance to a person's enjoyment of the right to respect for his or her private and family life guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention* […] *Respecting the confidentiality of health data is crucial not only for the protection of a patient's privacy but also for the maintenance of that person's confidence in the medical profession and in the health services in general* […] *Nevertheless, the interests of a patient and the community as a whole in protecting the confidentiality of medical data may be outweighed by the interest of investigating and prosecuting crime and in the publicity of court proceedings, where such interests are shown to be of even greater importance* […]".
[7] Recitals 51 – 54, Article 9 (1) and (2) (c) (h) and (i) GDPR.
[8] Recital 46, last sentence, Article 6 (1) (d) and (e) (NB: other bases may equally be applicable), 9 (2) GDPR.
[9] Recital 73, Article 23 (1) (e) and (i) GDPR.
[10] Recitals 74 – 76 and 78, Articles 24, 25 and 32 GDPR.

- They are to be considered by supervisory authorities as part of the circumstances of each individual case, when deciding whether to impose an administrative fine for violations of the GDPR.[11]

3. More precisely, does the COVID-19 outbreak and the relevant measures enable leniency of treatment on the part of supervisors for violations of the GDPR, as seems to be the case with certain privacy regulators outside the EU?

There are indeed privacy regulators outside the EU who have already signalled a more lenient approach concerning compliance with personal data protection during the COVID-19 outbreak. For instance:

- The UK Information Commissioner's Office stated that they are not going to take regulatory action if controllers' data protection practices do not meet their usual standards or in case of delays in responding to data subject requests.[12] More generally, as regards compliance with data protection, the ICO explained that they will take into account the compelling public interest in the current health emergency.[13]
- In the US, the Office of Civil Rights (OCR) at the Department of Health and Human Services (HHS), which is responsible for the protection of privacy of health information, notified health care providers that it will exercise its enforcement discretion and will not impose penalties for violations of the relevant regulatory requirements under certain conditions.[14]

However, as regards the EU, supervisory authorities in Member States, responsible for the application of the GDPR, as well as the European Data Protection Board (EDPB) have yet to address the question of leniency or *enforcement discretion* in view of the COVID-19 outbreak. On the contrary, thus far they have emphasized that the public health concerns caused by the COVID-19 outbreak and the corresponding measures are not incompatible with the personal data protection.[15]

---

[11] Article 83 GDPR.
[12] Information available on ICO website: https://ico.org.uk/for-organisations/data-protection-and-coronavirus/ (last consulted on 25 March 2020).
[13] Statement available on ICO website: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/data-protection-and-coronavirus/ (last consulted on 25 March 2020).
[14] Notification available on OCR website: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html (last consulted on 25 March 2020).
[15] Statements, guidelines, information available on the respective websites (last consulted on 25 March 2020), including: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf (EDPB); https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles (CNIL); https://www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/GesundheitSozialesArtikel/Datenschutz-in-Corona-Pandemie.html?cms_templateQueryString=CORONA&cms_sortOrder=score+desc (BfDI); https://www.autoriteprotectiondonnees.be/covid-19-et-traitement-de-données-à-caractère-personnel-sur-le-lieu-de-travail (APD); https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=163,39,44,101,194,223,3,99 (HDPA); etc.

The positions of the European supervisors, which in essence suggest the need for a balancing exercise, as explained in the answer to question 1 above, do little to enlighten controllers about how authorities would treat cases of non-compliance with the GDPR due to, or in the context of the COVID-19 outbreak. Nevertheless, while leniency or *enforcement discretion* do not appear in the guidelines or statements of the European supervisors, the GDPR as well as primary-law principles, such as the right to good administration, enable supervisors to take into account the exceptional circumstances under the COVID-19 outbreak and the measures taken in the fight against it. This could apply, for instance, to the exercise of their corrective powers when seized of possible infringements.[16]

4. More precisely, would the COVID-19 outbreak and the relevant measures justify the use of technologies, tools or practices deviating from usual data security standards, in medical devices with the aim of facilitating speedy and safe response to health emergency situations?

In the risk-based system of the GDPR, it is necessary to carry out an *ad hoc* assessment of the data processing operation concerned, when considering conflicting interests such as those involved in this question. Without prejudice to the foregoing, we outline below some key considerations and discuss the possible conclusions of such an exercise.

Security of personal data, encompassed in the concepts of integrity and confidentiality, is among the data protection principles laid down in the GDPR.[17] Detailed provisions set out the relevant obligations of controllers and processors.[18]

In particular, controllers are required to implement *appropriate technical and organizational measures* taking into account, amongst others, the *nature, scope, context, and purposes of processing* as well as *the risks for the rights and freedoms* of data subjects, as derives from the provisions concerning controllers' accountability, data protection by design and by default, and security of data processing.[19]

It must be recalled here that the GDPR is technology-agnostic and does not require any particular standard concerning data security.[20] Having said that, it lists a number of measures to be implemented, where necessary ("*as appropriate*"), such as pseudonymization and encryption of data, and techniques ensuring the confidentiality, integrity, availability and resilience of processing.[21]

Most importantly, the obligation to implement *appropriate* measures reflects the principle of proportionality. While controllers are required to consider measures enhancing data security on the one hand, they must also assess the consequences of the contemplated measures on competing interests, on the other. In essence, this points to the balancing exercise, explained in the answer to question 1. Thus, controllers are required to also take into account the consequences that a specific data security measure may entail as far as the

[16] Articles 58 and 83 GDPR (on powers and administrative fines), Article 41 Charter (on the right to good administration which is recognized as a general principle of EU law by the Court of Justice of the EU).
[17] Article 5 (1) (f) GDPR.
[18] Articles 24 ff and 32 ff GDPR.
[19] Articles 24 (1), 25 (1) and 32 (1) GDPR.
[20] Recital 15 GDPR.
[21] Article 32 (1) (a)-(d) GDPR.

fundamental rights to health care, medical treatment and health security are concerned. A thorough evaluation of the concrete measures, including their consequences, is a prerequisite for their justification in view of the objectives pursued in each instance.

Turning to the medical technology industry, several companies have proactively defined a list of data security measures for the processing of health-related personal data in accordance with their obligations under the GDPR. This is even more true where domestic laws are not prescriptive in terms of data security measures, but rather set out the principles as is the case with the GDPR.

Deviating from the default data security measures, normally deployed by medical technology companies, may, in principle, expose them to compliance risks under the GDPR. However, if this is decided in response to the COVID-19 outbreak and the measures taken in the fight against it, such deviation is arguably less likely to entail a violation of the GDPR, provided that the *ad hoc* assessment demonstrates that:

- the variation is strictly necessary in view of a competing interest worthy of legal protection, such as the rights to health care, medical treatment and health security, which would be otherwise endangered if the controller applies the default security measures;
- the security measures envisaged ensure an adequate level of data security; and
- a right balance is struck between the different interests at stake, i.e. the right to personal data protection and the said rights to health care, medical treatment and health security.

For instance, if protecting healthcare providers from unnecessary exposures to COVID-19 hinges upon incorporating into a medical device communication capabilities that go beyond their usual standards (e.g. introducing a wireless or Bluetooth-enabled remote monitoring / adjustment functionality in a ventilator on top of its wired connectivity feature), this modality would be unlikely to constitute a violation of the data security measures, subject to an *ad hoc* assessment demonstrating the above results. In the same vein, enabling a healthcare provider to give urgent advice to a patient suffering from COVID-19, or a staff member of a medical company to provide remote guidance or training to healthcare providers or such patients, may justify the use of features in the functioning of medical devices, which deviate from the security measures usually deployed, subject to an *ad hoc* assessment resulting in the same conclusions. In other words, in these situations, the need to protect the health of healthcare providers and medical company authorised staff as well as COVID-19 patients may justify the use of a technology for the handling of a medical device, which entails higher security risks if compared with the default security standards (e.g. wireless as opposed to wired connectivity). By analogy, this is apparently what has driven some regulators outside the EU to flag their exercise of enforcement discretion, as explained in the answer to question 3.

Please note that under the accountability principle the controller bears the burden of proof that the above conditions justifying the revised security measures are met.[22] Also, it must be recalled that privacy-intrusive actions or measures, taken by controllers (and regulators) when confronted with an emergency, are not allowed to be used in a systematic or irreversible manner. That would render them disproportionate and therefore unacceptable according to the EU framework on fundamental rights.[23] In practical terms, this means that while the COVID-19-related exceptional circumstances may under certain conditions justify a deviation

[22] Article 24 GDPR.
[23] Article 52 (1) Charter.

from the data security standards, normally employed, it should in no way lead to the lowering of security standards in a generalised manner. Furthermore, since compliance with the GDPR is an ongoing exercise, controllers are expected to gradually factor in the risks revealed under the COVID-19 outbreak in their products or services and thereby further enhance security standards.

All in all, currently it seems to be indeed allowed to use technologies, tools or practices deviating from usual data security standards, in medical devices, provided that this is absolutely necessary in the fight against the COVID-19 outbreak, the security measures envisaged ensure an adequate level of security, and a right balance is struck between the right to personal data protection and the rights to health care, medical treatment and health security, as this is to be evidenced by a dedicated *ad hoc* assessment. However, this does not mean that health emergency situations may as a rule justify the use of lower data protection standards. Controllers are required to continuously improve their security standards for all foreseeable situations. Other than that, in any case, it goes without saying that the rest of the data protection requirements as per the GDPR have to be fully respected, including amongst others the whole range of principles laid down in it.[24]

About MedTech Europe

MedTech Europe is the European trade association for the medical technology industry including diagnostics, medical devices and digital health. Our members are national, European and multinational companies as well as a network of national medical technology associations who research, develop, manufacture, distribute and supply health-related technologies, services and solutions.

For more information, visit www.medtecheurope.org.

[24] Article 5 GDPR: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.