Response to EDPB consultation on Data Protection by Design and by Default

MedTech Europe welcomes the opportunity to provide its comments to the EDPB's draft guidelines on Data Protection by Design and by Default (DPbDD) (the "Guidelines") and appreciates the importance given by the Board to DPbDD being incorporated from the early stages of planning a new data processing operation.

What DPbDD means for MedTech Companies

Medical technologies (MedTech) cover any products, services or solutions used to save and improve people's lives and which can be used in a care setting, such as disposables, diagnostics, capital equipment and surgical innovations, through to implant technology, biomaterials and connected health IT such as eHealth, mHealth, human genome decoding, disease prediction, biobanks, biomarkers and many more. These products and solutions, more often than not, rely on the collection, analysis, and sharing of health data, which is by nature personal data, to better understand diseases and treat them as part of an efficient and effective healthcare system. As such, MedTech Europe member companies understand and fully acknowledge the importance of DPbDD being incorporated from the early stages of planning a new data processing operation.

Depending on a specific phase in the lifecycle of a medical technology, MedTech companies may or may not be data controllers. Moreover, when a medical technology is on the market and used by healthcare providers and/or patients, the situation may not always be clear. Whether a company developing a product including software is a data controller, processor or neither depends on how and by whom the medical technology is intended to be used, as well as whether the company has/will have access to personal data when the device is used, and for what purposes[1].

Scope of the Guidelines

Article 25 of the EU General Data Protection Regulation 2016/679 (GDPR) provides that DPbDD requirements apply explicitly to controllers of personal data "*at the time of the determination of means for processing*". A strict reading of this article may not directly apply to data processors, or to those MedTech companies that do not process personal data at all. However, the Guidelines seem to imply that "*other actors, such as processors and technology providers*" may have to take those Guidelines under certain circumstances into consideration[2]. Moreover, the Guidelines see "processors and technology providers […]" as key enablers for DPbDD[3]. The draft Guidelines also encourage data controllers to regularly review and assess data processors to ensure that

[1] For example, a manufacturer that processes personal data, collected from a device, for its own purposes will likely be a controller. On the other hand, a manufacturer that does not access personal data from a device at all after sale may be neither a controller nor a processor.
[2] Paragraph 1, DPbDD Guidelines
[3] Paragraph 85, DPbDD Guidelines

MedTech Europe
Rue Joseph II 40, 1000 Brussels – Belgium
Tel. +32 2 300 96 43 – Fax. +32 2 300 96 44
info@medtecheurope.org – www.medtecheurope.org

they enable continual compliance with the DPbDD principles and support the data controller's obligations in this respect.

Considering the complex scenarios in the MedTech industry, the Guidelines are not always clear what obligation has to be fulfilled by each of the different players.

General remarks

The Guidelines appear to take an approach that seems to go beyond the language contained in the GDPR by imposing additional very prescriptive obligations on controllers, processors and other actors. As the Guidelines, once final, will most likely support and guide interpretation of the GDPR, this approach may result in or trigger a shift away from the risk-based approach whereby controllers' compliance with GDPR is based on impact assessments (including assessment of necessity and proportionality as well as assessment of appropriateness of organizational and technical security measures), and/or a shift of these responsibilities onto processors and 'other actors'.

In the current draft, however, the Guidelines are not (and may even not be able to be) clear on how exactly they apply to more complex situations where, e.g., a MedTech company designs and develops a certain product or solution, but may not, or only to a very limited extent, be involved in any personal data processing (or any personal data processing decision) that is ultimately done by a controller with the device. One potential means to ensure common understanding from the different players, in this case companies and healthcare providers, such as hospitals or labs, would be for example spelling out such scenarios as falling out of the scope of the final guidelines.

Finally, for MedTech companies it is difficult, if not almost impossible, to prove (retrospective) compliance with DPbDD for certain products, in particular, those products that have already received regulatory approval under the relevant medical devices' regulatory frameworks[4] and that have been on the market for many years prior to the GDPR coming into force. Listing out each of the key elements contained in the draft Guidelines, even if not relevant for a particular product and its processing, may result in controllers hesitating to use a product despite the political and economic pressure relating to increased use of digital products in healthcare, and in contra, where a MedTech companies cannot retrospectively demonstrate compliance with such detailed Guidance to the detriment of data subjects. Ultimately, this would also lead to a consequential knock-on effect from the policy perspective.

"State of the art"

Medtech products, in particular, those on the market for a long time, complied with the criteria of "state of the art" at the time of market access, and, even though they are continuously updated according to new standards

[4] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives

(e.g. patient safety), they may not comply with the "state of the art criterion" of nowadays. This would lead MedTech companies (processors in most cases) to have to demonstrate compliance with DPbDD retrospectively, which arguably is not possible.

In addition, MedTech Europe also suggests taking into consideration the distinction between, on one hand, medtech products, which need to comply with sector-specific regulations referenced above that may include (security) related design requirements, MedTech companies, among other obligations, have to implement solid quality management systems, and, on the other, regulated products and software that are already on the market and will remain on the market for several years to come on the other (e.g. because any successor product would again require to go through a new design and development phase subject to sector-specific regulations and supervision).

Certification

In paragraph 86 of the draft Guidelines, it is provided that "where there is no certification, controllers should seek to have other guarantees that technology and service providers comply with the requirements of DPbDD." MedTech Europe sees the approach of certifying processing operations in all instances as very difficult to obtain in the MedTech sector. Besides, MedTech Europe would appreciate if the Guidelines presented some kind of self-certification methods. Moreover, we have difficulties to understand what could be meant by the "*other guarantees*" controllers should seek to ensure that technology and service providers comply with the requirements of DPbDD. In this regard, the draft Guidelines seem to go above and beyond the recommendation contained in Recital 81 of the GDPR, which reads "*controllers should use only processors providing sufficient guarantees […] to implement technical and organisation measures which will meet the requirements of [the GDPR], including for the security of processing.*" Both suggestions create the risk of healthcare providers (e.g. hospitals) setting standards which are unclear, or otherwise impossible to meet by MedTech companies.

Further, MedTech Europe believes that the draft Guidelines have the potential to shift responsibility onto MedTech companies. For instance, the Guidelines state: "*Technology providers should seek to support controllers in complying with DPbDD*" and that "*controllers should not choose providers who do not propose systems enabling the controller to comply with Article 25 […]*"[5]. For MedTech companies, those controllers may be their own customers (e.g. hospitals, labs, clinics), and this would mean that MedTech companies may be held accountable if they do not support their customers in complying with DPbDD, even though a MedTech's produces or solutions have achieved regulatory approval under the applicable regulatory framework.

90/385/EEC and 93/42/EEC; Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU

[5] Paragraph 86, third recommendation, DPbDD Guidelines

Obligation of accountability

MedTech Europe has the impression that the Guidelines seem to confuse the obligation of accountability and DPbDD; in that accountability is about on-going assessments whereas DPbDD is more static and addresses the conception of a product or the commencement of personal data processing or design before actual processing starts.

Relevance of the cost of implementation

The draft Guidelines currently provide that controllers must factor in DPbDD as a business cost. However, Article 25 (and Article 32) is providing that cost is a factor in assessing proportionality and so may be taken into account when assessing what is required. Therefore, the fact that costs can be a relevant factor in determining what measures are appropriate should be acknowledged and clarified in the Guidelines, which is not sufficiently underlined in the current draft, in particular, in the conclusions.

Conclusion and recommendations

MedTech Europe welcomes the issuance of Guidelines that contain practical suggestions, but would suggest clarifying that these suggestions are examples rather than requirements and that data controllers remain responsible to assess, on a case by case basis, what privacy by design exactly means, taking into account the use of services provided by third parties which may or may not be processors, but might act as independent or joint controllers instead.

Concluding, we would appreciate if the above considerations are taken into account by Board, whether it is to update these Guidelines or for the development of additional ones.

About MedTech Europe

MedTech Europe is the European trade association for the medical technology industry including diagnostics, medical devices and digital health.
Our purpose is to make innovative medical technology available to more people, while helping healthcare systems move towards a more sustainable path. For more information, please visit http://www.medtecheurope.org.