2024

The European Health Data Space

Common statement on the Amendment proposals of the Council of the EU and the European Parliament

December 2023

This statement was written in partnership with Hogan Lovells LLP

EUCOPE

European Confederation of Pharmaceutical Entrepreneurs AISBL

EUCOPE

European Confederation of
Pharmaceutical Entrepreneurs AISBL

Common statement on the European Health Data Space and the Amendment Proposals of the Council of the European Union and the European Parliament

In partnership with Hogan Lovells LLP

Introduction

The following article provides an overview of EUCOPE's perspective on the Regulation on the European Health Data Space ("EHDS") with respect to the different proposals that are currently subject to the trilogue negotiations between the Council of the European Union ("Council"), the European Parliament ("EP") and the European Commission ("Commission").

The article will focus on the secondary use of health data in the EHDS, the objective of which is to improve the availability of electronic health data ("ehD") for purposes such as research, innovation, patient safety and personalised medicine. Here we outline EUCOPE's perspective on challenges and opportunities associated with each of the versions of the text and puts forward solutions to ensure the utility and success of the EHDS.

The outcome depends to a large extent on the way how three issues are regulated by the proposal:

- **Ensure sufficient safeguards for intellectual property rights and the protection of trade secrets.** The EHDS should provide measures to protect commercially confidential information in order to protect private trade secrets. Data containing trade secrets or commercially confidential information should not be part of the EHDS dataset catalogues. The EHDS should provide a mechanism for data holders to prevent such publication of their data.

- **Location of data processing and international data transfer.** Where data processing takes place and how the authorisation of international data transfers is regulated? The EHDS should avoid excessive data localisation and international health data transfer requirements that go beyond the requirements of the GDPR's framework.

- **Opt-out and/or opt-in.** Regulate the opt-out or opt-in rights of individuals in the EHDS. It should avoid any opt-in and only incorporate an opt-out mechanism as long as it does not lead to inconsistent implementation, increased health data disparities and excessive administrative burdens. The relevant legal bases under the GDPR should be leveraged and applied in a harmonised way across Member States.

Safeguards on IP right and trade secret protection

In the Commission's original EHDS draft of May 2022, the protection of private intellectual property rights and trade secrets (together referred to as "commercially confidential information") was described in a single sentence and has been hidden in paragraph 4 of Art. 33: "*Where such data [i.e. ehD containing protected intellectual property rights and trade*

secrets of private undertakings] are made available for secondary use, all necessary measures shall be taken to preserve the confidentiality of intellectual property rights and trade secrets". Such a provision is far from sufficient to effectively safeguard commercially confidential information.

The Council and EP proposals provide for significant improvements in the protection of IP rights and trade secrets in the EHDS. However, a closer look at the Council and EP proposals reveals that further changes are still urgently needed. In order to get a clearer picture of the further changes that need to be made, it is helpful to visualise the individual steps on which the secondary use mechanism is based.

Secondary use – procedure

At the present time, the procedure is structured in the following way: As a first step, each data holder will have to provide the competent national health data access body ("HDAB") with a general description of the datasets in its possession that are subject to secondary use according to Art. 33 of the EHDS drafts. The HDAB shall publish the received information of the datasets (metadata) in a publicly accessible catalogue. After consulting the catalogue, interested data users may submit a data access application to obtain access to the data of specific datasets. The request is to be submitted either to the HDAB or, if the requested dataset concerns only one data holder, the request can be made to that specific data holder.

The HDAB or the individual data holder shall verify that the requested data serves the purpose of use specified in the application that all requirements under the EHDS for secondary use are fulfilled and that there are no grounds under the EHDS or delegated acts or guidelines for refusing access. A data permit will be issued in favour of the data user if there is a positive outcome of this verification. When the HDAB grants the permit, it will request the relevant data holder(s) to provide the requested data so that the HDAB can make it available to the data user in a secure processing environment within two months. The data user may access the data within the secure processing environment for as long as and up to the extent permitted by a valid data permit. The regular access period currently under discussion between the Commission, the Council and the EP is between 5 and 10 years.

> **Evaluation and recommendation:** The first question that every company operating in the healthcare and life sciences sector with direct or indirect links to the EU is likely asking themselves is "*am I a data holder in the sense of the EHDS*?" and "*what health data do I have to make available for secondary use?*". While all three proposals try to answer the first question either by defining the scope of the EHDS (as in the Commission and EP proposals) or by specifying the definition of "data holder", the answer to the second question is not addressed at all. In particular, it is unclear whether only data collected and stored in the EU falls within the scope of the EHDS. If an EU-based company also have to provide data collected outside the EU, then data within the meaning of Art. 33 of the draft EHDS would be all data processed by an EU company, regardless of where it was originally collected and where it is stored. The EHDS should avoid excessive data localisation and international health data transfer restrictions that go beyond the requirements of the GDPR's framework which is critical to not dissuade international partners from conducting medical research and healthcare innovation in Europe.

*For any questions or further information on the EHDS-E please contact **Leander Vranken (EUCOPE, vranken@eucope.org)** or **Dr. Karolin Hiller (Hogan Lovells LLP, karolin.hiller@hoganlovells.com)***

Competence of HDAB

In all three EHDS proposals, the main responsibility for the protection of commercially confidential information lies with the national HDAB. While according to the EP proposal the HDAB is even responsible for determining whether the data should be qualified as commercially confidential information, it says in all three proposals that the HDAB is supposed to decide whether and how intellectual property rights and trade secrets should be protected. Both Council and the EP impose an obligation on data holders to inform the HDAB when they consider a particular dataset shall require specific protection and to identify the parts of the dataset concerned. The Council proposal further requires the data holder to justify to the HDAB why commercially confidential data require specific protection and to provide supporting evidence.

> **Evaluation and recommendation**: From the perspective of a private company, the decision to give the national HDABs a leading role in the safeguard mechanism is unjustified. The fact that the HDAB is given the sole responsibility to determine which data is to be protected by IP rights or protected as trade secrets is irrational and cannot be permitted under any circumstances. HDABs do not have the expertise to evaluate if datasets constitute trade secrets. In the absence of strong safeguarding mechanisms, it should always be the role of the data holder as the legitimate person for this to determine whether such datasets constitute trade secrets. If at all, it is only acceptable if the EHDS provides sufficient guardrails for identifying the required procedural steps and organizational and technical measures for protecting commercially confidential information (e.g., identified by the data holder as such based on reasonable grounds) and to prevent the single national HDAB from deviating too far from other views in its interpretation of the applicable EHDS provisions.

So far, only the EP proposal takes this aspect into account and provides for safeguards. The EP calls on the Commission to issue guidelines, including procedural steps and measures to assist the HDAB to ensure the confidentiality of ehD. In contrast, the Council proposal limits the Regulation by stipulating that the individual HDAB shall take all specific measures, including legal, organisational and technical measures, necessary to maintain the confidentiality of protected data. The Council proposal does not provide for uniform guidelines at EU level. Furthermore, it is unacceptable that in the Council proposal, in the light of the fundamental rights of private healthcare companies, that data holders must accept the decisions of the HDAB on whether and how protection of commercially confidential information is provided and with no given right of appeal. The EP proposal does provide for such a specific right for data holders (and data users) to challenge the decision of the HDAB on the protection of intellectual property rights and trade secrets.

The Council does not provide for a specific remedy, but it can be argued that the rights of data holders are equally protected under the Council proposal since Art. 43 (9) of the Council proposal says that any natural or legal person concerned has the right to an effective judicial remedy against a decision of the HDAB. Another merit of the Council proposal is that it regulates in the most precise and transparent way how data containing commercially confidential information are protected against possible misuse by data users. While the EP proposal only provides that the secondary use of ehD that is not covered by the data permit is prohibited and that a data permit can be revoked, the Council proposal does not stop there. Rather, it lays down guardrails for the competent HDAB on how to react preventively to a possible misuse of a data permit. Specifically, the Council proposal provides criteria and lists

*For any questions or further information on the EHDS-E please contact **Leander Vranken (EUCOPE, vranken@eucope.org)** or **Dr. Karolin Hiller (Hogan Lovells LLP, karolin.hiller@hoganlovells.com)***

risks that the HDAB should consider when deciding whether to grant data users access to the requested ehD. The HDAB shall refuse any access if the risk of misuse cannot or is not sufficiently mitigated by accompanying measures. Furthermore, if the HDAB is unable to take legal, organisational and technical measures to ensure the confidentiality of such data in secondary use, it shall also refuse access to such data.

> **Evaluation and recommendation**: To some extent, especially in comparison with the Commission's original initiative, each proposal contains improved approaches to the protection of commercially confidential information. However, none of the proposals are so far sufficient. In particular because the provisions for protective measures are applied too late. In general, measures to protect trade secrets come too late when the data holder has to provide the HDAB with a general description of the datasets already containing trade secrets when this information, and thus the existence of these datasets, is made publicly available in the dataset catalogue. The EHDS must provide for measures to protect commercially confidential information at a very early stage in order to effectively protect private trade secrets. I.e., the HDAB must keep out of the dataset catalogue any data containing commercially confidential information. In addition, the EHDS must provide remedies for data holders to prevent such publication by adding a mechanism to challenge such a request.

International data transfers and storing of electronic health data

As a rule, EU-based private healthcare companies do not operate only within the EU. They often have business partners all over the world or they are part of an international group. Therefore, it is of fundamental importance that ehD can also be used for secondary purposes outside the EU and be located and processed in non-European countries.

The EP proposal provides in Art. 60A that all ehD – regardless of whether for primary or secondary use – must be stored within the EU. Such an approach only makes sense for primary use of the ehD, i.e. requiring that the EHR systems is established and hosted in the EU. However, as far as secondary use is concerned, the obligation to store ehD only in the EU is not comprehensible when at the same time the EP proposal itself explicitly allows for the transfer of the ehD to a third country outside the EU on the basis of a data access permit issued by a HDAB (more details below). Once ehD has been transferred to an eligible data users outside the EU, they must be allowed to store the received ehD anywhere in a secure and protected environment. Otherwise, all non-EU data users would not be able to store the received ehD in their home country.

Mandatory storage of ehD within the EU may also be technically complicated for non-EU based companies. Regarding the storage of ehD, the Council proposal seems to follow a different strategy. According to Art. 60A of the wording of the Council proposal, the storage of ehD within the EU – or in exceptional cases also in third countries covered by an adequacy decision pursuant to Art. 45 GDPR – is only required for certain specifically identified processing activities. This means that the HDAB and the data holders would only have to carry out the act of pseudonymisation and anonymisation within the EU, as well as other legal, organisational and technical measures to ensure the confidentiality and protection of this data before leaving the EU. Once these safeguards are in place, other processing activities – such as storage upon receipt of pseudonymised ehD on request – would be permitted anywhere, provided that the other legal requirements under the EHDS (such as compliance under EU-General Data Protection Regulation 2016/679 ("GDPR") are met.

*For any questions or further information on the EHDS-E please contact **Leander Vranken (EUCOPE, vranken@eucope.org)** or **Dr. Karolin Hiller (Hogan Lovells LLP, karolin.hiller@hoganlovells.com)***

Evaluation and recommendation: International data transfers are not only essential to the interest of EU healthcare companies, but also for EU patients. Data flows are crucial for the development of innovative as well as personalised medicines. Therefore, the EHDS must limit the obligation to process ehD within the EU only (or exceptionally also in third countries, provided they are covered by an adequacy decision pursuant to Art. 45 GDPR) to the hosting of the EHR system and the processing of ehD for primary use within this EHR system. If the patient is requesting treatment outside the EU or in any legitimate secondary use scenario when ehD would be reused for research, the transfer, storage and any other processing of ehD outside the EU should be allowed when sufficient legal, organisational and technical measures are put in place by the third country ensuring a similar level of integrity and confidentiality of the transferred ehD as required under EU laws.

Regarding the transfer of ehD for secondary use outside the EU, the Council and the EP have chosen an approach similar to the one applied in the GDPR. This means that the Commission will be responsible for determining by means of a delegated act to which third countries the ehD may be transferred in case of a request for data access by a third country. The Council proposal stipulates that third countries that may be listed in the delegated act must (i) grant EU data users access to health data located in that third country under conditions that are not more restrictive than those provided for in the EHDS (principle of reciprocity), and (ii) the (personal) data transfer must comply with the provisions of Chapter V of the GDPR (Art. 44 et seqq. GDPR). If these conditions are met, data users located outside the EU may submit a data access application under the EHDS. Whether the EP also requires the principle of reciprocity in general and for all data users located outside the EU is not entirely clear. The wording of the provisions of the EP proposal refers only to “entities and bodies” or “third countries and international organisations”. However, there is no reason why the legal requirement for private data users to obtain access to data under the EHDS should be limited to compliance with Art. 44 et seqq. GDPR. It can be argued that if a third country and its public authorities and entities can only make a request for access to data if the principle of reciprocity is met, the same should apply to all natural persons residing in that country.

Evaluation and recommendation: The approach that a third country has to be recognised by the Commission as a country where ehD are sufficiently secured and protected of any infringement of the legitimate interests of the natural person concerned has already proven successful in the context of the GDPR. It is important that the legal requirements for a third country to be included on the Commission's list are sufficiently clear and adequate under a EHDS specific perspective and scope. Safeguards to protect only natural persons and their rights would under the EHDS not be sufficient as an adequate personal data protection is already guaranteed by the GDPR. It is important that commercially confidential information is also sufficiently protected in the case of third country applications. The principle of reciprocity can be an appropriate protection measure and, if chosen, it should be applied to all types of transfers of ehD to third countries. Beside this, the protection of commercially confidential information is not yet sufficiently addressed in any of the EHDS proposals and in the provisions for delegated acts of the Commission. Amendments are needed to ensure adequate protection of intellectual property rights and trade secrets.

*For any questions or further information on the EHDS-E please contact **Leander Vranken (EUCOPE, vranken@eucope.org)** or **Dr. Karolin Hiller (Hogan Lovells LLP, karolin.hiller@hoganlovells.com)***

Opt-out/ opt-in rights for natural persons to limit the use of their electronic health data for secondary purposes

The Commission proposal does not provide for any consent requirement to natural persons for secondary use beyond referring to national law (Art. 33 (5) of the Commission proposal). This approach has been justified because (a) data for secondary use will be either anonymised or pseudonymised, and because (b) there are further mechanisms provided in the proposal to safeguard personal data against abuse, including a list of permitted uses (Art 34) and a list with prohibited uses (Art. 35) as well as rules for governance and of practical nature. Now, however, both the Council and the EP proposals have introduced rights for natural persons to limit the sharing of their ehD for secondary use.

The Council proposal provides for a right of objection for natural persons (opt-out mechanism). It lays down general guardrails and leaves the final decision on whether and how to grant natural persons an opt-out to the individual Member States. This means that natural persons may object to the secondary use of their ehD under the EHDS only if and to the extent provided for by rules and safeguards introduced at national level. If a Member State does not introduce a specific right to object under the EHDS, Art. 21 GDPR applies (see recital 37a of the Council proposal). I.e. natural persons have the right to object if the data processing will be based on grounds in accordance with Art. 6 (1) (e) or (f) GDPR.

The EP proposal goes further than the Council proposal. It includes both opt-out and opt-in solutions (see recital 39a of the Parliament proposal). Each Member State shall generally provide for an opt-out right for natural persons regarding their ehD. For particularly sensitive data like genetic, genomic, and proteomic data, but also data from wellness applications each Member State shall even provide for a consent requirement (opt-in). The EP leave the individual Member State no choice on whether to introduce objection, respectively consent rights for its citizens but the implementation is obligatory. The Member States have only discretion on how these rights are shaped in detail.

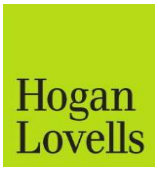
> **Evaluation and recommendation:** There are significant concerns about the risks associated with an uneven implementation of the opt-out / opt-in mechanism including potential setbacks and associated costs. The implementation of the EHDS already carries additional costs for all Member States. Any ambiguity in the objection/ consent mechanism will likely lead to disharmony in the sharing of datasets and will unnecessarily increase the implementation costs of the EHDS in the Member States. The Council's approach to leaving the decision up to the individual Member States whether citizens can opt out from secondary use only leads to more fragmentation, which goes against the very grain of the purpose of the EHDS. The strict approach of an opt-in mechanism for specific data categories would likely lead to health data disparities and foster that certain minority groups, but also young and generally healthy people exercise the right more often which increases the risk of scientific underrepresentation and undermine the reliability of data-driven health interventions. Against this backdrop, only a uniform opt-out mechanism is acceptable. The same opt-out mechanism should be applicable by all HDABs across all Member States in order to limit the scope of national derogation and ensure that the technical specifications are aligned all over Europe.

Regarding the impact for healthcare professionals and other data holders, it is critical that the opt-out mechanism is practical and as "light touch" as possible keeping low additional responsibilities and tasks imposed on them.

*For any questions or further information on the EHDS-E please contact **Leander Vranken (EUCOPE, vranken@eucope.org)** or **Dr. Karolin Hiller (Hogan Lovells LLP, karolin.hiller@hoganlovells.com)***

A functional opt-out mechanism would also need a well working infrastructure in place in all Member States. Only then such mechanism becomes implementable in all European healthcare systems. Further, the opt-out mechanism should also have limits that are well-defined, consistent, and transparent excluding that an opt-out right creates disproportionate effort or distorted results. Thus, an opt-out mechanism such as for medical registries and clinical trials should be excluded. It would render research impossible or would seriously impair the objectives of pharmaceutical studies. In addition, an opt-out mechanism needs sufficient investment, and budget as well as the necessary technical features to ensure full transparency. All citizens must be well informed about the opt-out, how to exercise it, when it does not apply and what it means for them and for society.

This statement was written in partnership and organised with support of **Hogan Lovells LLP**



*For any questions or further information on the EHDS-E please contact **Leander Vranken (EUCOPE, vranken@eucope.org)** or **Dr. Karolin Hiller (Hogan Lovells LLP, karolin.hiller@hoganlovells.com)***