60 YEARS YOUNG YEARS STRONG

BEUC The European Consumer Organisation

The Consumer Voice in Europe

CONSUMERS NEED STRONG SAFEGUARDS TO PROTECT THEIR HEALTH DATA

BEUC position paper on the proposed European Health Data Space

Contact: Wolfgang Schmitt – digital@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2022-104 - 10/10/2022

Why it matters to consumers

Consumers constantly generate health data, for example when they go to the doctor, use a blood-sugar-meter or access a nutrition or sports app. Health data is highly sensitive. It can not only have a big impact on a person's health but also, for example, on job applications or on getting approval for a bank loan. Because of this sensitivity, health data is subject to a high standard of protection under the General Data Protection Regulation. The creation of European Health Data Space must not lower that level of protection and take away control and transparency from consumers regarding their health data.

Summary

The European Commission proposed a Regulation to create a European Health Data Space on 3 May 2022. The proposed Regulation is a key pillar for the European Health Union and would create the first common EU data space in a specific area to emerge from the 2020 European strategy for data. However, this is a deeply flawed proposal that leaves many important questions unanswered and puts the protection of personal data and privacy at risk. These significant flaws need to be remedied in order for the initiative to achieve its objectives. To ensure that this proposal strikes the right balance between the various interests at stake, the European Parliament and EU's Council of Ministers must:

Establish consumer control over the primary use of health data (Chapter II) by:

1. Ensuring consumers must actively give consent (opt-in, not opt-out) to the primary use of their health data
2. Clarifying terminology on health data
3. Regulating access to data by health professionals
4. Improving transparency regarding access to consumers' health records
5. Promoting public awareness about how to make use of these new tools
6. Prohibiting any form of exclusion or discrimination against individuals that choose not to, or cannot, make primary use of their health data
7. Guaranteeing a high level of data security and confidentiality
8. Adding the EHDS to the Annex of the Representative Actions Directive (EU) 2020/1828.

Improve and ensure security of Electronic Health Record systems (Chapter III) by:

1. Electronic Health Record (EHR) systems must be reviewed and approved by a competent authority before entering the market and not self-certified by manufacturers.

Establish a system for secondary data use that effectively protects individuals (Chapter IV) by:

1. Restricting the list of legitimate purposes for secondary use

2. Including mandatory minimum quality requirements in the proposed Regulation for **anonymisation and pseudonymisation** of health data
3. **Removing genetic data from the scope** of the European Health Data Space
4. Upholding the full competence of health data access bodies **and preventing any possibilities for circumvention**
5. Removing **wellness application data** and **person generated electronic health data** entirely from the scope of the EHDS
6. Ensuring that if a health data access body fails to respond to a request for a data access permit within a deadline that there is **no automatic approval of the permit** by default
7. Giving **consumers the right to opt-out** from making their personal electronic health data available for secondary use
8. Preventing the use of electronic health data for any **advertising or marketing** activities
9. Ensuring that the secondary use of data will result in the longer term in **more affordable and accessible health technologies** for everyone
10. Providing a **closed list of 'minimum categories of electronic health data'** accessible for secondary use
11. Regulating requirements, technical specifications, and the IT-infrastructure of **HealthData@EU** within the EHDS.

1. Introduction

The proposal for a Regulation to create a European Health Data Space (EHDS)[1], presented by the European Commission on 3 May 2022, aims to unleash the full potential of health data by both helping individuals to make their health information easily accessible and supporting the secondary use of health data for research, innovation, policy-making and regulatory activities to improve public health care.

The EHDS concerns electronic health data and is the first proposal for a sector specific data Regulation within the 2020 European data strategy. Firstly, the EHDS **aims to empower individuals through better digital access to their personal health data,** nationally and cross-border, as well as fostering a Single Market for electronic health record systems, relevant medical devices and high-risk artificial intelligence (AI) systems. These processing operations are defined as **primary use of data.**

On the technical side, the EHDS would establish **mandatory supplementary cross-border service and infrastructure** to facilitate health data sharing within the EU. For the **primary use** of data this common infrastructure is called **MyHealth@EU.**

Furthermore, the EHDS proposal would establish a mechanism for the **secondary use** of electronic health data. This second pillar would make **anonymised or pseudonymised** electronic health data **accessible for research, innovation, policy-making and regulatory activities.** Member States would have to set up a health data access body to ensure that electronic health data was made available by data holders for data users.

[1] Regulation 2022/0140 (COD) on the European Health Data Space, published on the 3 May 2022.

2. Primary use of data (Chapter II)

Chapter II of the proposal focuses on the primary use of electronic heath data. It would introduce a **standardised set of 'priority categories'**[2] of health information of European citizens, accessible via a **cross-border service** that facilitates the exchange of electronic health data between individuals and health professionals throughout the EU. This cross-border service is called **MyHealth@EU.**

The EHDS proposal would ensure that health professionals[3] like doctors, nurses, dentists, and pharmacists have access to health data of natural persons under their treatment (Article 4(a)). **Health professionals would receive a right to access** at least the priority categories of electronic health data such as medical history, diagnoses and treatments, medications, allergies, immunisations, as well as radiology images and laboratory results from European individuals under their treatment. Member States would be able to limit this right of access by different health professionals to specific categories of personal electronic health data (Article 4(2)). Nonetheless, Article 4(3) would ensure that health professionals always had access to at least the priority categories of health data under Article 5.

At the same time, Article 3 would grant natural persons themselves a series of rights in relation to the primary use of their health data, including:

- The **right to access** their personal electronic health data, which should be facilitated via Electronic Health Record systems (EHR systems)
- The **right to receive an electronic copy** of their health data
- The **right to insert their electronic health** data in their own EHR
- The **right to give access** to, or request a data holder from the health or social security sector to **transmit** their electronic health data to, a data recipient of their choice from the health or social security sector in their own country or another Member State
- The **right to obtain information** on the healthcare providers and health professionals that have accessed their electronic health data.

Consumers would also have the right to restrict access to their personal electronic health data under Article 3(9). This restriction, nevertheless, **only applies to the content** of the data. Health professionals and or health care providers would still be informed about the existence and nature of the restricted electronic health data (Article 4(4)).

2.1. No to opt-out solution

According to Article 7 of the proposal, where data was processed in an electronic format, health professionals would have to **systematically register** the relevant health data **in an EHR system.** Consequently, the health data of all European individuals would be accessible by law and **without prior explicit consent from the affected consumer.**

This systematic registration of health data within an EHR system without prior explicit consent from the data subject is **inconsistent with the concept of informational self-determination**, one of the fundamental principles of data protection law in the EU. According to this principle, natural person should have the authority to decide themselves,

[2] The term 'priority categories of electronic health data' is defined in Art 5 but can be amended by the European Commission (EC) via delegated acts.
[3] Article 2(1)(b) follows the definition under Article 3(f) of the Directive 2011/24/EU.

when and within what limits information about their private life should be shared with others.

The current draft proposal would in practice lead to situations where a health professional like a pharmacist could have full access to all priority health data about a patient, including categories of health data that are not relevant for their profession, without the patient knowing. Irrespective of the fact that the EHDS does not foresee an informational campaign (or anything else) to raise awareness about the primary use of data and the rights of natural persons, natural persons should not have to protect their most sensitive electronic health data themselves, as this must be guaranteed by law. Such legal protection is crucial because, despite the benefits of the automatic integration of all health data for primary use, there are also considerable risks for the rights and freedoms of the natural persons concerned. Any data breach could lead to **potential misuse** of data **ranging from discrimination to exploitation of individuals.**

Because of the potentially large amount and the sensitive nature of the data involved, we consider that it is **absolutely necessary for consumers to be actively involved** in the process of giving access to health data for primary use in order to protect the rights and freedoms of natural persons. Consequently, the proposal must be amended so as to ensure that natural persons would have to give their **explicit consent** before their personal electronic health data was made available for primary use. The opt-out solution in the current proposal is certainly not compatible with the EU's obligation to contribute to a high level of protection of fundamental rights.

According to the proposal, the main objective of the primary use of data is to **empower individuals and to provide better access to and control of** their personal health data. The Commission uses therefore, as a model example, the transfer of pharmaceutical prescriptions from one Member State to another. EU citizens would be able to obtain their medication in a pharmacy located in another EU country, thanks to the online transfer of their prescription from their country of residence to another Member State.[4] But this objective could very well also be met with prior explicit consent. If a consumer wants a pharmaceutical prescription to be sent to a health professional in another Member State, this can be based on conventional consent. Health professionals can simply ask the patient during treatment whether they agree to the transfer or not. **Establishing an opt-out solution does not empower consumers but on the contrary, it takes away control and restricts their freedom to decide with whom their health information is going to be shared.**

[4] https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en

In order to ensure legal certainty with regard to obtaining consent, the proposal must provide a **model consent form** within its Annexes.

BEUC RECOMMENDATIONS:

- **Consumers must stay in control** and decide themselves whether they want their data to be electronically accessible across the EU or not. Therefore, we recommend amending the proposal to clarify that **consumers must give explicit consent** to the primary use of their electronic health data.
- Consumers should be given more decision-making opportunities and more detailed choices when it comes to the data sharing, like enabling access from a specific country before travel.
- For consistency, and legal certainty to protect fundamental rights, we recommend annexing a **model consent** form to the Regulation.

2.2. Accessible health data: clarify terminology

Article 2(2)(a) defines the term 'personal electronic health data' as "data concerning health and genetic data as defined in Regulation (EU) 2016/679, as well as **data referring to determinants of health**, or data processed in relation to the provision of healthcare services, processed in an electronic form" (emphasis added).

The proposed definition is immensely broad and includes all "data referring to determinants of health…". Consequently, this definition opens up the scope of the EHDS to **all kinds of socio-demographic categories of data** such as nutrition, income, creditworthiness, housing and energy consumption. The scope of the proposed EHDS Regulation should **for the sake of predictability** remain strictly limited to **health data.**[5]

Therefore, the proposal should not introduce a new definition but instead **rely on the existing definition of 'data concerning health'** under Article 4(15) GDPR[6]. This would also guarantee consistent interpretation and avoid potential conflicts with the GDPR.

Moreover, the list of 'priority categories of electronic health data' does not entail the 'blood type' of a natural person. We consider this to be information and would recommend adding 'blood type' to the 'priority categories of electronic health data' listed in Annex 1 of the EHDS.

Additionally, the EHDS proposal (Article 4(4)) indicates that after consumers have made use of their right to restrict access, **access then has to be "authorised"** by them. However, the proposal does not provide a definition of the term "authorised". We would recommend **relying on** existing and already **defined terms.** Instead of "authorised", health professionals should have to obtain "explicit consent" from the consumer according to Article 9(2)(a) GDPR.

BEUC RECOMMENDATIONS:

- Electronic health data shall be defined in the EHDS according to the same definition as in **Article 4(15) GDPR**

[5] AK Europe, Regulation on the European Health Data Space, 31 August 2022, https://www.akeuropa.eu/en/regulation-european-health-data-space, p 6.
[6] 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

- For consistency, and legal certainty to prevent a reduction of fundamental rights protection, we recommend replacing the term "authorisation" in Article 4(4) with the existing term "explicit consent" specified in Article 9(2)(a) GDPR.
- 'Blood type' should be added to the list of 'priority categories of electronic health data' in Annex 1 of the EHDS.

2.3. Regulate access to data by health professionals

According to Article 4(1)(a) of the proposal, health professionals would have access to electronic health data of natural persons under their treatment. The provision would grant access to all priority categories of electronic health data listed in Article 5, including patient summaries, electronic prescriptions, medicines dispensed, medical images and image reports, laboratory results and discharge reports **regardless of the health professional's area of expertise** and need of data to treat a patient. Accordingly, the present draft would allow dentists to access all reports from cardiologists and other medical specialists should Member States fail to establish additional laws.

Article 4(2) identifies this problem and would allow Member States to establish rules for access to categories of personal electronic health data required by different health professions and also refers to the data minimisation principle. However, **we recommend** that Member States must be **obliged** to implement such rules.[7]

Furthermore, Article 4(3) would grant health professionals access to at least 'priority categories of electronic health data' referred to in Article 5. Since Article 4(2) permits limitations, the relationship of Article 4(2) and 4(3) requires clarification to avoid ambiguity.

BEUC RECOMMENDATIONS:

- According to Article 4(2) Member States "may" establish additional rules on what categories of health data will be accessible for different health professionals. We recommend that Member States shall be obliged to establish such rules with the legislative objective to uphold the principles of purpose limitation and data minimisation.

2.4. Improve transparency regarding access to consumers' health records

According to Article 3(10) of the proposal, natural persons "have the right to obtain information on the healthcare providers or health professionals that have accessed their electronic health data". This provision is a **positive** example of strengthening control for natural persons by **promoting transparency**.

However, the wording of Article 3(10) leaves some latitude for how this provision would be applied in practice. It is not clear whether natural persons would be **automatically notified** when their data had been accessed or if the information would only be provided **upon request**. On this issue we share the opinion of the EDPB and EDPS[8], that automatic notification is the best way to empower natural persons. As most citizens will not use EHR

[7] EDPB-EDPS, Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, p 17, Nr 62.
[8] EDPB-EDPS, Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, p 17, Nr 58.

systems on a regular basis and so will monitor who accesses their data infrequently, they will often not be aware when their data has been accessed. Moreover, it should not become an obligation for natural persons themselves to monitor compliance with protection of their personal data. Consequently, it would be easier and more efficient to **automatically notify** natural persons using a service that they use regularly (e.g. e-mail), so that they are **made aware** of when their data is accessed and they are better able to stay in control.

Nevertheless, given that not every consumer wants to receive notifications, we recommend that consumers shall have the right to choose whether they want to receive them or not.

BEUC RECOMMENDATIONS:

- Article 3(10) should be changed to: "Natural persons shall have the right to obtain **automatic notifications** …".

2.5. Promote public awareness

The EHDS proposal does not include any provisions on **informing citizens** about EHR systems and the functions provided by them. Since implementation of the EHDS is supposed to lead to a major improvement for all EU citizens as regards the handling of their electronic health data, we consider it important to inform and educate consumers about how to make use of these new tools.

BEUC RECOMMENDATION:

- The EHDS proposal must require digital health authorities to promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing of personal health data.

2.6. Prohibit discrimination

Public authorities and health care organisations must not **exclude or in any way discriminate** against EU citizens that **do not want to or simply cannot** make use of the digital health tools and services that the EHDS would enable.

BEUC RECOMMENDATIONS:

- The EHDS proposal must prohibit any form of exclusion or discrimination against individuals that decide not to allow (fully or partially) the use of their data under Chapter II of the EHDS framework.

2.7. Guarantee a high level of data security and confidentiality

The EHDS proposal does not include any specific information about organisational, technical or security aspects of the MyHealth@EU platform or the corresponding IT-infrastructure. Furthermore, **many details are left to the European Commission for implementation**, such as:

- technical specifications for the priority categories of personal electronic health data (Article 6(1))
- requirements for the registration of electronic health data by healthcare providers and natural persons (Article 7(3))
- requirements for the interoperable cross-border identification and authentication mechanism for natural persons and health professionals (Article 9(2))
- adopting necessary measures for the technical development of MyHealth@EU including detailed rules concerning security, confidentiality and protection of electronic health data and the conditions and compliance checks necessary to join and remain connected to MyHealth@EU (Article 12(4))
- allocation of responsibilities among controllers and as regards the processor (Article 12(8))
- technical aspects of supplementary services to MyHealth@EU (Article 13(1))
- technical aspects to facilitate the exchange of electronic health data with other infrastructures, such as the Clinical Patient Management System or other services or infrastructures in the health, care or social security fields which may become authorised participants to MyHealth@EU (Article 13(2))
- specifying criteria to establish whether a national contact point of a third country or a system set up at an international level is compliant with requirements of MyHealth@EU for the purposes of the electronic health data exchange (Article 13(3)).

Since MyHealth@EU facilitates access to almost all electronic health data within the EU via a central platform, the EHDS proposal needs to legally ensure the highest level of data security and confidentiality. However, the current proposal would guarantee neither data security nor confidentiality. On the contrary, almost all security and confidentiality aspects have been left to the Commission for implementation. A high level of data security and confidentiality is a pre-requisite for MyHealth@EU and must not be an afterthought, that the Commission can deal with on some undefined point in the future. To ensure this high level of security, confidentiality and protection of electronic health data the Commission should also **consult the European Union Agency for Cyber Security (ENISA).**

BEUC RECOMMENDATIONS:

- The EHDS proposal must guarantee **a high level of data security, confidentiality and protection of electronic health data for MyHealth@EU.**
- **The European Union Agency for Cyber Security (ENISA) must be duly involved in the development of any technical implementing measures** related to the security, confidentiality and protection of MyHealth@EU.

2.8. Right to lodge a 'collective' complaint

Article 11 of the proposal foresees a right to lodge a complaint with a digital health authority. The Article explicitly includes consumers' "right to lodge a complaint individually or, **where relevant, collectively,** with the digital health authority" (emphasis added). We very much welcome this provision but would suggest clarifying the terminology.

The EHDS must be added to the Annex of Directive (EU) 2020/1828 [Representative Actions Directive]

The EHDS does not further **explain or define** what must be understood as a collective complaint or how the procedure is supposed to work. To guarantee consistency and effective redress for consumers, we recommend **adding the EHDS to the Annex of the EU Directive on Representative Actions so that qualified entities can represent consumers in case of infringements of the Regulation and for redress claims.**

BEUC RECOMMENDATION:

- Introduce a new Article which amends the Annex of the Representative Actions Directive to include the EHDS Regulation:

"In the Annex of Directive (EU) 2020/1828 the following point is added: Regulation (EU) XXX of the European Parliament and of the Council on the European Health Data Space"

3. Electronic Health Record systems (Chapter III)

An electronic health record system (EHR system) is any appliance or software intended by the manufacturer to be used for storing, intermediating, importing, exporting, converting, editing or viewing electronic health records (Article 2(2)(n)). An EHR system can be manufactured and placed on the market by any natural or legal person from anywhere in the world including health care providers, insurance companies or big-tech corporations.

According to Article 17(1)(d)(e) - in combination with Article 26 and 27 - **it would be up to manufacturers themselves to ensure compliance** with the essential requirements laid down in Annex II of the Regulation for EHR systems and products claiming interoperability with EHR systems. Therefore, it would be manufacturers that would have to draw up an EU declaration of conformity and affix the CE marking. **This would amount to a self-certification regime.**

Taking into account the quantity and sensitivity of data that will be processed by such EHR systems, **we consider it necessary that a competent authority reviews and approves EHR systems before they enter the market.** A self-certification regime is not sufficient to ensure protection and security of electronic health data.[9]

[9] https://www.tagesschau.de/investigativ/ndr-wdr/gesundheitsapps-patientendaten-101.html (23.6.2022).

Recent developments in Germany reflect the problems that a self-certification regime can cause. In Germany doctors are allowed to prescribe certain health apps for treatment. A German authority must approve these apps in advance but **is not obliged to undertake technical testing.** The authority just assesses the documents that the app developer draws up himself. An independent investigation of IT experts has already revealed massive security vulnerabilities with two apps. This experience clearly demonstrates that **self-certification is not sufficient.** Health apps, as well as EHR systems, must undergo thorough technical testing **before** they enter the market.

Furthermore, according to Article 28 of the proposal, Regulation 2019/1020 would apply to EHR systems. Accordingly, market surveillance authorities would be responsible for monitoring EHR systems and Chapter III. However, market surveillance authorities are mainly concerned with the surveillance of physical products and so lack the know-how, experience and resources to assess the eligibility of such highly sensitive software tools as EHR systems.

BEUC RECOMMENDATION:

- **Avoid self-certification.** The EHDS must ensure protection and security of priority categories of electronic health data EHR systems by requiring them to be reviewed and approved by a competent authority **before entering the market.**

4. Secondary use of data (Chapter IV)

Chapter IV of the proposal aims to facilitate the secondary use of electronic health data for purposes that promote public health or are beneficial to the health sector. We welcome this approach, to allow access to non-identifiable data for the improvement of the health sector or the development of health technologies. In particular, we see great potential in improving the situation for researchers.

Nevertheless, this privileged access for secondary use must not undermine the protection of individual's personal data and must not make sensitive health data a public good that can be harnessed for commercial profit. Moreover, the EHDS must establish rules to ensure that this **privileged right to access sensitive private health information** shall only be granted **for the benefit of the public and not for private businesses.**

The proposed Regulation would require Member States to designate one or more **health data access bodies** responsible for granting access to electronic health data for secondary use. These bodies would be in charge of verifying applications, anonymising or pseudonymising data and providing a secure processing environment and therefore **bear a heavy responsibility.** It is therefore important not to undercut their competences and to give them the powers and resources commensurate with their tasks.

4.1. Business innovations

One of the proposal's major targets for the secondary use of data is to boost the data driven economy by facilitating businesses access to electronic health data according to Article 33. Hence, Article 45 of the proposal foresees that "any natural or legal person" could submit a data access application and get access to anonymised or pseudonymised electronic health data if their intended purpose was in line with one of the legitimate purposes defined by Article 34(1). Consequently, according to Articles 34(1)(f)(g)(h), businesses could apply for access for "development and innovation activities" and/or "training, testing and evaluation of algorithms" as long as they contributed to public health, social security or ensured a high level of quality and safety of health care, of medicinal products or of medical devices and/or "for providing personalised health care consisting in assessing, maintaining or restoring the state of health or natural persons, based on the health data of other natural persons".

Under the proposal, the protection of personal data would be primarily ensured through **anonymisation and pseudonymisation.** Nevertheless, the proposal does not specify any minimum requirements for this anonymisation or pseudonymisation (see point 4.2). As a result, any technique could be applied, even if it did not sufficiently protect the electronic health data from re-identification.

Allowing access to health data purely for business purposes puts the protection of the rights and freedoms of individuals at risk and should not be allowed

Moreover, the proposal does not foresee **any boundaries** when it comes to the **amount of data that can be requested.** Accordingly, businesses could (potentially) request an unlimited amount of information from European consumers. Whether access would be granted would solely depend on whether the intended purpose was able to contribute to public health, social security or ensure a high level of quality and safety of health care, of medicinal products or of medical devices. Moreover, this wording allows a very broad interpretation of what can be understood as "contributing to".

Furthermore, the proposal would give any natural or legal person access to that data. Because of the sensitive nature and the potentially large amount of data accessed, there is **a high risk that the protection of fundamental rights** of consumers involved would be compromised. Consequently, we consider that **only** eligible applicants should gain access.[10] However, under the current proposal **anyone could request access to an unlimited amount of highly sensitive data**. That includes businesses or political parties that consumers might simply not want to support.

Given the profound intrusion into the personal health data of EU citizens, and the imminent risk of re-identification, that the EHDS proposal would enable for business purposes, we consider that **such privileged access** to electronic health data **is unjustified.** On the contrary, allowing businesses access to consumers' health data e.g. collected from wellness applications, would give consumers the feeling of **losing control over their data** and **diminish trust** in the safeguards and protections that the GDPR has built.

BEUC RECOMMENDATION:

- Because of the severity of the potential risk to the rights and freedoms of European citizens, we recommend **deleting Article 34(1)(f)(g)(h)** as these provisions

[10] See similar restrictions in Directive 2020/1828 (Representative Action Directive). There only 'qualified entities', that have to fulfil certain criteria, are eligible to file representative actions.

would enable businesses to access potentially unlimited amounts of health data for very broadly defined purposes.

4.2. Anonymisation and pseudonymisation

According to Article 44(2) of the proposal, the health data access bodies would have to provide the electronic health data in an anonymised format, where the purpose could be achieved with such data. Otherwise, under Article 44(3), access could be provided to electronic health data in pseudonymised format.

However, **effective anonymisation is difficult to achieve.** It requires expertise, know-how and resources. The Article 29 Working Party, the independent body that dealt with issues relating to the protection of privacy and personal data until it was replaced by the European Data Protection Board set up by the GDPR, explained the difficulties and risks that anonymisation entails and provided guidance on standard techniques (WP216, Opinion 5/2014 on Anonymisation Techniques, adopted on 10 April 2014). Pseudonymisation is even more problematic since the re-identification of natural persons is by definition always possible.

Although anonymisation and pseudonymisation **are the key safeguards to guarantee protection of the sensitive electronic health data of consumers,** the EHDS **does not define the terms or set any minimum requirements.** Consumers are therefore left in the dark about the level of protection that the EHDS could provide. As a result of this lack of definition, health data access bodies could not be held accountable if they delivered insufficient 'anonymisation'.

The Commission seems to be aware of these risks involved with anonymisation and pseudonymisation. Recital 64 of the proposal addresses the problem with re-identification and refers to Article 5(13) of the Data Governance Act (COM/2020/767 final) and the Delegated Act under the empowerment granted by this Article.

BEUC RECOMMENDATION:

- Given the possible risks of ineffectively anonymised and pseudonymised data processed and shared under the Act becoming personally identifiable, be it via cross-referencing with other data or other forms of re-identification, the EHDS proposal should include specific provisions, including **minimum quality requirements for mandatory anonymisation and pseudonymisation**, to prevent such practices throughout the value chain. These should take the form of specific requirements for anonymisation or specific standards to ensure its robustness.[11] This may possibly require the introduction of stronger protection concepts,[12] with far-reaching requirements intended to make re-identification impossible or at least considerably more difficult.

4.3. Genetic, genomic and proteomic data

According to Article 33(1)(e) of the proposal, **genetic, genomic and proteomic data** will be accessible for secondary use. This means, that those data can be accessed by political parties, businesses, private persons, researchers and other entities for the purposes outlined in Article 34. As a matter of fact, genetic, genomic and proteomic data are highly

[11] See also vzbv (2022) p. 16.
[12] For a more in-depth discussion, see vzbv (2022) p. 14.

sensitive and **can practically not be anonymised**. As a result, there is an **inherent risk of re-identification.** Furthermore, genetic, genomic and proteomic data that refer to a natural person **can never be changed.** That information constitutes highly sensitive data due to their comprehensive nature and long-term predictive potential concerning health, illness, also future illnesses, healing, ethnic origin and family lineage. Such data allows conclusions to be drawn also for blood relatives, influences elementary decisions of the persons concerned and is mostly unknown in terms of its meaning and significance even to the individuals themselves. **Genetic, genomic and proteomic data are therefore associated with a high risk of discrimination.**

In order to make such highly sensitive data available for secondary use, concrete and realistic benefits must be apparent to consumers. Such benefits might in principle be present when it comes to scientific research, but not to any of the other legitimate purposes listed in Article 34. **The risks of granting access to genetic, genomic and proteomic data for all these purposes are very high and outweigh the potential benefits involved.** Moreover, it is important to underline that it would of course still possible to make use of such data in compliance with the GDPR, which even foresees specific exemptions for scientific research under Article 89.

BEUC RECOMMENDATION:

- **Genetic, genomic and proteomic data** must be excluded from the scope of Chapter IV, Article 33(1)(e).

4.4. Bypassing the health data access body

According to Article 49 of the proposal, when an applicant requests access to electronic health data **only from a single data holder** in a single Member State, that request could be filed directly to the data holder. In such a case, **data holders could themselves issue a data permit.** If the data holder granted access, **they would have to provide the electronic health data in a secure processing environment.**

Although Article 49 would require a data holder to comply with the relevant provisions (Article 45, 47, 50 and 42), **the health data access body would not be involved at all in the assessment or in the preparation or granting access to data.** Data holders would therefore be themselves responsible for:

- verifying the legitimacy of the purpose
- anonymising or pseudonymising the electronic health data
- providing a secure processing environment and
- applying the data minimisation and purpose limitation principles.

Not all data holders are likely to have the resources and IT expertise necessary to undertake these tasks. Nevertheless, data holders could charge fees (Article 42) for undertaking these services according to Article 49(2). This is likely to encourage data holders to take on these difficult tasks themselves.

The tasks of the health data access bodies would be to guarantee compliance with the EHDS and provide security for the accessible data. Their role is key to protecting consumers and preventing abuses of the EHDS system. From a consumer perspective, allowing data holders to provide access to potentially large amounts of sensitive information, **without having an independent authority involved** to guarantee the protection of the personal data of the affected consumers, would severely compromise the rights and freedoms of natural persons.

BEUC RECOMMENDATION:

- It should not be possible to bypass the health data access bodies. **Article 49 must be deleted.**

4.5. Person generated electronic health data including wellness applications

The European Health Data Space proposal would open access to a number of highly sensitive types of electronic health data. **Specifically** included **are "person generated electronic health data,** including data from medical devices, **wellness applications or other digital health applications"** (Article 33(1)(f), emphasis added). Also included are "electronic data related to … **lifestyle, wellness** and behaviour data relevant to health" (see Article 33(1)(n), emphasis added).

The first problem with this aspect of the proposal is that the use of the vague and unspecific term 'wellness applications' would lead to a very broad scope that includes a high number of apps used by consumers on a daily basis. Nevertheless, consumers would not receive any individual notification that their data was accessible or had been accessed. Not only does the proposal not foresee such a provision but Recital 44 explicitly recommends that this information should not be provided. Nor would consumers have any rights to **restrict** (contrary to what is foreseen when it comes to primary use of data) or **reject access** (see below (point 4.6) our recommendation for a right to opt-out from secondary use).

As a result, even for well-informed consumers, it would be difficult to understand which specific apps would share their health data and which not. For example, Article 33(1)(n) includes the very broad term "behaviour data relevant to health". As we know, social media apps can cause mental illnesses like depression or anorexia. As a result, behaviour data generated by social media apps can be considered to be "relevant to health" and would therefore be accessible for secondary use. The same conclusion can be drawn for data related to "professional status" – maybe LinkedIn? – and to "education" – maybe even a language app like Duolingo? In any case, the **intrusion into the privacy of consumers would be enormous.**

The second problem is that Article 33(1)(f) would give access to **person generated health data, including data from medical devices.** Medical devices are defined as devices that help treat and/or alleviate diseases, disabilities (etc). Such devices may even be **implanted into the body of natural persons** (e.g. blood sugar meters for diabetes patients). Although making such data accessible for secondary use can have positive effects for public health, the right to individual privacy should not be abolished completely. For instance, private businesses and governments do not have a comparable legal right to walk into our private houses and/or bedrooms to gather information to improve policy-making or develop products even if this could bring benefits in some circumstances. Nevertheless, Article 33(1)(f) would not only facilitate access to our private premises **but to data collected from the inside of our bodies**, from devices that **many consumers' health depends on.** Despite potentially good intentions, the ends do not justify all the means. What is protected offline should also be protected online. Consequently, it is important to protect those highly private spaces of citizens and allow access **only with consent** (see also the qualified protection of information stored in the terminal equipment of a consumer under the ePrivacy Directive 2009/136/EC).

The third problem is that there are numerous concerns as to **the quality and reliability** of data gathered via apps and connected devices and the **potential risk that products, services, or regulatory activities based on them** may have for consumers. Applicants

would have no possibility or legal right to assess the quality of the accessed data. This is likely to be a serious problem for data provided by **wellness apps**. Typically, **users themselves** are responsible for measuring and collecting those data. The quality of the collected data therefore depends heavily on the reliability of the users and the measuring devices. Additionally, data holders are not obliged to provide a description of how data has been collected.

Also, it is very unlikely that applicants would detect false measurements or data-biases from the data received. As a result, once access had been granted, there would be no additional safeguards to protect consumers from products, services or regulatory activities based on flawed or biased data.

The Commission seems to be aware of this problem and the risks of secondary use of low-quality or biased data. The proposal therefore includes the possibility to make use of data-quality labels (Article 56). Nevertheless, **labelling data would be a voluntary** option that could therefore not be seen as a sufficient safeguard.

In practice, there is a high risk that businesses, policy makers and researchers would base their work and decisions on low-quality and biased data. That would inevitably **lead to biased AI algorithms** and **false scientific conclusions and flawed 'health' products and services**. As a result, consumers would be confronted with ineffective or even harmful health applications, medical devices or political decisions. To reduce these risks, we recommend excluding person generated and lifestyle, wellness and behaviour data from Article 33(1)(f)(n).

BEUC RECOMMENDATION:

- Remove Art 33(1)(f). The 'minimum categories of electronic data for secondary use' **must exclude** "person generated electronic health data" from their scope, including data from "medical devices, wellness applications or other digital health applications".
- Remove **"lifestyle, wellness and behaviour data relevant to health"** from Article 33(1)(n).

4.6. Automatic data permits

Article 46 of the proposal would regulate how a health data access body has to handle a data request. In the first instance, health data access bodies would have two months to issue a data permit. This period could be extended by two additional months where necessary. Nevertheless, the last sentence of Article 46(3) foresees that: "Where a health data access body **fails to provide a decision** within the time limit, **the data permit shall be issued."**

Such **automatic granting of data permits without any assessment is unacceptable.** If a health data access body failed to provide a decision in time, e.g. because it was understaffed or received too many requests, the solution should never be **automatic approval** of those requests**.** This provision undermines the principles of the rule of law, the rights and freedoms of consumers as well as the importance of the tasks of the health data access bodies to protect them.

BEUC RECOMMENDATION:

- **Data permits should not be granted automatically if the health data access body does not respond to a request.** The sentence "Where a health data access body fails to provide a decision within the time limit, the data permit shall be issued" must be deleted from Article 46(3).

4.7. Right to opt-out of Chapter IV

Chapter IV of the EHDS proposal would introduce new rights to access and reuse electronic health data of EU citizens.[13] In practice this would mean that anonymised or pseudonymised electronic health data, could be accessed by anyone. As a result, Chapter IV would put **applicants to use electronic health data in a privileged position.**

Consumers on the contrary, **would not get any additional rights or in practice even be informed about the processing of their data.** There are two reasons for that. Firstly, anonymised data are not considered to be personal data and therefore do not fall under the scope of the GDPR. Secondly, for the remaining pseudonymised data, according to Article 38(2), health data access bodies would not be obliged to provide the specific information under Article 14 GDPR. This is further clarified in Recital 44, that states that Article 14(5) GDPR would apply, and that health data access bodies would be exempted from the information obligations under Article 14 GDPR. Thus, health data access bodies would only have to provide "general information concerning the conditions for the secondary use". As a result, consumers would not receive any individual information when their data was accessed.

In order to **redress this imbalance** and to put consumers back in control of their personal data, we suggest implementing **a right to opt-out from Chapter IV** of the EHDS proposal. This right to opt-out would prohibit electronic health data from consumers from being accessible for secondary use if the consumers concerned objected. Our suggestion is that health data access bodies would have to establish a register where consumers could declare their wish to opt-out from the secondary use of their data. This would ensure that whenever a health data access body prepared electronic health data to be accessed by applicants, they could remove the data of those consumers that had declared their wish to opt-out.

To set a standard and make it easy for consumers, we recommend that health data access bodies provide an opt-out template.

BEUC RECOMMENDATION:

- Consumers must have a **right to opt-out** from their personal electronic health data being available **for secondary use.**
- Health data access bodies should **provide an opt-out template** for consumers.

4.8. Lack of a general prohibition on using health data for advertising

Article 35 of the proposal prohibits the secondary use of health data for a number of specified reasons that includes e.g. using data against persons, **advertising or marketing, excluding people from insurance contracts or increasing their**

[13] Excluded are only data that reside with micro, small or medium sized enterprises.

premiums, or developing dangerous products. Overall, BEUC welcomes this list of prohibited purposes but would prefer **a broader approach** when it comes to the prohibition of **advertising or marketing activities.** Article 35(c) prohibits advertising or marketing activities "**towards** health professionals, organisations in health or natural persons". Advertising toward organisations that are **not in the health sector would** - according to the wording - **not be prohibited.** The target audience of the adverts should not be the deciding factor for whether or not the use of the data for this purpose is admissible.

BEUC RECOMMENDATION:

- The **processing of health data for all advertising purposes should be prohibited, regardless of the target audience**. The sentence "towards health professionals, organisations in health or natural persons" should therefore be deleted from Article 35(c).

4.9. Public return on granting access

Chapter IV of the proposal introduces a right to access electronic health data from Europeans. This right to access must be considered as a privilege, because without it, applicants would require consent from data holders and/or individuals concerned and would most likely have to pay for using this data. As a result, individuals should also share in any success that stems from their data.

We take positive note of Article 46(11)(12) and Article 38(3), which would require that results and/or output of secondary use would have to be shared publicly and that relevant findings that could have an impact on the health of an individual would be forwarded to them or their health professionals. This is a first and important step to improve public health and social security.

A second step concerns the commercial use of those results and outputs following secondary use of electronic health data under Article 33(1)(f)(g)(h). Although services and products developed with secondary use of health data would have to "contribute to" public health and/or health care, businesses and innovators would not be subject to any more specific conditions when offering them on the market. This would also imply that they could ask for any price that they considered reasonable, irrespective of whether consumers could afford them or not.

Among other things, the EHDS proposal is meant to unlock access to health data to develop better healthcare services and treatments. **The increased access to such data should result in the longer term in more affordable and accessible health technologies** and effectively "contribute to public health or social security …" as outlined in e.g., Article 33(1)(f)(g).

BEUC RECOMMENDATION:

- We recommend adding a Recital stating that "Member States should provide a multiannual strategy for ensuring that secondary use of data results in the longer term in more affordable and accessible health technologies for everyone."

4.10. Implementing and Delegated Acts

As with Chapter II (primary use of data), Chapter IV also leaves many important details to implementing or delegated acts. For example, the Commission would be empowered to determine, by means of implementing acts:

- requirements, technical specifications, the IT architecture of HealthData@EU, conditions and compliance checks for authorised participants to join and remain connected to HealthData@EU and conditions for temporary or definitive exclusion from HealthData@EU (Article 52(13)(a))
- the minimum criteria to be met by the authorised participants in the infrastructure (Article 52(13)(b))
- the responsibilities of the joint controllers and processor(s) participating in the cross-border infrastructures (Article 52(13)(c))
- the responsibilities of the joint controllers and processor(s) for the secure environment managed by the Commission (Article 52(13)(d))
- common specifications for the interoperability and architecture concerning HealthData@EU with other common European data spaces (Article 52(13)(e))
- the minimum specifications for cross-border datasets for secondary use of electronic health data, taking into account existing Union infrastructures, standards, guidelines and recommendations (Article 58).

In addition, the European Commission would be empowered to adopt delegated acts to:

- **amend the list of 'minimum categories of electronic data'** to adapt it to the evolution of available electronic health data (Article 33(7))
- amend the list of **aspects to be covered by a data permit** in paragraph 7 of Article 46.

From the perspective of a consumer, the **EHDS proposal does not therefore conclusively clarify what types of data would be considered as 'minimum categories of electronic data'** and hence, accessible for secondary use. Moreover, it remains unclear which technical specifications the HealthData@EU platform would provide to protect sensitive consumer health data. These very relevant details need to be defined within the EHDS Regulation before any natural or legal person can access the electronic health data concerned.

BEUC RECOMMENDATION:

- Delete Article 33(7) "The Commission is empowered to adopt delegated acts in accordance with Article 67 to amend the list in paragraph 1 to adapt it to the evolution of available electronic health data".
- The EHDS proposal must guarantee **a high level of data security, confidentiality and protection of electronic data** for HealthData@EU (Article 52(13)(a)) and should **the European Union Agency for Cyber Security (ENISA) should be involved to ensure that**.

END

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.