BEUC The European Consumer Organisation

The Consumer Voice in Europe

# AI MUST BE SMART ABOUT OUR HEALTH

## BEUC POSITION ON ARTIFICIAL INTELLIGENCE IN HEALTHCARE

**Contact: Jelena Malinina – health@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-2019-078 - 02/12/2019

## Why it matters to consumers

We utilise more and more digital products and services to manage our health. Devices, apps, social media, platforms collect enormous amount of data about us. When combined with new analytical tools such as artificial intelligence (AI), use of this data can bring significant changes or even entirely transform the way we are diagnosed, treated and cared for. However, the use of AI in healthcare raises concerns, notably in relation to the trustworthiness of this technology and its impact on consumer health and privacy. There is a strong need for comprehensive safeguards to ensure AI benefits us without compromising our protections, fundamental rights and freedoms.

# RECOMMENDATIONS

AI is a complex phenomenon requiring a multi-dimensional change in the way we conduct medical research, regulate the medical profession and healthcare companies, and use biomedical data. Health data is recognised as a special category of data under the General Data Protection Regulation due to its sensitivity.[1] Thus, AI uses in health also requires a special, *vertical* regulatory approach, in addition to ensuring a strong *horizontal* cross-sector regulation of AI.[2] [3] BEUC's key recommendations to ensure that the application of AI in healthcare benefit patients and consumers are as follows:

- Patients and consumers should have the following enforceable rights[4]:

  - right to transparency, explanation and objection;
  - right to accountability and control;
  - right to fairness;
  - right to non-discrimination;
  - right to safety and security;
  - right to access to justice;
  - right to reliability and robustness.

- The EU should establish a legal framework for AI as well as update laws that are relevant for the health sector such as EU safety and liability legal frameworks to ensure that they are fit for purpose and that patients and consumers are well protected with regards to the use of AI in medical devices and health services.

[1] General Data Protection Regulation, 2016/679, Article 9: https://eur-lex.europa.eu/eli/reg/2016/679/oj
[2] BEUC Position Paper, Automated Decision Making And Artificial Intelligence - a Consumer Perspective, June 2018,https://www.beuc.eu/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf
[3] BEUC Position Paper, AI Rights for Consumers, October 2019, https://www.beuc.eu/publications/beuc-x-2019-063_ai_rights_for_consumers.pdf

- Ethics are a fundamental basis of the medical research and medical profession, particularly in the context of healthcare. However, AI can only be used when supported by changes in the existing regulatory frameworks and the establishment of universal, comprehensive and binding AI legislation including patient/consumer-centred safeguards.

- The EU should identify and promote best practices ensuring robustness[5] of AI systems in the health sector both at the stages of development and actual use to reduce potential biases and errors of AI-based decision-making.

- The EU and the Member States should ensure that the new Medical Devices Regulation and In-Vitro Diagnostic Regulation are implemented with a view to new technologies: guidelines and specifications are needed for the evaluation of safety and effectiveness of software, AI and deep learning powered devices throughout the entire usage cycle.

- The EU and the Member States should conduct regulatory assessments of the medical professions frameworks to determine whether they are fit for the use of patient/consumer-centred AI in health.

- The EU and Member States must ensure that AI in healthcare is applied in full respect of EU data protection rules, while observing the balance between the interests of advancements in medical research and patient/ consumer protection. This must be achieved through diligent implementation of the GDPR principles and adequate use of provisions and exemptions on health research.

- During the evaluation and review report of the EU data protection legislation which is due in May 2020, the European Commission should specifically evaluate the need to establish rules on (1) anonymisation techniques of health data; (2) data access and control when it comes to use of data coming from multiply sources; and (3) quality and safety standards for all information systems where health data is processed.

- The EU should establish a pan-European network of Health Research Ethics Committees that could develop guidelines for AI assessment in health research.

- The EU and Member States should put in place mechanisms to ensure professional and educational assistance to both patients and the healthcare professionals to better understand and assess AI decision-making.

[5] According to EC's Ethics Guidelines on Trustworthy AI (2019), robustness requires that AI systems be developed with a preventative approach to risks and in a manner such that they reliably behave as intended while minimising unintentional and unexpected harm and preventing unacceptable harm. This should also apply to potential changes in their operating environment or the presence of other agents (human and artificial) that may interact with the system in an adversarial manner. In addition, the physical and mental integrity of humans should be ensured.

# Contents

## Healthcare Products are Changing

**Legal frameworks must be adjusted to the change brought up by the technology.**

Healthcare products and services are rapidly changing due to new digital technologies.[6] Electronic health record (EHR), medical websites, and a plethora of health and wellness apps offer patients and consumers an opportunity to better manage their own health, connect to their health providers and easily access their medical information. These devices and services generate enormous amount of health and non-health data from its millions of users.

Does this data have a value? Yes and no: terabytes of data remain terabytes of data unless the information is analysed and put into a specific context. This is where new digital technologies come at hand. Artificial intelligence (AI) and algorithms can perform a variety of analytical tasks based on specific purposes and/or instructions. The more data is available, the more AI can learn, adapt and improve its precision, a process known as machine learning. Accordingly, AI has become a hot topic in the digital world and climbed to the top of the political agenda.

AI has been identified as one of five key issues for the current term of the European Parliament, elected in May 2019, by the European consumer movement.[7] It is also a top priority for the EU which aims to promote AI technology and increase public and private investments in it to at least €20 billion annually over the next decade.[8] The new European Commission President-elect Ursula von der Leyen also committed to put forward legislation for a coordinated European approach on the human and ethical implications of AI in the first 100 days from the beginning of the European Commission's mandate.[9]

In 2019, the EU's High-Level Expert Group on Artificial Intelligence published the Ethics Guidelines on AI[10] along with the Policy and Investment Recommendations.[11] The group, of which BEUC is a member, recognises health as one of the key sectors for AI application and highlights key elements of trustworthy AI:

- Human agency and oversight;
- Technical robustness and safety;
- Privacy and data governance;
- Transparency;
- Diversity, non-discrimination and fairness;
- Societal and environmental well-being;
- Accountability.

[6] BEUC Position Paper, Digital Health. Principles and Recommendations, October 2018, https://www.beuc.eu/publications/beuc-x-2018-090_digital_health_-_principles_and_recommendations.pdf

[7] BEUC Paper, Consumer Priorities for European Parliament Elections, May 2019, https://www.beuc.eu/publications/beuc-x-2018-107-consumer_priorities_for_the_2019_european_parliament_elections.pdf

[8] European Commission, Factsheet: Artificial Intelligence for Europe, July 2019, https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe

[9] European Commission, Political Guidelines for the Next European Commission 2019-2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[10] European Commission's High Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, April 2019, https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top

[11] European Commission's High Level Expert Group on Artificial Intelligence, Policy and Investment Recommendations for Trustworthy Artificial Intelligence, June 2019, https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence

This paper set outs BEUC's position on this area and provides recommendations for necessary regulatory safeguards to protect the health and well-being of patients and consumers. It is built on BEUC's general position paper on *'Automated Decision Making and Artificial Intelligence - A Consumer Perspective'*,[12] as well as on BEUC's 'AI Rights for Consumers'[13].

## Promises and Risks

**Health-specific safeguards are needed in addition to common regulatory AI framework.**

The high interest in AI is predominantly based on the technology's promise to deeply change our societies and result in increased convenience and efficiency for consumers. More than for other sectors, AI is claimed to hold great potential to revolutionise our health systems and medical services. AI in health promises to deliver precise diagnosis, personalised treatments, better care and other benefits.[14]

However, special attention must be given to health-specific safeguards (vertical regulation), in addition to common regulatory needs relevant for all sectors (horizontal regulation).[15] The need for protection already starts at the level of data-collection. All AI-driven benefits come with a condition to have as much data available as possible for the machine to perform the task at its best. However, a large proportion of this data is personal and sensitive, as it contains a lot of details about patients' and consumers' health. This raises new questions of personal data protection in the context of AI, as well as concerns over the trustworthiness of algorithm-powered diagnosis, transparency and ethical use of AI and the level of responsibility and liability of the developers and healthcare professionals. Patients and consumers need clear legally defined rights when it comes to use of AI in healthcare sector:

| | |
|---|---|
| **right to transparency, explanation and objection** | Patients and consumers must be able to have an explanation on how the decision on their health was made; they must be informed on the use of AI for diagnostic/treatment purpose and have a right to object the decision and seek for a second opinion. |
| **right to accountability and control** | Algorithm-based tools in health must undergo a thorough assessment before their launch. Throughout products lifecycle, their performance must be monitored and assessed by the deployers and dedicated authorities. |
| **right to fairness** | Fairness of algorithms used in healthcare must be insured to avoid potential bias in decision-making. |
| **right to non-discrimination** | Personal medical data is highly sensitive, thus uses of AI in health must be thoroughly and independently monitored to prevent discrimination and deepening of health inequalities between different populations. |

[12] BEUC Position Paper, Automated Decision Making And Artificial Intelligence - a Consumer Perspective, June 2018, https://www.beuc.eu/publications/beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf

[13] BEUC Position Paper, AI Rights for Consumers, October 2019, https://www.beuc.eu/publications/beuc-x-2019-063_ai_rights_for_consumers.pdf

[14] See e.g. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341692

[15] BEUC Position Paper, *Automated Decision Making And Artificial Intelligence - a Consumer Perspective*, June 2018,https://www.beuc.eu/publications/beuc-x-2018 058_automated_decision_making_and_artificial_intelligence.pdf

| | |
|---|---|
| **right to safety and security** | AI tools in healthcare must be safe and secure by design and by default. |
| **right to access to justice** | In case of damage occurring due to AI, patients and consumers must have a right to redress and public enforcement. |
| **right to reliability and robustness** | Algorithms in healthcare must be constantly scrutinised to ensure their high reliability and trustworthiness. |

## PRIMUM NON NOCERE (*FIRST, DO NOT HARM)* BASED AI

Since ancient times, medical progress has been driven by this Hippocratic principles – *primum non nocere*, which means 'first, do not harm'. AI in healthcare cannot be an exception but must follow the same principle as any other medical advances of 'first, do not harm', in order to serve people at its best. Medical research and practice are key elements of healthcare and this section is aimed to look whether the current practices are ready for the technological advancements.

### AI and Ethics

**Ethics for AI are necessary but by far not sufficient.**

There is a clear need to ensure that AI products and solutions in healthcare are ethical and in line with the core principles of medical research and practice. BEUC considers that the development of an ethical approach to the application of AI in healthcare is necessary. Nonetheless, non-binding ethical principles certainly do not ensure adequate protection for consumers.

At the EU level, the Ethics Guidelines for Trustworthy AI[16] developed by the European Commission's High-Level Expert Group on Artificial Intelligence, of which BEUC is a member, can be useful but binding legislation is needed to achieve consumer-centred AI development and application.

The Guidelines put forward several important principles such as transparency, non-discrimination, accountability, safety, oversight etc. Far from being novel, these principles already exist in EU legislation, for example, in consumer, data protection, and competition law.

For AI to deliver on its promise, consumers must trust the technology; this among others implies that they must have a possibility of knowing and having a say on how their data is used. In this respect, following ethical principles throughout the whole AI development and use cycle is a must. However, for ethics not to become an occasionally applied principle, AI can only be used when based on a strong regulatory framework(s) with universal, comprehensive and binding AI principles and consumer-centred safeguards. **The next step for the EU to take is therefore to look at both horizontal (cross-sector) and vertical (sector-specific, e.g. health) regulation of AI.**

[16] European Commission's High Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, April 2019, https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top

## AI and Health Research

**Medical research practice needs to be adopted to better assess AI and uses of big data.**

Human research has always been a driver for the medical progress. However, it involves significant risks, and therefore, in the modern practice, health research is a closely monitored and regulated activity based on universal ethical principles.

It is important that an ethical approach to AI is applied already at the health research and product development stage. In the current practice of health research this is not properly done. At present, the Research Ethics Committees (RECs), which protect the rights and well-being of research participants, struggle to assess the risks and benefits of research projects involving big data and big data analytics. Traditional tools and legal requirements for ethics review in clinical research, such as informed consent or minimal risk, is often of limited value when it comes to the evaluation of big data projects, simply because these criteria were not defined with big data health research in mind. Informed consent is, for example, often not practical to obtain for studies involving a retrospective analysis of data from millions of individuals.[17]

Big data further challenges the mandate of the RECs: studies involving publicly available and anonymised data have traditionally been perceived to be outside of the RECs review. However, this is problematic, as big data analytics can reveal sensitive information, given that anonymised data can be de-anonymised.[18] **Therefore, BEUC recommends reconsidering the role of RECs to ensure their involvement in the review of research projects based on anonymised data. This involvement should be ensured at both national level and in international health research. There is also a need to develop concrete criteria of big data/AI assessment by the RECs on the following:**

- whether and how each project attempts to address the social benefits, if any, of research;
- how data subjects involved in the study can exercise control over their data;
- how data is collected, stored and shared;
- whether patient(s) consented to the use of data;
- which measures of accountability are being employed by the researchers; and,
- whether the collected data can be reused for secondary purposes and what measures are implemented to prevent that.[19]

[17] Balas EA, Vernon M, Magrabi F, Gordon LT, Sexton J, editors. Big Data Clinical Research: Validity, Ethics, and Regulation. MedInfo; 2015.
[18] Sun, Chloe & Yu, Jiguo & Jiang, Honglu & Chen, Yixian & Cheng, Xiuzhen. (2019). De-anonymizing Scale-Free Social Networks by Using Spectrum Partitioning Method. Procedia Computer Science. 147. 441-445. 10.1016/j.procs.2019.01.262.
[19] Ibid

### Why data quality matters

AI can greatly help physicians in disease diagnosis and treatment prescription, but it must always be kept in mind that while training an algorithm there is the risk of feeding the software not only with loads of data but also underlying biases.

IBM Watson for Oncology is one of the best-known AI examples of why data quality matters. IBM began selling Watson to recommend the best cancer treatments to doctors around the world. Practical experience, however, showed that Watson for Oncology often resulted in unsafe and incorrect treatment recommendations. Watson's algorithm was largely based on the data of American patients and care methods, and it created a bias against patients at foreign hospitals, as their methods were not considered for the initial coding of algorithm.[20]

## AI and Medical Practice

**Clarity on how AI should be used in the medical practice is required.**

AI-powered tools can be used in a variety of ways in the medical field: from predicting infectious disease epidemics to performing surgeries. For instance, AI diagnostic tools could help doctors to analyse X-ray images, and thus, speed up the diagnosis and reduce the need for more invasive diagnostic procedures. On average, 10% of mammography screenings have inconclusive results for breast cancer and require further biopsies which can often cause major mental and physical discomfort for patients.[21] AI tools could remedy this situation.

AI in medical practice can be used as an assisting tool for healthcare professionals or it can be incorporated into the medical device. However, adoption of novel technologies into medical practice raises questions of: (1) the responsibility of healthcare professionals; (2) how to ensure transparency on /information about the utilised algorithm; and (3) human autonomy.

### Lack of clarity on the responsibility

The responsibility of healthcare professionals towards patients is rather straightforward. The right to health is a fundamental one in our societies subject to legal protection.[22] Furthermore, medical professions and services are regulated by a number of laws and constitutional provisions that are legally binding. Thus, in addition to a strong ethical basis, there are clear legal obligations for the healthcare professionals when it comes to accountability and liability, for instance. To determine when 'something went wrong', doctors' actions and decision-making paths are assessed. However, in the context of AI use in medical practice there is no regulatory framework which would determine to what

[20] Statnews, IBM pitched its Watson supercomputer as a revolution in cancer care. It's nowhere close, September 2017, https://www.statnews.com/2017/09/05/watson-ibm-cancer/

[21] Shah R, Chircu A. Iot and AI In Healthcare: A Systematic Literature Review, Issues in Information Systems. 2018 Jul 1;19(3).

[22] Office of the United Nations High Commissioner for Human Rights, the World Health Organisation, The Right to Health, June 2008, https://www.ohchr.org/Documents/Publications/Factsheet31.pdf

extent doctors can rely on a machine incapable of understanding the value of human life. If an AI-powered device is defective and causes harm to a patient, the rules on product liability should apply. However, existing liability rules do not extend to digital content products and services[23], which further deepens the gap in patient and consumer protection in case AI causes damages.

Before any wide application of AI in medical practice, **BEUC recommends that:**

- The European Commission and Member States conduct regulatory assessments of medical professions frameworks to determine whether they are fit for the use of consumer-centred AI in health. E.g. through establishing rules on healthcare professionals', developers' responsibility and liability when AI is involved into medical decision-making.
- The EU updates EU horizontal consumer law as well as the EU safety and liability legal frameworks to ensure that they are fit for purpose in the context of AI.

### Lack of transparency

According to BEUC Member Verbraucherzentrale Bundesverband – vzbv, German consumers feel insecure about the growing use of AI processes: only 18% see more opportunities than risks when decisions are made on the basis of algorithms.[24]

Thus, in addition to clear regulatory requirements on accountability and liability, there is a need to ensure algorithmic transparency, so it is possible to track the moment when 'things got wrong', and allow for a timely intervention by healthcare professional in case machines made a mistake. Algorithmic transparency is also crucial to ensure patient and consumer right to information and explanation.

Transparency is also an essential element to assess clinical validity of algorithms used in healthcare. Already starting from clinical investigations, explainability is required to justify clinical validation of the algorithm-based product. However, if a system is protected by intellectual property rights or trade secrets, it would result in *'blackbox algorithms'*, making them impossible to assess. Even in case of transparent algorithms, the trustworthiness of clinical validation might be put in question as there are no clearly established legally binding assessment criteria to evaluate the validity of such systems. To make sure algorithms used in healthcare are reliable, robust and transparent, **BEUC recommends that the EU promotes:**

- Clear standards and legally binding assessment criteria to ensure transparency of AI systems in healthcare.
- Usage of high-quality health data for the development of AI applications to reduce errors of AI-based decision-making and ensure its reliability.

### Problem of human autonomy

Algorithmic transparency is crucial to prevent situations where medical decision-making is done in a 'black box' environment. Black-box algorithms that make inexplicable decisions are unacceptable in any sector but in a context where decisions have an impact on life or death the consequences of algorithmic failure could be grave.

[23] BEUC Position Paper, Review of Product Liability Rules, April 2017, https://www.beuc.eu/publications/beuc-x-2017-039_csc_review_of_product_liability_rules.pdf

[24] Verbraucherzentrale Bundesverband – vzbv, Artificial Intelligence: Trust Is Good, Control Is Better, April 2019, https://www.vzbv.de/sites/default/files/downloads/2019/04/04/2019_vzbv_factsheet_artificial_intelligence.pdf

Even without going to extremes, it is important that AI decisions can be explained and challenged, if needed, to ensure human autonomy in the decision-making process and avoid overreliance on the technology.

**How AI affects decision-making**

A study[25] investigating human-automation interaction found out that when the system provided the correct decision support recommendation, the participants' decision-making was faster and more accurate. But when the system gave an incorrect recommendation, participant's decision-making performance dropped to near zero. The participants assumed the system was correct and took a wrong action themselves. When the system simply failed to give any recommendation at all, participants were more prone to taking no action when they should have.

Doctors should in principle be able to understand the general logic behind algorithm-based decisions, thus ensuring transparency and a possibility to intervene, where needed.[26] Information about algorithm functioning should be provided to physicians, as well as an adequate training on AI tools management. However, it is not realistic to imply that physicians must possess advanced knowledge in computer science, thus it is important for the hospitals using AI have specifically trained personnel to assist doctors with technical questions.

Some AI products might provide medical information directly to patients, thus posing a high burden on them. If AI, for example, would give direct information to patients about an oncological diagnosis or treatment, a patient who would want to understand the rationale behind the information would need to have both cellular pathology and computer science knowledge to make sense of an AI's decision.[27] Furthermore, interventions based on AI can significantly reduce the autonomy of patients about their health, as in some case it might diminish an opportunity of a meaningful dialogue and shared decision-making.[28] Therefore, when using AI it is important to keep it as an assistive tool but not as a substitute to a healthcare professional.

To make sure algorithm-powered AI is trustworthy, **BEUC recommends that the EU promotes:**

- Educational programmes and trainings for healthcare professionals on AI uses.
- Mechanisms to ensure professional assistance is provided to both patients and the doctors to better understand and assess AI decision-making.
- Educational campaigns targeting consumers to create greater awareness and understanding of AI uses in health.

[25] Wickens, Christopher D., Benjamin A. Clegg, Alex Z. Vieane, and Angelia L. Sebok. "Complacency and Automation Bias in the Use of Imperfect Automation." *Human Factors* 57, no. 5, August 2015: 728–39. doi:10.1177/0018720815581940

[26] Ferretti, A. , Schneider, M. , & Blasimme, A. Machine Learning in Medicine: European Data Protection Law Review Volume 4, Issue 3, 2018, https://edpl.lexxion.eu/data/article/13107/pdf/edpl_2018_03-011.pdf

[27] Ibid

[28] Vayena, Effy et al. Machine learning in medicine: Addressing ethical challenges. PLoS medicine vol. 15, November 2018, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6219763/

### AI as a medical device

AI-powered medical devices have to comply with the safety and performance requirements of the European Medical Devices Regulation[29] (MDR) or In Vitro Diagnostic Devices Regulation[30] (IVDR). Both MDR and IVDR are expected to strengthen consumers safety when using software-based solutions intended for medical purpose. For devices that incorporate software or for software that are devices in themselves, MDR require that the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation. MDR provisions also oblige the manufacturers to set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended. In addition, based on the Software Qualification and Classification Guidelines[31] many of AI-based products will fall under the scope of MDR and IVDR, thus manufactures should be mindful of the new principles.

**BEUC calls on the EU and the Member States to ensure that the Medical Devices Regulation is implemented with a view to new technologies: guidelines and specifications are needed for the evaluation of safety and effectiveness of software, AI and deep learning powered devices throughout the entire usage cycle.**

## AI AND HEALTH DATA PROTECTION

The General Data Protection Regulation (GDPR)[32] is the foremost legal instrument to deal with the complexities of digital realities. The GDPR applies when AI is under development (using personal data), and also when it is used to analyse and make decisions about individuals.

### Need to ensure effective application of GDPR principles

**Continuous assessment of the implementation of GDPR principles is fundamental to achieve the balance between privacy protection and medical progress in the context of AI use.**

[29] Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices, April 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02017R0745-20170505

[30] Regulation (EU) 2017/746 of the European Parliament and of the Council on in vitro diagnostic medical, April 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0746

[31] Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR: https://ec.europa.eu/docsroom/documents/37581?locale=en

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

In most cases, development and use of AI requires enormous amounts of data. GDPR is accused[33] by its detractors to 'hurt' and 'restrict' the development of AI, mainly as a result of the principles of 'transparency'[34], 'purpose limitation' and 'data minimisation'.[35]

At first glance, applying these principles could indeed be challenging for AI, especially in the context of healthcare. For instance, if AI is used for health research it might not always be possible to precisely define the purposes of processing in advance. Also, where AI is used for a condition diagnosis, it might not be possible to exactly define how a decision is made.

However, this does not mean that the GDPR is an obstacle to bring AI benefits to patients and consumers.

Firstly, the GDPR provides a research exemption from the principle of purpose limitation, when appropriate safeguards are in place. Scientific research is generally considered to be a compatible purpose for processing under Article 6(4) of the GDPR. If the data has been initially collected on a lawful basis, further processing for secondary research purposes is possible. **However, the difficulty here is to establish a distinction between scientific development and actual application of AI.**[36] **Further guidelines from data protection authorities are therefore needed.**

Secondly, data minimisation is more than a principle which limits data collection. The data minimisation principle also imposes proportionality, which limits intervention in the data subject's privacy that the use of personal data can involve. When personal data cannot be anonymised and personal data is needed for the algorithm to function, this principle forces developers to achieve their objective in a way that is least invasive for data subjects, to balance out privacy protection and medical advancements. **In this sense the use of pseudonymisation and other encryption techniques to protect the data subject's identity can be helpful**.[37]

Given that it is difficult to know in advance what information is necessary and relevant for the development of an algorithm – and that data needs and relevance can change – **the developer must implement the data minimisation principle through a continuous assessment of the algorithm**. This will both protect the rights of data subject and will reduce the risk of irrelevant information being fed to the algorithm.[38] **Furthermore, a strong oversight combined with continuous evaluation of practical AI implementation by an independent agency is required.**

[33] Center for Data Innovation, the EU needs to reform GDPR to remain competitive in the algorithmic accountability, May 2019, https://www.datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/

[34] The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be use. *GDPR Recital 55*

[35] Under the GDPR, the reason for data processing must be clearly established and indicated when the data is collected (*purpose limitation principle, GDPR Art 5(b)*); Furthermore, the data should be limited and relevant to what is necessary in for the purpose of processing (*data minimisation principle, GDPR Art 5 (c)* )

[36] The Norwegian Data Protection Authority, Artificial Intelligence and Privacy, January 2018, https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

[37] Ibid

[38] Ibid

### Big Tech goes Health

Strong GDPR compliance and vigilance are especially important given an increased interest of big tech companies like Google in healthcare sector.

For instance, Google has acquired DeepMind Health which collaborated with the United Kingdom's National Healthcare Service (NHS) and had access to millions of patient records. This acquisition raises serious privacy concerns.

Currently DeepMind had contracts to process medical records from three NHS trusts covering nine hospitals in England to develop its 'Streams' mobile application. The app alerts doctors and nurses when patients are at risk of acute kidney injury. While DeepMind stated that these data will never be connected to Google accounts or used for any commercial purposes, , during DeepMind's mammography partnership with Royal Surrey County Hospital NHS Foundation Trust, digital images of mammograms were hosted on Google's Cloud service.39 Previously DeepMind was also involved in a data protection scandal over 1.6 million patient records unlawfully handed by NHS to the company.

## Personal vs Non-personal Data

**More safeguards for health data are needed.**

The use of AI in healthcare is largely conditioned on the collection of large repositories of data, including EHR, clinical measurements, genome sequences, lifestyle data from the connected medical devices, apps, social media platforms. This means that health data[40] about patients and consumers comes from a variety of sources.

Combining health and non-health data, personal and non-personal data for AI analysis poses new challenges beyond 'standard' protection mechanisms foreseen by the European data protection framework. For example, while user consent is one of the main means to control personal data, consent alone may not provide the necessary protection regarding all extensive possibilities of AI health data uses. The GDPR provides clear provisions on health research when it comes to standard sources of health data, such as electronic health records, biomedical data, secondary research etc. GDPR also recognises a special regimen for this data due to its sensitivity. However, when standard sources are combined with expanded sources of data acquired outside of conventional clinical or academic settings, and collected through smartphones or social media, informed consent is not really possible for the user.

In addition, data anonymisation techniques, even when comprehensive, still leave a possibility for de-identification, especially when combined with personal data. For genomic

[39] Wired, Why Google consuming DeepMind Health is scaring privacy experts, November 2018, https://www.wired.co.uk/article/google-deepmind-nhs-health-data

[40] Health data can be *personal* (relating to an identifiable person) or *non-personal* (when an individual can no longer be identified. Personal data that has been de-identified, encrypted or pseudonymised but can still be used to re-identify a person remains personal data and falls within the scope of the General Data Protection Regulation[40] (GDPR). GDPR is the EU's main legal instrument to protect individuals, also laying down important provisions on health data processing. Personal data that has been rendered *anonymous* in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible. Non-personal health data is not regulated by the GDPR.

research, anonymisation might not be possible at all, as it seeks to establish the continuous tracking of the individual's life story. In the interest of health research, the genomic data from the biobanks are often made available for researchers to study for other purposes than genomic research, but in an anonymised form. However, it is not clear whether the data is truly anonymised. This is a scenario of a closed environment between a biobank and researchers, however, this could also happen within larger settings and involving both public and private actors, where analytical tools could easily de-identify previously anonymised data sets.[41] In such situations when AI tools are applied the data might not be sufficiently protected.

The challenges associated with the use of big data and AI technology in health are not only arising from the characteristics and scope of the data – but also from the ways in which the data is combined, the policies, systems and technologies used to manage the data, and the ways in which the data may be used.[42] In the context of health data, patients might however easily sacrifice personal data protection and privacy in exchange for a promise of treatment or at least an improved health condition. The questions of privacy and ethical AI use cannot be neutrally assessed by patients to whom their health matters most. In addition to diligent GDPR compliance and enforcement, **BEUC therefore encourages the European Commission during the GDPR review in 2020 to specifically assess whether the EU data protection legislation is fit for purpose or whether additional regulatory safeguards are needed to establish:**

- Rules on harmonised and strong data anonymisation techniques for health data.
- Rules on data access and data control when it comes to the use of algorithm-based solutions/automated decision making and multiple source data (e.g. data from EHR, social media and a medical device).
- Quality and safety standards for all information systems where health data is processed.
- More oversight mechanisms to monitor compliance of all involved in handling of personal biomedical data with privacy protection rules and other ethical norms, and to ensure their accountability in case of data misuse.[43]

ENDS

[41] Townend, D. Hum Genet, Conclusion: harmonisation in genomic and health data sharing for research: an impossible dream? Human Generics, August 2018, https://link.springer.com/article/10.1007/s00439-018-1924-x#citeas

[42] Vayena, Effy, Dzenowagis, Joan, Brownstein, John S & Sheikh, Aziz. (2018). Policy implications of big data in the health sector. Bulletin of the World Health Organization, 96 (1), 66 - 68. World Health Organization. http://dx.doi.org/10.2471/BLT.17.197426

[43] Ibid

*This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).*