PROCESSING PERSONAL HEALTH DATA IN THE CONTEXT OF THE EUROPEAN ONLINE PHARMACY MARKET: LAWFUL BASES UNDER THE GDPR AND SWEDISH LAW

DAVID FÅHRAEUS*

In recent years, the European online pharmacy market has grown significantly and is expected to continue to grow at a rapid pace. One of the key factors that can further catalyse this growth is the personal health data that online pharmacies may collect. If online pharmacies process these data lawfully and with the public interest in mind, this may provide the opportunity to positively transform not only the online pharmacy market but also the entire healthcare industry. In order to maximise the benefits of these personal health data for improving public health but at the same time protect European citizens' privacy, further analysis of the data protection laws and their applicability in the context of the online pharmacy market is necessary. Currently, there still lacks clarity, for example, regarding the lawful bases under the GDPR for processing personal health data for online advertising purposes. This article therefore identifies three key purposes for which online pharmacies may choose to process personal health data, namely for prescribing medicines, online advertising and scientific research, and assesses the lawful bases under the GDPR that may be applicable to them. Swedish law will also be addressed in order to provide an example of the interaction between national laws and the GDPR when processing personal health data in the online pharmacy markets of Member States.

1 INTRODUCTION

The online pharmacy market is beginning to take off in Europe, especially in the aftermath of the Covid 19 pandemic. It is estimated that during the period 2019-2025, it will grow at a CAGR of over 15%.[1] For example, in Sweden, which is one of Europe's most developed online pharmacy markets, pharmaceutical e-commerce is worth 5-6% of the total e-commerce market.[2] Furthermore, 98% of all postcodes in Sweden received prescription medicines from online pharmacies.[3] Another growing market in Europe is Germany. It is

* The author of this text is currently a PhD student at Uppsala University researching the entrance of dominant online platforms into the European online pharmacy market and whether certain strategies that they may use can be considered anti-competitive under European competition law. The author would like to thank Santa Slokenberga, Senior Lecturer at Uppsala University, and Vladimir Bastidas, Prefect of the Law Faculty at Uppsala University, for their valuable feedback and comments during the process of writing this article. In particular, Santa's extensive knowledge of the GDPR and the health industry has been extremely helpful.

[1] Shop Apotheke, 'Annual Report 2021' (2016) Pg. 50 <https://corporate.shop-apotheke-europe.com/en/investorrelations/publikationen/> accessed 15 November 2022.

[2] Swedish Competition Authority et al, 'Joint Nordic Report: Online Pharmacy Markets in the Nordics' (2021) 6. Sweden is one of the most advanced countries in Europe in terms of the provision of online pharmacy services. Prescription medicines can be sold online and are processed through an advanced e-prescription system. Furthermore, Sweden also allows for online only pharmacies meaning there is no requirement to also provide a brick-and-mortar pharmacy to the consumer.

[3] ibid 46.

estimated that revenue in the German online pharmacy market will reach over 1 billion US dollars in 2022.[4]

The potential of this market has attracted big players in the US and Europe such as Amazon Pharmacy, MEDS and Shop Apotheke.[5] Through investments in innovation, these companies are creating comprehensive online pharmacies with features such as online marketplaces, telehealth apps and medication management all being incorporated into their services.[6] Due to these advancements, there is great potential to transform the healthcare industry in Europe and have an impact not only on the product supply chain, such as providing patients with quick home deliveries,[7] but more importantly, on the information supply chain allowing for health data to be easily transferred throughout the entire healthcare system.[8] Furthermore, the large amounts of health data collected by online pharmacies, if used lawfully, can help to greatly improve the healthcare system both through drug discovery and drug repurposing as well as pharmacovigilance. Yet, in order to maximise the potential that online pharmacies can have on the healthcare system, there must be clarity as to the ways in which online pharmacies can lawfully process health data.

The European General Data Protection Regulation[9] (GDPR) addresses the processing of personal health data although gaps in knowledge still exist as to its interpretation in different contexts. For example, whether online pharmacies can process personal health data in certain scenarios such as for the purpose of advertising lacks a straightforward answer under the GDPR. Even though the GDPR has been subject to extensive scholarly debate, there is generally a gap in the literature regarding the processing of personal health data by online pharmacies and its compatibility with the GDPR.

---

[4] Statista, 'Online Pharmacy – Germany' <https://www.statista.com/outlook/dmo/digital-health/ehealth/online-pharmacy/germany> accessed 15 November 2022.

[5] Amazon Pharmacy is the online pharmacy business belonging to Amazon which was created in 2020. Amazon Pharmacy does not operate an online pharmacy service in Europe just yet although the Amazon Pharmacy trademark was registered in the EU in 2020. See EUIPO, 'Amazon Pharmacy Trademark Information' <https://euipo.europa.eu/eSearch/#details/trademarks/018178963> accessed 15 November 2022. MEDS is a Swedish online pharmacy operating only in Sweden. Shop Apotheke is a German online pharmacy operating in several European Member States.

[6] Shop Apotheke has developed an online marketplace and also incorporated 'Smart Patient' into its service which is a leading company in providing support to patients to improve medication management. See Shop Apotheke, 'Annual Report 2021' (n 1) 10 and 14. MEDS has been collaborating since 2019 with Kry, a Swedish telehealth app, allowing patients to easily purchase their prescriptions that were obtained from doctors on the Kry app through the MEDS webpage. See Kry, 'Kry och MEDS samarbetar för smidigare och snabbare vård' (*Kry*, 20 November 2019) <https://www.kry.se/press/nyheter/kry-och-meds-samarbetar-for-smidigare-och-snabbare-vard/> accessed 15 Novemeber 2022. Amazon also operates an online marketplace and has for example collaborated with MEDS in Sweden to allow them to sell their products through Amazon Marketplace. See Daniel Norman, 'Meds samarbetar med Amazon: "Första gången vi säljer utanför vår egen butik"' (*Market*, 12 October 2021) <https://www.market.se/affarsnyheter/affarsutveckling/meds-samarbetar-med-amazon-forsta-gangen-vi-saljer-utanfor-var-egen-butik/> accessed 15 November 2022.

[7] Sathiadev Mahesh and Brett Landry, 'Online Pharmacies: E-strategy and Supply Chain for Pharmaceutical Products', [2016] 115 <https://www.academia.edu/1342308/ON_LINE_PHARMACIES_E_STRATEGY_AND_SUPPLY_CHAIN_FOR_PHARMACEUTICAL_PRODUCTS> accessed 15 November 2022.

[8] ibid.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1. In the following footnotes, this regulation will be referred to as 'GDPR' which is an acronym for the European General Data Protection Regulation.

This paper therefore seeks to explore the different ways in which online pharmacies can process health data under the GDPR in order to achieve their business interests, while at the same time contributing to the protection of the individual's fundamental right to privacy. In order to fulfil this objective, this paper will be divided into the following parts: Part 2 will briefly assess the importance of health data and consumer privacy in the online pharmacy market. Parts 3, 4 and 5 will then address the main purposes for which an online pharmacy can process health data and then examine how such processing may be lawfully carried out under the GDPR and Swedish law. Part 3 will address processing for dispensing prescription medicines, part 4 will address processing for online advertising and lastly, part 5 will address processing for scientific research. The reason for choosing these purposes is first, dispensing prescriptions is the core activity of an online pharmacy and second, both online advertising and scientific research are key processing activities for online pharmacies to significantly improve their services and gain a competitive advantage.[10] Although data protection rules applicable to health care generally stem from the GDPR, its application still largely depends on national specifications. Therefore, Swedish law will be used in this paper as an example of how to apply the different lawful bases under the GDPR in the context of an EU Member State's national laws. Furthermore, only the national provisions that are relevant for the specific processing purposes will be addressed as a general assessment of the Swedish legal framework for health data is outside the scope of this article.

2 THE IMPORTANCE OF HEALTH DATA AND CONSUMER PRIVACY IN THE ONLINE PHARMACY MARKET

This part aims to emphasise the benefits for public health that may arise from the lawful processing of personal health data by online pharmacies. The growth of large market actors such as Amazon Pharmacy, MEDS and Shop Apotheke has the potential to transform the healthcare industry in Europe. Patients could be able to access an enormous variety of medicines at competitive prices which may be delivered to patients' doorsteps, in some cases within several hours. With regards to home delivery, this might have enormous benefits for older or disabled patients and those living in rural areas who may have better accessibility to pharmaceutical care and services. Furthermore, patients with chronic illnesses could also benefit as they will have their prescriptions sent through the post every month and thus are more likely to adhere to their medication dosages.[11] Yet although these advantages can have the potential to bring great value to the patients using an online pharmacy, the added value compared to going down to a local brick and mortar pharmacy is not that significant, especially when addressing consumers that are neither old age, disabled or chronically ill.[12]

[10] For example, accurate advertisements will improve the quality of the online pharmacy service and make it more attractive for users. This will allow online pharmacies to grow and maximise network effects between the users. Scientific research will help online pharmacies gain insights on for example adverse reactions to drugs and thus provide patients with better advice.

[11] Patients with type II diabetes mellitus were found to have achieved a significantly higher proportion of days covered with online pharmacy services compared to patients who utilised a standard brick and mortar pharmacy. See Phil Schwab et al, 'A Retrospective database study comparing diabetes-related medication adherence and health outcomes for mail-order versus community pharmacy' (2019) 25(3) Journal of Managed Care and Specialty Pharmacy PL 332.

[12] Sathiadev Mahesh and Brett Landry, 'Online Pharmacies: E-strategy and Supply Chain for Pharmaceutical Products', (*Academia*, 2016) 122

The real added value to the healthcare system as a whole is not the great variety of medicines on offer or the quick home deliveries but rather the enormous amount of information that online pharmacies can process and then supply throughout the entire value chain.[13] In a typical scenario, physicians provide patients with basic information on medicine use and then a brick and mortar pharmacist will provide additional information such as usage warnings, allergic reactions and potential inter-drug reactions.[14] An online pharmacy however has the potential to provide a lot more in terms of additional information. This it can do through internally or externally analysing the large amounts of data it collects 24/7 from, for example, patient reviews as well as follow ups and consultations online with its pharmacists. This analysis can provide far more accurate assessments of potential patient risks and also help inform patients through Q&As about any doubts they have during their prescription cycle.[15] In addition, an online pharmacy can also ensure that data is more efficiently communicated among pharmacists, physicians and manufacturers.[16] For example, online pharmacies can become the point of contact between individual physicians and manufacturers by reporting back to them regarding side effects and performances of the administered medicines.[17] An online pharmacy's ability to process and communicate large amounts of data is what will differentiate them from normal brick and mortar pharmacies.

The benefits of efficient processing and communicating of data for Europe and the world could be immense. Public health may be greatly improved as pharmacies will be able to deliver more efficient, sustainable and high-quality healthcare services to patients.[18] Key market failures in the online pharmacy market may also be reduced. For example, asymmetries of information in the pharmaceutical distribution chain are high as patients lack the adequate knowledge regarding the medicines they buy.[19] Online pharmacies could eliminate this asymmetry between manufacturers, pharmacies and patients due to the greater efficiency they provide in the information supply chain.[20] Furthermore, both governments as well as consumers could save enormous sums of money due to better adherence by

<https://www.academia.edu/1342308/ON_LINE_PHARMACIES_E_STRATEGY_AND_SUPPLY_CHAIN_FOR_PHARMACEUTICAL_PRODUCTS> accessed 15 November 2022. Mahesh and Landry argue that, with regard to the online pharmacy market, '[t]he efficiencies gained from product supply chain changes using eBusiness approaches are small'.

13 ibid 119.

14 ibid.

15 Mahesh and Landry (n 12) 119.

16 Swedish Competition Authority et al, 'Joint Nordic Report: Online Pharmacy Markets in the Nordics' [2021] 15.

17 Mahesh and Landry (n 12) 121.

18 Pharmaceutical Group of the European Union, 'Position Paper on Big Data & Artificial Intelligence in Healthcare' [2019] 2, 5. Public expenditure on health and long-term care in the EU has been increasing over the past decades is estimated to account for 8.5% of GDP. Member States' ability to provide high quality care to all will greatly depend on whether their health systems can manage use the potential of big data in health care to become more resilient and sustainable. The PGEU also states that 'innovative solutions that make use of digital technologies, including eHealth, Big Data, AI are seen by the European Commission as opportunities to transform healthcare systems'.

19 Declan Purcell, 'Competition and Regulation in the Retail Pharmacy Market' (2004) 14 Studies in Public Policy, Trinity College Dublin, 6 <http://www.tara.tcd.ie/handle/2262/60273> accessed 15 November 2022.

20 Mahesh and Landry (n 12) 115.

patients to their prescribed medication.[21] It is estimated that non-adherence to prescription medication in the European Union is estimated to cost €1.25bn annually.[22]

In order for online pharmacies to be able to maximise the efficiencies in the information supply chain, there must be clarity regarding the processing of health data in the context of the European online pharmacy market. Currently, approximately 30% of the entire world data volume is being generated by the healthcare industry.[23] This demonstrates the importance of health data but also the required urgency to clarify the legal framework. Furthermore, organisations and professionals throughout the world identify privacy as one of the biggest challenges for using data in health care. The Pharmaceutical Group of the European Union has for example identified privacy as an important challenge that must be addressed in order to keep patients' trust in the health system unchanged.[24] This applies not only to medical services, but also to online pharmacies as essential actors in ensuring accessibility to medicinal products.

3 PROCESSING PERSONAL HEALTH DATA FOR DISPENSING PRESCRIPTION MEDICINES

In order to address the lawful bases for processing of personal health data in the EU, it is necessary to first explain the general structure that the GDPR establishes. First, Article 6(1) provides a list of lawful bases for processing personal data.[25] These include for example consent, compliance with a legal obligation or performance of a task carried out in the public interest.[26] Second, if the data being processed falls under a special category of data such as personal health data, these lawful bases do not suffice. As the GDPR considers the processing of special categories of personal data to be of such a significant risk to an individual's fundamental right to privacy, as a rule, it is prohibited.[27] This prohibition however has exceptions thus allowing the processing of such categories of personal data as long as one of the conditions that enable lifting of the prohibition set out in Article 9(2) GDPR is met.[28] The lawful bases under Article 9(2) are for example explicit consent, the provision of health or social care or reasons of public interest in the area of

[21] Please see the section on Scientific Research in part 5 of this paper which addresses the benefits of data collected by online pharmacies to improve non-adherence of prescription medicines.
[22] Pharmaceutical Group of the European Union, 'Targeting Adherence: Improving Patient Outcomes in Europe through Community Pharmacists' Intervention' [2008] 4.
[23] Greg Wiederrecht et al, 'The health care data explosion' (*Royal Bank of Canada*) <https://www.rbccm.com/en/gib/healthcare/episode/the_healthcare_data_explosion> accessed 15 November 2022.
[24] PGEU, 'Position Paper on Big Data & Artificial Intelligence in Healthcare' (n 18) 6. Privacy has also received attention in this context outside the EU. For example, the Chief Privacy Officer for Express Scripts, the largest independent Pharmacy Benefit Manager in the US, has identified privacy as one of the biggest challenges to using data in health care. See Janna Lawrence, 'Could Big Data be the Future of Pharmacy?' (*The Pharmaceutical Journal*, 20 April 2017) <https://pharmaceutical-journal.com/article/feature/could-big-data-be-the-future-of-pharmacy> accessed 15 November 2022.
[25] GDPR, art 6(1).
[26] ibid.
[27] ibid art 9(1).
[28] ibid art 9(2). The GDPR adds these additional requirements as it considers that there is a far higher risk for individuals having their fundamental right to privacy violated in the case of processing special categories of personal data.

public health. It is important to note that Member State national laws may also provide for more specifications regarding the different lawful bases under Article 9(2) GDPR.

In the case of an online pharmacy wishing to process personal health data, it must adopt a two-step approach by firstly identifying a lawful basis under Article 6(1) and then additionally identifying a lawful basis in order to lift the prohibition under Article 9(2). The application of this two-step approach will in the following paragraphs be carried out in order to identify the correct lawful bases for each of the different purposes of processing. It is important to lastly mention that according to Article 9(4), 'Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health'.[29] In this paper, Swedish law will be the focus with respect to Article 9(4).

3.1 PURPOSE

The first common purpose for processing personal health data is to dispense prescription medicines to patients. When a customer requests a prescription medicine from an online pharmacy, an online pharmacist will have to process the health information on the prescription and check for example the patient's identity number and contact details as well as the prescription and medical information.[30] According to recital 35 of the GDPR, information collected about a natural person during the provision of healthcare services, which includes pharmacy services, will be considered health data.[31] In this case, an online pharmacy is providing an essential healthcare service therefore the personal data being processed is likely to fall under personal health data. Furthermore, although not referring specifically to prescriptions, the European Data Protection Board (EDPB) has stated that information, such as medical history and results of examinations, collected by a healthcare provider in a patient record constitutes personal health data.[32] A patient's prescriptions are normally kept in their medical history records therefore this implies that information on a prescription will most probably constitute personal health data.[33] In addition, the European Data Protection Supervisor (EDPS) has specifically stated that personal health data 'would normally include medical data (e.g. doctor referrals and *prescriptions*, medical examination reports, laboratory tests, radiographs)'.[34]

---

[29] ibid art 9(4).

[30] Apotek Hjartat Privacy Policy <https://www.apotekhjartat.se/om-oss/var-personuppgiftsbehandling/> accessed 15 November 2022.

[31] GDPR, recital 35.

[32] European Data Protection Board, 'Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak' [2020] 5. The scope of what constitutes personal health data is extremely broad. In Opinion of the AG Athanasios Rantos in Case C-252/21 *Meta Platforms and Others* EU:C:2022:704, visiting and clicking integrated buttons on for example third party websites/apps was considered to constitute personal health data.

[33] European Commission, 'Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format' [2019] OJ L39/18, Annex Point 2.1. The EU Commission has proposed a Baseline for the European electronic health record exchange format which includes e-prescriptions.

[34] European Data Protection Supervisor, 'Guidelines concerning the processing of health data in the workplace by Community institutions and bodies' [2009] 2.

3.2 LAWFUL BASES

The first step in the GDPR for processing personal health data for the dispensing of prescription medicines will require finding a lawful basis under Article 6(1). There are several lawful bases that could be chosen from the list such as consent,[35] for the performance of a contract,[36] compliance with a legal obligation[37] or for the performance of a task carried out in the public interest.[38]

From the previously mentioned options, the appropriate choice of a lawful basis will often depend on the laws of the Member State where an online pharmacy operates. With regards to compliance with a legal obligation in Sweden, Act (2009:366) on trade in medicinal products states that a pharmacy that has a license to sell medicines must supply all prescribed medicinal products as soon as this can be done.[39] The Swedish online pharmacies Apotek Hjartat and Apoteket.se use this lawful basis as grounds for processing.[40] In the case of processing for the performance of a task carried out in the public interest, one could argue that the overall purpose of a community pharmacy is to perform a task carried out in the public interest however, in Sweden, this is not clearly established by law.[41]

Processing for the performance of a contract is also a suitable option since when a patient purchases prescription medicines from an online pharmacy, a valid contract is established with the patient and the processing of personal health data in the prescription is necessary to perform the contract.[42] For example, the Swedish online pharmacy Apotea chooses this lawful basis for processing personal health data in prescriptions.[43] With regards

---

[35] GDPR, art 6(1)(a).
[36] ibid art 6(1)(b).
[37] ibid art 6(1)(c).
[38] ibid art 6(1)(e).
[39] Act (2009:366) on trade in medicinal products (lag (2009:366) om handel med läkemedel), 6 § paragraph 3 states that pharmacies must 'supply all prescribed medicinal products, and all prescribed goods covered by the Act (2002:160) on medicinal product benefits, etc. as soon as this can be done'. Furthermore, 9a § states that 'When dispensing a prescription, a pharmacist shall provide information and advice in accordance with 6 § paragraph 11 and shall perform such other tasks as are of particular importance for the safe handling and use of the medicinal product'. 6 § paragraph 11 states that pharmacies must 'provide individual and producer-independent information and advice on medicinal products, the replacement of medicinal products, the use of medicinal products and self-care to consumers and ensure that the information and advice is provided only by staff with sufficient competence for the task'. One could also interpret 9a § as constituting a legal obligation to process personal health data in prescriptions in order to provide information and advice on medicinal products including their use and replacement. All translations in this footnote were made by the author of this article.
[40] Apotek Hjartat and Apoteket.se use compliance with a legal obligation as their lawful basis. See Apotek Hjartat Privacy Policy (n 30); see also Apoteket.se Privacy Policy <https://www.apoteket.se/kundservice/integritetspolicy/> accessed 15 November 2022.
[41] Community Pharmacy GDPR Working Party, 'The General Data Protection Regulation and associated legislation Part 1: Guidance for Community Pharmacy' [2018] 8. The Community Pharmacy GDPR Working Party in the UK identified the performance of a task carried out in the public interest as generally an adequate lawful basis although not specifically for dispensing prescription medicines. It is important to note however that according to recital 45 of the GDPR, where processing is necessary for the performance of a task carried out in the public interest, the processing should have a basis in Union or Member State law. See also Chap.2, 2 § Paragraph 1 of Act (2018:218) with Additional Provisions to the EU Data Protection Regulation. In Sweden there is no clear law establishing that pharmacies carry out a task in the public interest.
[42] European Data Protection Board, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects' [2019] 9. The EDPB states that the requirements for the processing being necessary for the performance of a contract are that the processing takes place in the context of a valid contract and that the processing is necessary in order so that the particular contract with the data subject can be performed.
[43] Apotea Privacy Policy <https://www.apotea.se/integritetspolicy> accessed 15 November 2022.

to consent, this is a valid lawful basis although it is important to consider that the GDPR establishes that consent may be withdrawn at any time.[44] Additionally, consent must be freely given meaning that the data subject cannot feel compelled to give consent.[45] Consent therefore might be problematic when the patient depends on the online pharmacy to provide them with their prescription medicines as they may feel compelled. This would suggest that consent would be more suitable as a safeguard rather than a lawful basis in itself.[46]

On the other hand, as an online pharmacy is processing extremely sensitive personal health data, ensuring that the patient is aware of the processing taking place is important. This might suggest that consent may in fact be the most appropriate lawful basis. Yet for practical reasons, relying only on consent to dispense prescription medicines may pose unnecessary hurdles for online pharmacies offering secondary care that could be resolved by other valid lawful bases. Although processing personal health data in this context poses a risk to the patient's fundamental right to privacy, a legal obligation and the performance of a contract are sufficiently strong lawful bases to justify processing. Furthermore, when processing for the performance of a contract, Advocate General (AG) Rantos has clarified that the processing must be objectively necessary meaning that there cannot exist realistic, less intrusive alternatives.[47] There are no realistic, less intrusive alternatives to prescribe a medication as the pharmacist must look at the patient's personal health data. Therefore, the potential risk to the privacy of the individual that may arise from the processing is justified.

In addition to a lawful basis under Article 6, a legal basis to lift the general ban to process health data in Article 9(1) GDPR needs to be established under Article 9(2). In this case, potentially suitable lawful bases are explicit consent,[48] reasons of substantial public interest,[49] the provision of health or social care or treatment,[50] the establishment and reasons of public interest in the area of public health.[51] With regards to explicit consent, this might again serve as an additional safeguard however for the reasons mentioned above, it may be difficult to demonstrate that explicit consent was given and furthermore, explicit consent may create unnecessary hurdles when providing secondary care. Additionally, reasons of substantial public interest under Article 9(2)(g) may be harder to prove and furthermore, they must be established in EU or Member State law that provides for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.[52]

In the case of reasons of public interest in the area of public health, the GDPR provides some examples of this lawful basis in Article 9(2)(i) such as 'protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.'[53] One could argue in this case that the processing by an online pharmacy of personal health data when dispensing prescription

---

[44] GDPR, art 7(3).
[45] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' [2020] 7.
[46] Directorate General Santé of the European Commission, 'Assessment of the EU Member States' rules on health data in the light of GDPR' [2021] 29. Online pharmacies can use a lawful basis such as compliance with a legal obligation together with consent as an additional safeguard in case of uncertainty.
[47] Opinion of AG Rantos in Case C-252/21 *Meta Platforms and Others* (n 32), para 54.
[48] GDPR, art 9(2)(a).
[49] ibid art 9(2)(g).
[50] ibid art 9(2)(h).
[51] ibid art 9(2)(i).
[52] ibid art 9(2)(g).
[53] ibid art 9(2)(i).

medicines guarantees the high standards of quality and safety of health care. Recital 54 of the GDPR elaborates that 'public health' in the context of Article 9(2)(i) should be understood as all elements related to health including for example healthcare needs and the provision of health care.[54] In any case, this would have to be established in EU or Member State law and furthermore, this law has to provide for suitable and specific measures to safeguard the rights and freedoms of the data subject.[55] In Sweden, this is not addressed in the Data Protection Act although it is mentioned in its preparatory works (these texts have legal authority in Sweden).[56] According to the preparatory works, the Swedish Government considered that including a specific provision in Swedish law was not necessary for Article 9(2)(i) GDPR to be applicable in Sweden and furthermore, the requirement of confidentiality of special categories of personal data was already addressed in other laws relating to healthcare thus providing for appropriate and specific measures to safeguard the rights and freedoms of the data subject.[57]

Another highly relevant lawful basis for processing personal health data in this context is for the provision of health or social care or treatment.[58] Shop Apotheke for example uses this as its lawful basis for dispensing prescription medicines.[59] Looking to Article 9(2)(h) in the GDPR, it states that processing may be carried out for the provision of health or social care or treatment 'on the basis of Union or Member State law *or* pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3'.[60] Therefore when using this lawful basis, it might be the case that a provision for the processing of personal health data in the context of health or social care or treatment is established in Union or Member State law but this is not necessary.[61] Instead, an online pharmacy can rely on the fact that it is a health professional and that there is a contract with the patient when dispensing prescription medicines.[62] It is important to note that in addition to entering into a contract with the patient, the processing must be under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law.[63] In

[54] ibid recital 54.
[55] ibid art 9(2)(i).
[56] Government bill [prop.] 2017/18:105 Data Protection Act.
[57] Government bill 2017/18:105 (n 56) 96.
[58] Community Pharmacy GDPR Working Party, 'The General Data Protection Regulation and associated legislation Part 1: Guidance for Community Pharmacy' [2018] 8. The Community Pharmacy GDPR Working Party in the UK identified the provision of health or social care or treatment as relevant for community pharmacies.
[59] Shop Apotheke Privacy Policy <https://www.shop-apotheke.com/datenschutz.htm> accessed 15 November 2022.
[60] GDPR, art 9(2)(h), emphasis added.
[61] In Sweden, 8 § paragraph 1 point 1 of the Pharmacy Data Act (2009:367) states that personal data may be processed if it is necessary for 'the dispensing of prescribed medicinal products, and such prescribed goods as are covered by the Act (2002:160) on medicinal product benefits etc., and for measures in connection with the dispensing'. Furthermore, 9(a) § states that 'Personal data referred to in Article 9(1) of the EU Data Protection Regulation (sensitive personal data) may be processed on the basis of Article 9(2)(h) of the Regulation, provided that the obligation of professional secrecy in Article 9(3) of the Regulation is met'. These translations were made by the author of this article.
[62] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare [2011] OJ L88/45. In Article 3(2)(f), the definition of 'health professional' includes a pharmacist.
[63] GDPR, art 9(3).

Sweden, a pharmacist's obligation of professional secrecy is established in the Patient Safety Act.[64]

4 PROCESSING PERSONAL HEALTH DATA FOR ONLINE ADVERTISING

4.1 PURPOSE

The following part will address how online pharmacies may process personal health data for online advertising. In this case, an online pharmacy might be interested in sending its customers via email, sms or other channels relevant information as well as offers based on previous purchases or the use of the web page.[65] In particular, this will involve placing customers into a specific segment based on purchasing history, age, sex and specific preferences.[66] With regards to personal data concerning customer purchases, this may include click data meaning that the customer has demonstrated an interest in the product but not necessarily purchased it.[67] Online pharmacies may also want to use these data to create recommender systems that suggest products based on what they know about the consumer.[68] Additionally, they may wish to create a profile on the customer by inferring the health status of the individual based on certain observations gathered from non-sensitive data.

The advantages of this type of processing may benefit both the online pharmacy and the consumer.[69] On the one hand, the online pharmacy can increase its sales to consumers which in turn will provide it with even more data. The consumer may benefit by receiving product recommendations that are based on their current health status. For example, an online pharmacy could process personal health data collected from a patient's prescription which shows that this patient has diabetes. The online pharmacy could then send the consumer product recommendations such as blood sugar level testing kits. In this case, the consumer's health will be improved since they will be sold the most adequate and relevant products for their conditions.

---

[64] Chap. 6, 12 § and 16 § of Patient Safety Act (2010:659).

[65] MEDS Privacy Policy <https://www.meds.se/integritetspolicy/> accessed 15 November 2022. MEDS is one of the largest online pharmacies in Sweden and sells both non-prescription and prescription medicines. It is also important to mention that data regarding a data subject's visit to a web page, eg an online pharmacy website, can constitute personal health data. The definition of what constitutes personal health data is extremely broad. See Opinion of AG Rantos in Case C-252/21 *Meta Platforms and Others* (n 32).

[66] MEDS Privacy Policy (n 65).

[67] ibid. As previously mentioned, the scope of personal health data is extremely broad and therefore click data will most probably constitute personal health data. See fn 65 in this text.

[68] Recommender systems are not the same as targeted advertisements as they only recommend products that the user might like based on search queries and do not specifically target users with advertisements. The author has included recommender systems in this part due to their similarity to online advertising. They are fundamental for online platforms, such as online pharmacies, as they are a valuable source of network effects and help platforms to grow. Users provide data to the platform which allows the platform to help new users with suggestions for products based on the observations of past users. They also have the potential to reduce search costs for the users. See Paul Belleflamme and Martin Peitz, *The Economics of Platforms: Concepts and Strategy* (Cambridge University Press 2021) 60.

[69] In certain cases, the consumer will be a patient depending on the type of products that they are purchasing.

4.2 LAWFUL BASES

The first step in the GDPR for processing health data for the purpose of online advertising requires identifying a legal basis under Article 6(1). The possible options are consent,[70] necessary for the performance of a contract[71] and the legitimate interests of the controller.[72] Necessary for the performance of a contract and legitimate interests will be addressed first as in the case of consent, the first and second steps under article 6 and 9 GDPR directly complement each other and therefore will be addressed together.[73]

With regards to necessary for the performance of a contract, some of the requirements have already been addressed in part 3 with reference to AG Rantos' Opinion. In this Opinion, he provides the general requirements for processing personal data for personalised content, such as when using recommender systems.[74] When specifically applying this to personalised advertisements, he mentions that it is important to assess the 'degree of personalisation' of the advertising that is objectively necessary.[75] He states that consideration must also be had to the fact that the data being used in that case came from sources outside the Facebook website.[76] Applying this to online pharmacies and personalised advertisements, this lawful basis could be relied on as long as the data being collected comes from their own websites and not cookies on other websites. However, this lawful basis may be hard to justify as an online pharmacy, unlike Facebook, does not rely on personalised advertisements as the core of its business model.

In the case of legitimate interests, the GDPR has stated that this lawful basis might be used for direct marketing purposes however this concept is quite vague.[77] Furthermore, it is explained in recital 47 that a controller wishing to use legitimate interests as a lawful basis must carry out a balancing test to ensure that the interests or the fundamental rights and freedoms of the data subject do not override the interests of the controller.[78] This balancing test will require a case by case interpretation and means that there is no legal certainty as to whether the GDPR will permit the processing of personal health data for this purpose.

---

[70] GDPR, art 6(1)(a).
[71] ibid art 6(1)(b).
[72] ibid art 6(1)(f).
[73] ibid art 6 and 9 GDPR.
[74] Opinion of AG Rantos in Case C-252/21 *Meta Platforms and Others* (n 32), para 56. One important criterion which he identifies is to what extent the processing corresponds to the expectations of an average user. With regards to recommender systems, they are more likely to fall under necessary for the performance of a contract rather than targeted advertisements as they are probably within the expectations of the average user. On the other hand, the Swedish Authority for Privacy Protection has stated that a digital marketplace that wants to suggest products to users based on their search queries cannot rely on necessary for the performance of a contract as this is not objectively necessary for the provision of the service. See Swedish Authority for Privacy Protection, 'Processing of personal data for the provision of online services' <https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/foretag/behandling-av-personuppgifter-vid-tillhandahallande-av-onlinetjanster/> accessed 29 December 2022.
[75] Opinion of AG Rantos in Case C-252/21 *Meta Platforms and Others* (n 32), para 64.
[76] ibid.
[77] GDPR, recital 47. In the Opinion of AG Rantos in Case C-252/21 *Meta Platforms and Others* (n 32), it states that the notion of 'legitimate interest' is rather elastic and open ended. Direct marketing purposes are also mentioned when addressing legitimate interests (footnote 84 of the Opinion).
[78] GDPR, recital 47.

AG Rantos has elaborated on a set of cumulative conditions to help apply legitimate interests.[79] These conditions were applied by the Court of Justice of the European Union to the equivalent provision before the GDPR was enforced. They require that

> first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence.[80]

With regards to the final point involving the balancing of interests, AG Rantos refers to recital 47 of the GDPR which states that it is essential to take into consideration the reasonable expectations of the data subject based on their relationship with the controller.[81] Furthermore, the fact that the legitimate interest is a purely economic interest as well as the potential impact on the user, in that case of Facebook, should be taken into consideration.[82] What AG Rantos' assessment demonstrates is that applying legitimate interests in the context of marketing purposes is far from straightforward. This still leaves room for legal uncertainty, in particular with regards to its application in the context of the online pharmacy market. For example, whether an online pharmacy processing a user's personal non-health data to provide healthcare product recommendations is a purely economic interest requires more clarification as product suggestions may also serve the purpose of improving the health of the users.

Since legitimate interests and necessary for the performance of a contract are only lawful bases under Article 6(1) of the GDPR, it is also necessary to proceed with the second step to identify a lawful basis under Article 9(2). Under the second step, the two relevant lawful bases are explicit consent and data that have been manifestly made available to the public by the data subject.[83] In the case of data manifestly made public by the data subject, this has been addressed by the EDPB in the context of targeted advertising.[84] Here the EDPB states that this assessment requires a case-by-case review and that the word 'manifestly' entails a high threshold for relying on this exemption.[85]

Manifestly making data available to the public has also been addressed in AG Rantos' Opinion in a similar context.[86] AG Rantos considered whether visiting or clicking buttons integrated on websites or apps, such as dating websites/apps, which reveal special categories

---

[79] Opinion of AG Rantos in Case C-252/21 *Meta Platforms and Others* (n 32).
[80] ibid para 59. For an understanding of how to apply these provisions, see paras 60-66.
[81] ibid para 62.
[82] ibid.
[83] The other possible options under Article 9(2) GDPR are reasons of substantial public interest or for the provision of health or social care or treatment. To argue that advertising products to consumers falls within these lawful bases is questionable. Furthermore, they both establish that the processing must be 'necessary' for these reasons and arguing that advertising is 'necessary' is unlikely to succeed. See Article 9(2)(e) for data made manifestly public by the data subject.
[84] European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' [2020]. Here the EDPB defines the targeting of social media users as including personalised advertising.
[85] ibid 35. The EDPB also lists several elements that are relevant when carrying out an assessment such as the nature of the social media platform and whether it is intrinsically linked with connection with close acquaintances (eg online dating platforms).
[86] Opinion of AG Rantos in Case C-252/21 *Meta Platforms and Others* (n 32).

of personal data about the data subject, can be considered manifestly making data available to the public. He provides an interesting assessment and interprets the adverb 'manifestly' to require the data subject to be *fully aware*, by an *explicit act*, that he or she is making sensitive personal data public.[87] Furthermore, he mentions that since making data manifestly public is an exception to the general prohibition under Article 9(1) GDPR, the application of the provision should be applied stringently.[88] AG Rantos does not however specifically address the notion of 'public' in this context although he mentions the term 'general public'[89] and not a specific group of people, even if they are part of the general public. Finally, he concludes in his reasoning that visiting websites or apps is not manifestly making data public since this information is only available to the administrator of the website.[90] With regards to clicking on buttons integrated into the websites or apps, he states that although the data subject is clearly expressing their wish to share certain sensitive information about themselves to the public outside the website/app, this is done with the intention of reaching a specific group of people and not the general public as a whole.[91]

AG Rantos' reasoning regarding visiting websites/apps is quite logical due the data being available only to the administrator and not the general public however his assessment regarding integrated buttons is more questionable. In the case being addressed, this was in the context of Facebook like and share buttons being integrated into third party websites/apps outside the Facebook webpage.[92] AG Rantos' reasoning casts some doubts as an individual should be fully aware that by clicking a like button on a dating website, there runs the risk that they are revealing sensitive information about themself to the general public. The only reason that this would not be the case is if only the friends of the individual who were signed up on Facebook were able to see the like click but normally anyone, in particular Facebook users in general, can see the like clicks on third party websites.[93]

On a final note, this Opinion still leaves questions unresolved such as, for example, whether an individual leaving a comment on a dating website falls under manifestly making sensitive personal data available to the public. The EDPB states that an individual explicitly stating on their social media page for example that they are a member of a political organisation is considered manifestly making data public however in this scenario, the individual has simply commented and has not mentioned their sexual orientation.[94] Could the difference be that the individual, in the case of actively writing a post, is 'fully aware' that it would be made available to the general public whereas clicking a like button is not? Or is this also a case of not being 'fully aware' since leaving a comment is not the same as explicitly stating your sexual orientation? There is still ambiguity in this regard and further clarification is required.

---

[87] ibid para 42.
[88] ibid.
[89] ibid para 44.
[90] ibid para 44.
[91] ibid.
[92] Opinion of AG Rantos in Case C-252/21 *Meta Platforms and Others* (n 32) para 44. See footnote 54 of the Opinion.
[93] The EDPB states that elements such as the accessibility of the page where the sensitive data is published and whether the data subject has published the sensitive data him or herself should be taken into consideration. See EDPB, 'Guidelines 8/2020 on the targeting of social media users' (n 84) 35.
[94] EDPB, 'Guidelines 8/2020 on the targeting of social media users' (n 84) 32. Here the EDPB defines the targeting of social media users as including personalised advertising.

With regards to consent, this is probably the most plausible lawful basis due to the uncertainties surrounding manifestly making data public.[95] The EDPB has addressed consent for the processing of special categories of data, which includes health data, for targeting social media users.[96] The EDPB in its guidelines shows particular concern for the processing of special categories of data for advertising although it does suggest the legality of this practice under the GDPR.[97] In order to process special categories of data for advertising, the EDPB states that the controller will need to identify a lawful basis under Article 6 of the GDPR as well as an additional lawful basis under Article 9(2) GDPR.[98] With regards to the lawful bases under Article 9(2), it identifies explicit consent as a valid option.[99]

In the context of the online pharmacy market, it is relevant to point out that the EDPB also permits explicit consent as a lawful basis for using inferred or combined special categories of personal data to categorise individuals for targeted advertisements.[100] This would suggest that as long as the customer has provided explicit consent, personalised advertisements for non-prescription medicines may be based on inferences regarding the health status of an individual from observed data. Allowing online pharmacies to infer the health status of an individual is however controversial as it involves profiling. Separate explicit consent should therefore be required both for processing personal health data provided by the data subject to the online pharmacy and for any processing for the purpose of inferring the health status of data subjects. For example, a data subject may not object to an online pharmacy processing personal health data on their prescriptions for offering targeted advertisements. However, the data subject may be less comfortable with the online pharmacy inferring their health status based on additional data they collect such as the supplements and food products they consume.[101] This is an important distinction as using personal data to create inferences regarding the health status of an individual involves profiling which can result in a significant violation of an individual's fundamental right to privacy.

In order to obtain explicit consent, it will have to be obtained with strict adherence to regulations and guidelines. One interpretation of explicit consent in the context of an online pharmacy market processing personal health data can be derived from the EDPB guidelines on consent under the GDPR.[102] Although these guidelines do not refer to health data and online advertising, they at least provide some understanding of the expectations of EU regulators when obtaining explicit consent. Examples provided for correctly obtaining explicit consent are to create 'Yes' and 'No' checkboxes which clearly state that 'I, hereby, consent to the processing of my data (for the purpose of) […].'[103] Additionally, a two-step verification can also be used which firstly provides the data subject with an email that allows

[95] See Shop Apotheke's Privacy Policy (n 59). Shop Apotheke, for example, uses consent as a lawful basis for processing of personal data regarding certain products or marketing campaigns.
[96] EDPB, 'Guidelines 8/2020 on the targeting of social media users' (n 84) 9. Here the EDPB defines the targeting of social media users as including personalised advertising.
[97] ibid 5.
[98] ibid 30.
[99] ibid.
[100] ibid 32. The EDPB provides an example such as inferring someone's state of health from the records of their food shopping combined with data on the quality and energy content of foods.
[101] EDPB, 'Guidelines 8/2020 on the targeting of social media users' (n 84).
[102] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (n 45).
[103] ibid 21.

them to accept the purpose of processing and secondly provides them with a verification link that must be clicked, either via SMS or with a verification code.[104]

Although these guidelines are reasonable, further clarifications are required. With regards to statements such as "'I, hereby, consent to the processing of my data (for the purpose of) […]', more detailed examples are necessary as data subjects may not fully understand the complexity of the processing of their personal health data for online advertising. Online pharmacies may for example create ambiguous statements when requesting a data subject to provide explicit consent in order to base targeted advertising on inferences regarding their individual health status. The average user of an online pharmacy may not understand the implications of granting consent for this type of processing. Therefore, more concrete examples could be provided by the EDPB and data protection authorities on how to define the different marketing purposes for processing personal health data.

Another potential source for addressing the use of health data for advertisements is the EU Commission's Draft Code of Conduct on privacy for mobile health applications.[105] This document, which has been criticised and is still not final, addresses the question of how mobile health apps can show advertisements in its app.[106] Firstly, it requires that the use of advertisements must be clearly authorised by the user prior to the app being installed.[107] Secondly, it requires that consent be obtained either through an opt-out or opt-in option depending on the context.[108] If the app uses contextual advertising shown in the app, meaning without sharing personal data to a third party and does not require the processing of information specifically linked to an individual, then a prior opt-out consent option may be provided to the customer.[109] However, in the case that the advertising uses personal data which is shared to a third party or that personal data is used to create user profiles across multiple apps and services, or because data concerning health is processed to target customers, then prior opt-in consent must be obtained.[110] Furthermore, this consent must be explicitly given by the data subject.[111]

---

[104] ibid.

[105] European Commission, 'Draft Code of Conduct on privacy for mobile health applications' [2016]. <https://digital-strategy.ec.europa.eu/en/library/code-conduct-privacy-mhealth-apps-has-been-finalised> accessed 29 December 2022. It is important to note here that this Draft refers to Article 29 Working Party's Opinion 2/2010 on online behavioural advertising suggesting that the Commission still considers this Opinion to be relevant.

[106] Osborne Clarke, 'mHealth apps: The Code of Conduct on Privacy, explained' (*Osborne Clarke*, 18 July 2018) <https://www.osborneclarke.com/insights/mhealth-apps-the-code-of-conduct-on-privacy-explained> accessed 15 November 2022.

[107] European Commission, 'Draft Code of Conduct on privacy for mobile health applications' (n 105) 13. Note here that this is following the same requirements in Article 29 Working Party's Opinion 2/2010 on online behavioural advertising which establishes the need for *prior* explicit consent.

[108] ibid.

[109] ibid. The Commission uses an example of an app that monitors blood sugar concentration levels for diabetes patients. If ads are placed on the app for products to help diabetes patients and these ads are not based on specific blood sugar measurements of a customer, this will only require prior consent with an opt-out option. It is important to mention that explicit consent is not needed as there is no processing of health data since, although these ads target patients with health products, they are general ads based on the context of the app and not on the individual's health data.

[110] ibid.

[111] ibid.

If we apply this in the context of the online pharmacy market, should online pharmacies wish to implement targeted advertising using personal data from their customers, they would be able to do so as long as, prior to registering, there is an opt-in consent option demonstrating that the customer has actively chosen to tick the box. Furthermore, by drawing upon the previous example found in the EDPB guidelines on online advertising, explicit consent should also be obtained by using a clear statement stating that 'I, hereby, consent to the processing of my data (for the purpose of) […]' with an additional two-step verification procedure through email.

With regards to the various legal bases in the GDPR, (explicit) consent should be the preferred option for processing personal health data for online advertising as relying on necessary for the performance of a contract, legitimate interests and making data manifestly available to the public are more problematic due to the uncertainty regarding their application. It is important however to emphasise the potential benefits of targeted marketing as providing personalised content may improve the overall experience of the user of an online pharmacy service.[112] Furthermore, personalised recommendations of health products relying on personal health data can also have a public health benefit since citizens can receive suggestions based on their previous or current illnesses. Recommending health products can for example prevent risks of negative reactions to certain medicines as well as providing additional benefits to patient treatment.[113] Yet, due to the significant risk to the individual's fundamental right to privacy and the fact that the interest that is being balanced against this is primarily of a private nature, (explicit) consent should be the preferred option.[114] Furthermore, the possibility of allowing a data subject to provide (explicit) consent ensures that the efficiencies from recommending products are possible but only when the data subject is fully aware.

It is important to note that (explicit) consent also has its risks since the data subject cannot feel compelled to provide consent.[115] Due to these risks, online pharmacies may refrain from processing personal health data for online advertising altogether. To ensure that data subjects are protected but also that online pharmacies continue to offer the possibility of more personalised content, providing clear guidelines on how to obtain (explicit) consent for processing personal health data for online advertising is recommended. In particular, it is advisable to emphasise that (explicit) consent *must* be clearly and specifically requested for each separate purpose, as suggested above, and that the purposes for processing are written in layman's terms. It may also be a good suggestion to advise online pharmacies to incorporate a clearly visible notice on their privacy policy stating that the data subject is not obliged in any way whatsoever to provide (explicit) consent for the processing of their personal health data for online advertising and that refusing to do so will not have any

[112] See fn 68.
[113] See above section 4.1 on recommender systems.
[114] AG Rantos states that in the case of personalised advertising as a legitimate interest, the purely economic nature of the processing should be taken into consideration. AG Rantos considers that personalised advertising is of a purely economic nature however this might not be entirely true when recommending health products. See Opinion of AG Rantos in Case C-252/21 *Meta Platforms and Others* (n 32), para 64.
[115] See fn 45.

significant impact on the quality of the service being provided.[116] These suggestions may help to minimise the risk that the data subject is unaware of what they were consenting to.

In the case of Swedish law, pharmacies can process personal data, even if not within the standard activities of a pharmacy, if the data subject has provided explicit consent.[117] The activities listed in Swedish law, where processing of data for pharmacies is valid, are for example the dispensing of prescribed medicinal products, health-related customer service, systematic and continuous development and quality assurance of outpatient pharmacies and administration, planning, monitoring and evaluation of outpatient pharmacy activities and the production of statistics.[118] Advertising is not included in this list although one could argue that the purpose is a health-related customer service in the case that an online pharmacy offers the patient additional products that could aid in their treatment. Lastly, the Swedish Data Protection Authority has specifically addressed processing for behavioural advertising.[119] In this context, the authority addresses necessary for the performance of a contract although it generally dismisses this lawful basis for behavioural advertising.[120] Furthermore, it states that relying on the fact that personalised advertising indirectly finances the service is not sufficient to rely on this lawful basis.[121]

5 PROCESSING PERSONAL HEALTH DATA FOR SCIENTIFIC RESEARCH

5.1 PURPOSE

Scientific research purposes are also a way for online pharmacies to extract value from the health data they collect. Over recent years, Big Data[122] for scientific research is becoming increasingly more valuable due to advancements in machine learning and artificial intelligence. Now more than ever before, online companies are able to access and process enormous quantities of quality data from consumers on an ongoing basis. The benefits for public health research are immense and can help pharmacies, physicians and pharmaceutical companies provide more accurate treatments for patients.[123] For example, in the area of mobile health (mHealth), the ability to extract additional conclusions from previously unrelated data sets will give researchers new insights for medical research.[124] By combining big data sets, researchers can link certain diseases such as obesity, cardiovascular or

[116] There will always be a deterioration in the quality of the service if you don't provide your personal data since your experience will be less personalised, in particular with regards to recommender systems. Therefore, the word 'significant' is suggested.
[117] 6 § Paragraph 2 of the Pharmacy Data Act (2009:367).
[118] ibid 7 §.
[119] Swedish Authority for Privacy Protection, 'Processing of personal data for the provision of online services' <https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/foretag/behandling-av-personuppgifter-vid-tillhandahallande-av-onlinetjanster/> accessed 29 December 2022
[120] ibid.
[121] ibid.
[122] PGEU, 'Position Paper on Big Data & Artificial Intelligence in Healthcare' (n 18) 3. According to the PGEU, 'In healthcare, Big Data refers to large routinely or automatically collected data, which is electronically stored. This data can be reused and comprise links among existing databases to improve health system performance'.
[123] ibid 5.
[124] European Data Protection Supervisor, Opinion 1/2015, 'Mobile Health, Reconciling technological innovation with data protection' [2015] 9.

depression to data obtained from wearable devices such as human behaviour, lifestyles, geographic area etc.[125] Pharmacists also have an important role in mHealth and even eHealth as more and more patients are asking for advice on how to interpret personal health data they acquire from various sources such as media, the internet and mobile apps.[126] This requires the pharmacist to interpret personal health data through wearable devices and digital points-of-care tests which have an extremely important role in early detection of undiagnosed chronic disease and potential adverse events and also the monitoring of adherence and effectiveness of therapies.[127]

The potential for collecting valuable research data for online pharmacies is infinite. Through the collection of these data, online pharmacies together with scientific researchers can mine large data sets to determine the most effective treatments for specific conditions, identify certain patterns of drug side effects and also patterns of hospital readmissions.[128] For example, a pharmacy could use prescription data to identify and take action against prescribers who exhibit extreme patterns of use of 'high-risk drugs'.[129] This could be done by comparing this information with what the average prescribing of those drugs is in a geographic area. Once the prescribers who are prescribing excessive amounts of 'high-risk drugs' are identified, they may be contacted to ask for explanations as to why they do so and if an insufficient explanation is provided, an online pharmacy could choose not to fill prescriptions issued by these providers. It should be noted here that the possibility of not filling prescriptions of certain providers might be problematic under the laws of Member States in the EU. In Sweden, there is a legal obligation for pharmacies to supply all prescription medicines as soon as possible.[130] Choosing to not fill certain prescriptions will likely infringe this law.

Further uses of personal health data for scientific research include analysing health data gathered from patients to predict whether they might not adhere to their prescribed medicines. Express Scripts, one of the largest pharmacy benefit managers in the United States, collected 22 million gigabytes of healthcare data from 83 million patients to identify whether they were at risk of non-adherence.[131] By identifying multiple dimensions of variables that can influence adherence such as drug related characteristics (side effects experience or physician experience with drug), factors related to the condition itself (patient tenure or adherence to other drugs), healthcare system factors (expertise of physician or dispensing pharmacy), and socio demographic and patient factors (demographics or household stability), Express Scripts was able to identify patients at high risk of non-adherence.[132] If a patient was at risk of non-adherence, Express Scripts would provide

---

[125] ibid.
[126] PGEU, 'Position Paper on Big Data & Artificial Intelligence in Healthcare' (n 18) 3.
[127] ibid.
[128] Carolyn Ma et al, 'Big data in pharmacy practice: current use, challenges, and the future' (2015) 4 Integrated Pharmacy and Research Practice PL 91, 92.
[129] ibid 94. This study was carried out by CVS Pharmacy in the US which used two 2 years worth of data to identify and take action against prescribers who exhibited extreme patterns of use of 'high- risk drugs'. CVS then elected not to fill the prescriptions of certain prescribers that could not justify these extreme patterns.
[130] See fn 39.
[131] Lawrence (n 24).
[132] Jason Hichborn et al, 'Improving patient adherence through data-driven insights', (*Mckinsey*, December 14, 2018) <https://www.mckinsey.com/industries/life-sciences/our-insights/improving-patient-adherence-through-data-driven-insights> accessed 15 November 2022.

personalised interventions by assigning the patient to a therapeutic resource centre where groups of pharmacists and nurses with disease specific experience were on hand to provide expert advice via telephone on medicine adherence.[133] Express Scripts claims that for hepatitis C patients, the support it provided has cut that rate of non-adherence to curative treatment from 8.3% to 4.8% saving approximately 30,000 dollars in medicine costs for patients.[134] It also claims that by using over 300 factors to predict patient adherence for more than 12 different diseases including diabetes and high blood pressure, it has managed to obtain a 94% accuracy rate in its predictions.[135]

With regards to the destination of health data for scientific research, it is not always the case that online pharmacies will have to outsource it to specialised life science companies or academic institutions. This will provide significant competitive advantages in the case that the research is not shared with rivals. In the case of Big Tech companies, Google, through its comparative online shopping services for pharmacies and Amazon, through its online pharmacy service, will be able to collect and use valuable research data internally to perform their own studies on health-related issues. Alphabet, Google's parent company, already has its own life science companies called Verily and Calico. Although recently disbanded, Amazon had potentially entered the life science industry by partnering with Berkshire Hathaway and JP Morgan to reportedly achieve a better satisfaction of their respective workforces.[136] Furthermore, in 2021, Jeff Bezos invested in a biotech startup called Altos Labs that studies human ageing.[137] Concerns have been raised regarding Big Tech companies collecting data for scientific research. Their ability to construct large repositories of data on public health, fitness, genomic and health records and thus control and establish the rules of access to large-scale databases could allow them to reshape the domain according to their values and interests.[138] Furthermore, the large data sets they collect on individuals' health and lifestyle could result in significant risks to privacy.[139]

5.2 LAWFUL BASES

It is important to note that when dealing with personal data being processed for the purpose of scientific research, there are two types of data usages. The importance of making this distinction is that depending on the type of use, the lawful basis will be different.[140] In the first case, there is primary use which means that personal health data is directly collected for

---

133 Lawrence (n 24).
134 ibid.
135 ibid.
136 Caterina Lucchini, 'Amazon's first steps into the business of life sciences' (*Pharma World* 13 April 2018) <https://www.pharmaworldmagazine.com/amazons-first-steps-into-the-business-of-life-sciences/> accessed 15 November 2022.
137 Antonio Regalado, 'Meet Altos Labs, Silicon Valley's latest wild bet on living forever' (*MIT Technology Review,* September 4 2021) <https://www.technologyreview.com/2021/09/04/1034364/altos-labs-silicon-valleys-jeff-bezos-milner-bet-living-forever/> accessed 15 November 2022.
138 Luca Marelli, Giuseppe Testa and Ine Van Hoyweghen, 'Big Tech platforms in health research: Re-purposing big data governance in light of the General Data Protection Regulation's research exemption' (2021) 8(1) Big Data and Society SAGE Journals <https://journals.sagepub.com/doi/full/10.1177/20539517211018783> accessed 15 November 2022.
139 ibid.
140 EDPB, 'Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak' (n 32) 6.

the purpose of scientific research.[141] In the second case, there is secondary use which means personal health data is further processed for another purpose than that for which it was initially collected.[142] Secondary use is the most relevant in the context of data collected by online pharmacies.

With regards to specific lawful bases under the GDPR for the primary use of health data for scientific research, Article 9(2)(j) provides a lawful basis when processing is necessary for scientific research purposes.[143] According to the GDPR, processing of personal data for scientific research purposes should be interpreted in a broad manner 'including for example technological development and demonstration, fundamental research, applied research and privately funded research'.[144] Furthermore, the GDPR specifies that scientific research should also include studies carried out in the 'public interest in the area of public health'.[145] The EDPS has taken its own view regarding the definition of scientific research stating that in order for the research to fall within the specific protection regime of the GDPR, '3) the research is carried out with the aim of growing society's collective knowledge and wellbeing, as opposed to serving primarily one or several private interests'.[146]

These definitions do not mean that private actors, such as an online pharmacy cannot carry out scientific research. Profit-seeking commercial companies and not only academics or public institutions may carry out scientific research according to the GDPR.[147] The key is that the research is carried out in the public interest. Although the public interest requirement is reasonable as large private corporations should not be able to use European citizens' personal health data for their own economic interests, there still exists uncertainty as to how to define public interest in this context. This is problematic as loopholes may be found and can pose significant threats to an individual's fundamental right to privacy. Furthermore, large technology platforms are increasingly becoming gatekeepers of valuable personal health data for scientific research[148] which they may use for objectives that should in fact fall outside the notion of public interest in the GDPR. The current EU legal framework and guidelines are currently insufficient to address these concerns. Vague definitions provided by the EDPS such as when 'research is carried out with the aim of growing society's collective knowledge and wellbeing'[149] do not provide sufficient clarity and therefore further explanations are required.

In this regard, much welcome action is beginning to be taken at a European level to guarantee that health data is used for public interest purposes. The European Health Data Space (EHDS) regulation, currently being proposed by the European Commission, is becoming of increasing relevance in the area of health data and scientific research in

---

[141] ibid.
[142] ibid.
[143] GDPR, art 9(2)(j).
[144] ibid recital 159.
[145] ibid.
[146] European Data Protection Supervisor, 'A Preliminary Opinion on data protection and scientific research' [2020] 12.
[147] EDPS, 'A Preliminary Opinion on data protection and scientific research' (n 146) 11. Recital 159 of the GDPR makes reference to Article 179(1) TFEU which allows for private actors to conduct scientific research.
[148] Jane Thomason 'Big tech, big data and the new world of digital health' (2021) 5(1) Global Health Journal, 2 <https://www.sciencedirect.com/science/article/pii/S2414644721000890> accessed 22 December 2022.
[149] EDPS, 'A Preliminary Opinion on data protection and scientific research' (n 146) 12.

Europe.[150] The objective of the EHDS is to create a common space where natural persons can easily control their electronic health data.[151] It will also make it possible for researchers, innovators and policy makers to access this electronic health data in a trusted and secure way that ensures and safeguards the privacy of European citizens.[152] The EHDS will be relevant for large technology platforms as well as online pharmacies as they will be considered data holders and thus will have a duty to make a vast array of electronic health data available on these common spaces.[153] The current EHDS proposal logically does not permit using the health data on these common spaces for advertising purposes.[154] There are of course disadvantages to the EHDS such its potential to limit the incentives of private entities to collect and process vast amounts of valuable health data but this discussion is beyond the scope of this article.

With regards to other lawful bases under the GDPR for the processing of personal health data for scientific research, the EDPS has provided clarifications in one of its preliminary opinions.[155] For example, it mentions explicit consent as a suitable option when processing for scientific research.[156] What is interesting here is that if an online pharmacy relies on explicit consent rather than scientific research under Article 9(2)(j) GDPR, this would suggest that they could use personal health data for research that does not have to serve the public interest. This could result in the exploitation of personal health for questionable purposes. It could also provide them with significant competitive advantages, especially for dominant players, who may use their health data insights to eliminate rivals.[157] Yet if the individual is fully aware of what they are consenting to, from a strictly data protection law perspective, processing for non-public interests should be possible.

In addition to explicit consent, public interest in the area of public health under Article 9(2)(i) GDPR is also mentioned as a lawful basis for processing special categories of personal data for research.[158] This is in line with the GDPR which states that scientific research may include studies in the public interest in the area of public health.[159] Again, there is ambiguity as to the definition of public interest. In this context, the EDPS refers to CJEU case law which states that it must imply a 'pressing social need' as opposed to private or commercial advantages.[160]

On a final note, it is important to mention that although the GDPR permits the use of health data for scientific research purposes other than explicit consent, if an online pharmacy were to rely on legal bases such as scientific research or public interest in the area of public

[150] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' COM (2022) 197 final.
[151] ibid.
[152] ibid.
[153] ibid. See Article 33(1) of the proposal for an extensive list of electronic health data that must be made available for secondary use. Furthermore, Article 33(3) states that this electronic health data includes data processed for the provision of health or care or for public health or collected by entities and bodies in the health or care sectors.
[154] ibid. See Article 35(c).
[155] EDPS, 'A Preliminary Opinion on data protection and scientific research' (n 146).
[156] EDPS, 'A Preliminary Opinion on data protection and scientific research' (n 146) 19.
[157] This is particularly concerning in the case of Big Tech platforms that are increasingly more present in the healthcare industry.
[158] EDPS, 'A Preliminary Opinion on data protection and scientific research' (n 146) 23.
[159] ibid.
[160] ibid.

health, it is required that there is a provision either in Union law or the national law of the relevant Member States. Therefore, in the absence of Union or national law allowing for scientific research on the basis of public interest or scientific research, an online pharmacy could not rely on these articles for processing personal health data for scientific research purposes. National laws in this context will be discussed at the end of this section with Swedish law as an example.

Regarding secondary use of personal data under the GDPR, this is permitted for scientific research purposes under Article 5(1)(b). This article provides that personal data should only be collected for specified, explicit and legitimate purposes and not for other purposes that are incompatible with the initial purpose of processing.[161] There are however exceptions to this rule. Article 5(1)(b) states that 'further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes'.[162] Therefore, should a controller wish to further use personal data that it has collected lawfully from a data subject for scientific research purposes, this will be a compatible purpose with the initial purpose and will not require obtaining the data subject's consent or identifying a Union or Member State law permitting the secondary use. In order for the processing for the initial purpose to be considered lawful, it will have to comply with the requirements in Article 6(1) and Article 9(2) GDPR.

Although scientific research purposes are considered compatible with the initial purpose of collecting personal data, the GDPR provides some additional requirements in order to ensure sufficient protection for the data subject. These requirements are firstly that the controller of the personal data, when further processing the data, must have 'assessed the feasibility to fulfil (scientific) purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data)'.[163] The wording of this recital is not particularly clear as it is not established whether anonymisation or pseudonymisation is required. In order to find an interpretation, one may look elsewhere in the GDPR. Article 89(1) of the GDPR seems to provide further clarification stating that further processing for scientific purposes should be carried out through anonymisation if possible.[164] In the case that anonymisation is not possible, pseudonymisation should be implemented as a safeguard.[165] Even though an answer exists in the GDPR, the lack of clarity regarding the appropriate safeguards is problematic and requires an explanation from the EDPB. Due to the significant risks to the individual's fundamental right to privacy, it is essential that both the private and public sector are clearly aware of the safeguards that they need to implement and act accordingly.

In addition to the requirement concerning anonymisation and pseudonymisation, the GDPR also requires that when the controller intends to further process personal data for a purpose other than that for which it was collected, the data subject must be provided with

[161] GDPR, art 5(1)(b).
[162] ibid. Recital 50 of the GDPR also confirms this exception.
[163] GDPR, recital 156.
[164] ibid art 89(1).
[165] ibid.

information on the new purpose of processing by the controller.[166] This does not require that the controller provide the data subject with a new lawful basis. The data subject must simply be informed that their personal data will be used for a new purpose which in this case is for scientific research.

Although the GDPR provides guidance on the secondary use of personal data for scientific research purposes, the provisions referred to above do not provide any clarity in the case of personal *health* data. The EDPB has however provided some guidance on this matter. More concretely, the EDPB has addressed the question of whether a healthcare provider collecting personal health data from patients and wishing to use those data for a scientific research project is considered compatible with further processing.[167] Here, the EDPB responds that the controller will have to take into account the lawful bases under Article 9 GDPR since health data is involved.[168] Additionally, the EDPB states that even if the healthcare provider relies on a lawful basis in Article 9 GDPR for the initial purpose of processing, this lawful basis might not extend to the processing of health data for scientific research purposes.[169] What this means is that should a healthcare provider, eg an online pharmacy, collect personal health data for the purpose of prescribing medicines and, rely on for example the provision of health care under Article 9(2)(h) GDPR as a lawful basis, this lawful basis may not extend to further processing for scientific research purposes and therefore an exemption based on Union or Member State's law for the processing of health data for scientific research purposes must be identified. This is in line with Article 9(2) GDPR when processing for scientific research purposes.[170]

The opinion of the EDPB is also in line with the EU Commission's Draft Code of Conduct on privacy for mobile health applications, which addresses personal data collected via my mHealth apps for secondary purposes, eg for 'big data' analysis.[171] As previously mentioned, this Draft Code of Conduct is not a final draft and is still subject to revision.[172] According to the Commission, secondary processing of special categories of personal data for scientific research purposes is compatible with the original purpose for which the personal data was collected if done in accordance with any national or EU level rules adopted for such secondary processing.[173] What this means is that according to the Commission, further processing of personal health data for scientific research purposes is not automatically compatible with the original purpose of processing, as would be the case for personal data under Article 5(1)(b) GDPR, but rather requires the identification of an exemption based on Union or MS law as required in Article 9(2) GDPR for the processing of health data for scientific research purposes.[174]

---

166 ibid art 13(3).
167 European Data Protection Board, 'EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research' [2020] 7.
168 GDPR, art 9.
169 EDPB, 'EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research' (n 167) 7.
170 GDPR, art 9(2).
171 European Commission, 'Draft Code of Conduct on privacy for mobile health applications' (n 105).
172 Osborne Clarke (n 106).
173 European Commission, 'Draft Code of Conduct on privacy for mobile health applications' (n 105) 14.
174 GDPR, art 5(1)(b).

The Commission also clarifies in the Draft Code of Conduct that the controller of the personal data must comply with the principle of data minimisation[175] and furthermore, whenever possible, to anonymise or pseudonymise the personal data.[176] This requirement of anonymisation or pseudonymisation is in line with recital 156 of the GDPR.[177] Furthermore, the Draft Code of Conduct provides that processing of non-anonymised and non-pseudonymised data for scientific purposes should only take place if all other options are exhausted.[178] Lastly, it is important to note that the secondary use of personal health data is only possible for historical, statistical and scientific purposes and not for example big data analytics for market research or communication of health data to insurance companies or employers.[179]

The secondary use of personal health data is also addressed in eTRIX's Code of Practice on secondary use of medical data in scientific research projects which is a legally binding document and was funded by the European Union.[180] In this Code of Practice, the objective is to provide a set of harmonised rules in the EU applicable to secondary use of medical data.[181] With regards to secondary use of personal medical data for scientific purposes, this Code of Practice establishes that the data controller, eg an online pharmacy, must verify that the initial data collection complied with all the applicable legal and ethical requirements and that the secondary use meets current legal and ethical standards.[182] Furthermore, the secondary use of medical data in scientific research shall be anonymised and if this is not possible, the reasons must be justified and documented and the data used shall be pseudonymised.[183] Lastly, the Code of Practice states that in the case of secondary use of personal health care data for research projects, it must be based on either explicit consent of the data subject or on a national law or decision by a competent data protection supervisory authority.[184] Again, there is no automatic compatibility for further processing of personal health data for scientific purposes which is in line with the EDPB and the EU Commission's position.

The EDPB, the EU Commission and eTRIX's Code of Practice all provide the same guidelines regarding the secondary processing of personal health data for scientific research purposes. What may be concluded from these legal instruments is that although the GDPR does not require an additional lawful basis for the further processing of non-special categories of personal data for scientific purposes, it does require an additional lawful basis for further processing of personal *health* data for scientific purposes. These lawful bases are either explicit consent or a national law or decision by a competent data protection

---

[175] Article 5(1)(c) of the GDPR defines data minimisation as the act of ensuring that personal data collected by a processor is 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'. Data minimisation should be applied for all types of processing.
[176] European Commission, 'Draft Code of Conduct on privacy for mobile health applications' (n 105) 14.
[177] GDPR, recital 156.
[178] ibid.
[179] ibid.
[180] Innovative Medicines Initiative eTRIX, 'Code of Practice on Secondary Use of Medical Data in Scientific Research Projects' [2016]. This project was partly funded by the European Union.
[181] Innovative Medicines Initiative eTRIX (n 180) 9. By medical data, the Code of Practice refers to 'Any data concerning patients or study participants health, collected within the context of health care or clinical trials (e.g., name, address, living conditions, health data, life style habits, social security number, image data…)'.
[182] ibid 13.
[183] ibid 13. The Code of Practice establishes rules for anonymization and pseudonymisation in pages 14 to 16.
[184] ibid 18.

supervisory authority permitting the further processing of personal health data for scientific research. In addition to identifying a lawful basis, a controller must justify that it has done its utmost to try to anonymise and pseudonymise as well as comply with the data minimisation principle. It is important to mention that if an online pharmacy manages to anonymise the personal data it collects from patients, there is no need to identify an additional lawful basis as the GDPR is not applicable to anonymised personal data.[185] An additional lawful basis would only need to be identified if the data could not be anonymised. Lastly, the data subject must also be informed of the new purpose of processing, in this case for scientific research.

The fact that all of the previously mentioned legal instruments provide the same guidelines is a positive note as there seems to be a general consensus at an EU level regarding the requirements for secondary processing of special categories of personal data. Preventing the compatibility possibility under Article 5(1)(b) GDPR from extending to processing special categories of personal health data is a logical measure. Due to the great risk that this type of processing poses for the individual's fundamental right to privacy, allowing for processing for a secondary purpose such as scientific research without obtaining a new legal basis would provide little protection. Although this is a positive requirement, the fact that there still exists ambiguity regarding the definition of scientific research, in particular the notion of 'public interest', means online pharmacies relying on a new legal basis such as scientific research may still find loopholes.

Lastly, with regards to processing personal health data for the purpose of scientific research in Sweden, there is no specific legislation regulating this matter.[186] This issue was discussed in the preparatory works for the Swedish Data Protection Act although it was considered that the GDPR combined with additional safeguards in other national laws were sufficient.[187] In the case of Article 9(2)(j) allowing for processing for scientific research purposes, the requirement of the GDPR for a national law to establish this lawful basis is not fulfilled in Sweden and thus relying on this article is problematic. Some scholars have argued that, generally, the lawful basis for processing special categories of personal data in Sweden is public interest which would include public interest in the area of public health under Article 9(2)(i) GDPR.[188] In the case of private research such as that carried out by pharmaceutical companies, as it is less likely that the public interest requirement will be fulfilled, explicit consent would be the appropriate legal basis.

Explicit consent may also be the only possible legal basis for processing health data for research in Sweden as is established in certain cases under the Ethical Review Act.[189] With regards to secondary use of personal health data for scientific research purposes, Swedish law does not provide any specifications on this matter and therefore the aforementioned interpretation of the GDPR should be relied upon. Finally, the Swedish Data Protection

---

[185] Article 2(1) GDPR states that '[t]his Regulation applies to the processing of personal data […]'. Article 4(1) defines personal data as 'any information relating to an identified or identifiable natural person'. Anonymised data does not relate to an identifiable natural person and therefore lies outside the scope of the GDPR.

[186] Magnus Stenbeck, Sonja Eaker Fält, and Jane Reichel, 'Swedish Law on Personal Data in Biobank Research: Permissible But Complex' in Santa Slokenberga, Olga Tzortzatou and Jane Reichel (eds), *GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation across Europe* (Springer 2021) 385.

[187] Government bill 2017/18:105 (n 56) 96. Preparatory works in Sweden have legal authority.

[188] Magnus Stenbeck et al (n 186) 385.

[189] 1 § of the Ethical Review Act (2003:460) states that the Act 'contains regulations concerning the ethical vetting of research concerning humans and biological material from humans. It also contains regulations concerning consent to such research'.

Authority has provided some vague guidance on the application of Article 9(2)(j) for scientific research purposes in the context of clinical research.[190] For example, when addressing whether the processing can be considered proportionate to the purpose pursued, it states that it is crucial to clearly identify the risk and consequences to the data subject as a result of the processing.[191] Furthermore, it suggests appropriate safeguards that could be used such as opt-out options allowing for the individual to object.[192]

6 CONCLUSIONS

This article has demonstrated the importance of personal health data for the European online pharmacy market and how these data might lead to the potential transformation of the healthcare industry. Through the rich sources of personal health data that they have access to, online pharmacies have the ability to collect vast amounts of valuable health data that if used correctly, can improve the lives of patients all across Europe. For example, we have seen the ability of online pharmacies to detect potential adverse reactions and patients at risk of non-adherence. Furthermore, data from for example patient reviews, patient purchase trends and pharmacist consultations could be extremely valuable for drug discovery and pharmacovigilance. In addition, the ability of online pharmacies to improve the information supply chain throughout the healthcare system to ensure greater coordination and information exchanges between the different actors will have an enormous impact on health care.

This article has also attempted to help maximise these benefits that online pharmacies can create for health care by providing more clarity, and possibly more legal certainty, regarding the legal instruments applicable to the processing of personal health data in the online pharmacy market. By identifying three key scenarios where online pharmacies may process personal data, namely for dispensing prescription medicines, online advertising and scientific research, and interpreting how the GDPR and Swedish law regulates them, this article has intended to provide online pharmacies with more legal certainty thus allowing them to maximise the utility of these health data without infringing the data subject's fundamental right to privacy.

With regards to the current legal instruments analysed in this text and their ability to regulate the processing of personal health data by online pharmacies, this paper has demonstrated that work still needs to be done. Important areas that still need to be developed are for example the processing of personal health data for online advertising. In particular, balancing legitimate interests in the case of personalised advertisements still leaves a lot of room for interpretation in the context of the online pharmacy market. There also exists uncertainties as to what constitutes manifestly making data available to the public when processing for online advertising. Both of these issues pose a serious risk to the fundamental right to privacy of the data subject, in particular due to the sensitivity of the data being processed. Hopefully more clarifications will be provided in future guidelines and case law.

---

[190] Swedish Authority for Privacy Protection, 'Yttrande över Personuppgiftsbehandling vid antalsberäkning inför klinisk forskning' <https://www.imy.se/remissvar/personuppgiftsbehandling-vid-antalsberakning-infor-klinisk-forskning/> accessed 29 December 2022.

[191] ibid.

[192] ibid.

National laws can also help to provide more concrete rules applicable to specific sectors. Additionally, the definition of scientific research needs to be further addressed as notions such as 'public interest' and 'with the aim of growing society's collective knowledge and wellbeing' still allow room for loopholes for large corporations serving private interests. The EHDS however is a welcome proposal by the European Commission and will certainly ensure that health data used by online pharmacies can be accessed by everyone and ultimately used for the public interest. National laws implementing the GDPR provisions on processing for scientific research purposes will also play an extremely important role in defining public interest.

On a final note, future legal instruments adopted at an EU and national level regarding the processing of personal health data by online pharmacies should always try to find the right balance in order to facilitate the use of personal health data to transform the healthcare system and at the same time protect the individual's fundamental right to privacy. As has been demonstrated in this article, the potential of analysing vast amounts of personal health data by online pharmacies to innovate and benefit public health is immense. Finding this balance is of course a complex task and will require significant discussions between the private, academic and public sectors.

LIST OF REFERENCES

Belleflamme P and Peitz M, *The Economics of Platforms: Concepts and Strategy* (Cambridge University Press 2021)
DOI: https://doi.org/10.1017/9781108696913

Hichborn J, Kaganoff S, Subramanian N, Yaar Z, 'Improving patient adherence through data-driven insights', (*Mckinsey*, December 14, 2018) <https://www.mckinsey.com/industries/life-sciences/our-insights/improving-patient-adherence-through-data-driven-insights> accessed 15 November 2022

Lawrence J, 'Could Big Data be the Future of Pharmacy?' (*The Pharmaceutical Journal*, 20 April 2017) <https://pharmaceutical-journal.com/article/feature/could-big-data-be-the-future-of-pharmacy> accessed 15 November 2022
DOI: https://doi.org/10.1211/pj.2017.20202637

Lucchini C, 'Amazon's first steps into the business of life sciences' (*Pharma World* 13 April 2018) <https://www.pharmaworldmagazine.com/amazons-first-steps-into-the-business-of-life-sciences/> accessed 15 November 2022

Ma C, Smith HW, Chu C, and Juarez DT, 'Big data in pharmacy practice: current use, challenges, and the future' (2015) 4 Integrated Pharmacy and Research Practice PL 91
DOI: https://doi.org/10.2147/iprp.s55862

Mahesh S and Landry B, 'Online Pharmacies: E-strategy and Supply Chain for Pharmaceutical Products', [2016] <https://www.academia.edu/1342308/ON_LINE_PHARMACIES_E_STRATEGY_AND_SUPPLY_CHAIN_FOR_PHARMACEUTICAL_PRODUCTS> accessed 15 November 2022

Marelli L, Testa G and Van Hoyweghen I, 'Big Tech platforms in health research: Re-purposing big data governance in light of the General Data Protection Regulation's research exemption' (2021) 8(1) Big Data and Society SAGE Journals <https://journals.sagepub.com/doi/full/10.1177/20539517211018783> accessed 15 November 2022
DOI: https://doi.org/10.1177/20539517211018783

Purcell D, 'Competition and Regulation in the Retail Pharmacy Market' [2004] Studies in Public Policy, Trinity College Dublin <http://www.tara.tcd.ie/handle/2262/60273> accessed 15 November 2022

Regalado A, 'Meet Altos Labs, Silicon Valley's latest wild bet on living forever' (*MIT Technology Review,* September 4 2021)

<https://www.technologyreview.com/2021/09/04/1034364/altos-labs-silicon-valleys-jeff-bezos-milner-bet-living-forever/> accessed 15 November 2022

Schwab P, Racsa P, Rascati K, Mourer M, Meah Y and Worley K, 'A Retrospective database study comparing diabetes-related medication adherence and health outcomes for mail-order versus community pharmacy' (2019) 25(3) Journal of Managed Care and Specialty Pharmacy PL 332
DOI: https://doi.org/10.18553/jmcp.2019.25.3.332

Stenbeck M, Eaker Fält S, and Reichel J, 'Swedish Law on Personal Data in Biobank Research: Permissible But Complex' in Santa Slokenberga, Olga Tzortzatou and Jane Reichel (eds), *GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation across Europe,* (Springer 2021)
DOI: https://doi.org/10.1007/978-3-030-49388-2_21

Thomason J 'Big tech, big data and the new world of digital health' (2021) 5(4) Global Health Journal 165
DOI: https://doi.org/10.1016/j.glohj.2021.11.003

Wiederrecht W, Sasson Darwish, Callaway A, 'The healthcare data explosion' (Royal Bank of Canada)
<https://www.rbccm.com/en/gib/healthcare/episode/the_healthcare_data_explosion> accessed 15 November 2022