

Progress Report on the General Data Protection Reform

September 2015

european public health alliance





Progress report on the general data protection reform.

Introduction

In July 2012, following the release of the European Commission's draft proposal for a comprehensive reform of data protection rules in the European Union (EU), the European Public Health Alliance (EPHA) issued a Briefing on the General Data Protection Reform (GDPR)¹ providing an overview of key elements and outlining particular concerns from a public health perspective. This included, inter alia commentaries on the 'right to be forgotten', data access and portability, and the role of health data for public health and research aims. The briefing was complemented by an EPHA position paper published in November 2012 which called for a 'comprehensive and far-sighted' Regulation that would safeguard privacy without restricting the use of data for vital health research and clinical trials², which are important for driving forward health gains for Europe's citizens. This position provided the basis for EPHA's subsequent monitoring and advocacy work in this area.

EPHA's overall stance continues to be that health data is particularly sensitive. Misuse of health data can have irreversible and long-term negative consequences for the individual and their social environment, as well as severe repercussions for an individual's fundamental rights.³ Health data thus require a higher level of protection than other types of personal data.

That said, there is an important balance that needs to be struck between protecting privacy and ensuring health research can continue. Personal data play an invaluable role in health research undertaken to make epidemiological progress, combat rising health inequalities and protect public health.

The Data Protection Regulation – as well as existing law - aims to ensure that health data is not misused or used to discriminate. The draft law prohibits the processing of health data except under specific circumstances, for example if consent is given or if the personal data is used for health or research purposes (by approved researchers). It has thus been designed to strengthen controls against discrimination.

The present report serves as a follow-up to previous EPHA policy documents and articles on this topic, taking into account that the public debate has much advanced

¹ <http://www.eph.org/a/5211>

² Given that the Clinical Trials Directive revision is occurring in parallel to the GDPR, it is important to ensure that the transparency provisions contained in the new Clinical Trials Directive do not get compromised by lack of coherence with the GDPR.

³ http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf



since 2012, in line with developments at European (EU) and national levels. Indeed, over the last three years, the General Data Protection Reform GDPR has become perhaps one of the most closely followed pieces of EU legislation – certainly in terms of attracting the interests of a great many stakeholders and lobbyists.

The first objective of this report is to discuss the GDPR from an EPHA ‘health equity perspective’. Secondly, and in particular related to the European Parliament’s amendments and the ongoing trilogue negotiations, light shall be shed on the importance of data sharing for (public) health research purposes to **reinforce EPHA’s stance that health and scientific research should be exempt from obligations to seek specific consent from data subjects.**

Legislative Package

The rapid development of information and communication technology (ICT) has changed the way(s) in which data is collected, processed, stored, shared and disclosed. Today, individuals leave digital traces with every online activity they engage in, and innovative technology such as e- and mHealth, cloud computing and ‘Big Data’ allow for the collection and storage of vast amounts of personal data, including health data. In our globalised world, digital data transfers have become almost routine; however, most individuals are not aware of the potential implications, both positive and negative, of exposing their personal data, and of the complexities that govern the access to and ‘ownership’ of data at different stages of the process.

Against this background, the EU is currently finalising its reform of the existing EU data protection framework (notably, **Directive 95/46/EC**)⁴ in order to ensure that the opportunities afforded by the digital age can be beneficial for people without compromising their right to privacy, and their ability to take appropriate decisions regarding their personal data. The EU General Data Protection package consists of a **draft Regulation** setting out a general EU framework for data protection and a **draft Directive** on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities. This report will focus on the evolving developments related to the proposed Regulation only.

The first goal of the new data protection framework is to fulfil the EU’s mandate according to Article 16 TFEU to protect the privacy and personal data protection of EU citizens. The legal system for the protection of personal data shall be made fit for dealing with increasingly complex digital and technological changes. The second objective is to strengthen individual’s rights, however this goes hand in hand with accelerating the EU’s digital economy, increasing consumer trust, and reducing ‘red tape’ for businesses by creating a single set of rules.⁵ The successful operation of the Digital Single Market (DSM) shall not be encumbered; it is one of the Juncker Commission’s ten priorities. This includes the delivery of the actions contained in the DSM Strategy, launched in May 2015⁶. The third objective is ‘to improve the clarity and coherence of the EU rules for personal data protection and achieve a consistent and effective implementation and

⁴ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 governs the protection of individuals with regard to the processing of personal data and on the free movement of such data. Directive 2002/58/EC deals with the processing of personal data and the protection of privacy in the electronic communications sector.

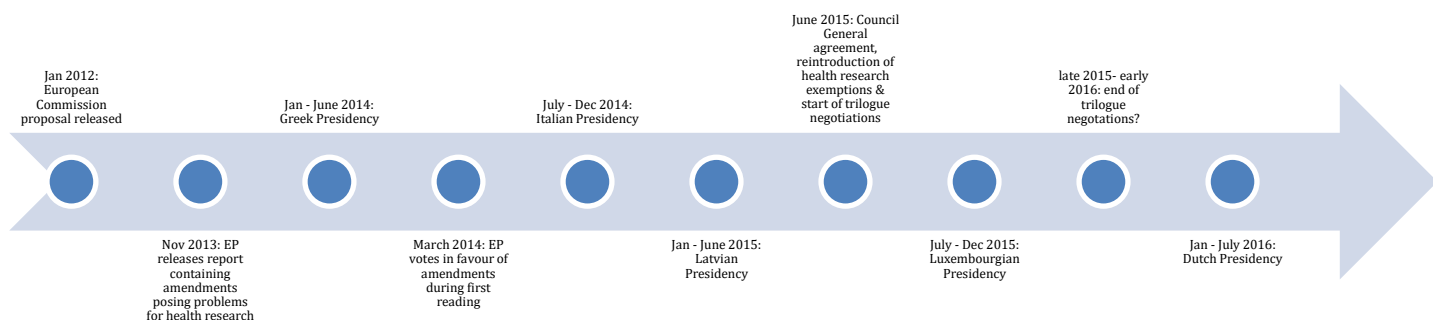
⁵ <http://www.epha.org/a/5539>

⁶ For more information on the DSM strategy’s initiatives, see http://ec.europa.eu/news/2015/05/20150506_en.htm



application of the fundamental right to the protection of personal data in all areas of the Union's activities'.⁷

State of play of legislative process



As can be gleaned from the above timeline, since the release of the Commission’s initial legislative proposal and at time of writing, over three and a half years have passed, which translates into eight different Presidencies of the Council of the European Union (hereinafter “Council”). The latter finally agreed on a General Approach on the draft Regulation at the Justice and Home Affairs Council meeting on 15 June 2015 under the Latvian Presidency in Riga.

The current stage is that the European Parliament, the Council and the Commission are engaged in trilogue negotiations in order to decide on a final draft. As a first step, they are seeking to agree on a roadmap towards the finalisation of the reform.⁸ The shared ambition is to end the trilogue negotiations in December 2015 under the current Luxembourgian Presidency, following the important progress made since the beginning of the year.

The earliest that the modernised framework could be adopted is at the end of 2015, with the Regulation coming into force two years later. However, negotiations could last longer than expected due to the extensive differences between the Council and Parliament texts; the rapporteur has already stated that negotiations might continue into 2016.⁹

⁷ See http://ec.europa.eu/justice/data-protection/review/index_en.htm

⁸ http://europa.eu/rapid/press-release_IP-15-5176_en.htm

⁹ <http://www.euractiv.com/sections/infosociety/eu-lawmaker-warns-data-protection-rules-delay-till-2016-311100>



Context

To recall, the **European Commission** released its proposal for a draft legislative package on data protection in January 2012. The original text introduced a specific and explicit consent obligation for the use and storage of personal data. However, in order to take account of the specific needs of research, it contained **an exemption for the use of research, subject to certain safeguards in Article 83**.

The Commission's proposal was sensible since obliging scientists to seek consent for every new research activity is a very burdensome task that often cannot be accomplished or else is very difficult. Seeking consent can even skew the results of research in some instances or – if studies are large in scope or take place across different countries – it can make studies unfeasible in terms of administration and cost.

Two years later, on 12 March 2014, the **European Parliament** voted in its first reading in plenary in favour of the new rules. The scope of the reforms expanded following the PRISM cyber espionage programme scandal, which amplified public fears over the potential misuses of personal data by governmental authorities and by private companies. Hence the Parliament's amendments under rapporteur Jan Philipp Albrecht (Greens, Germany) introduced more restrictive rules on the use of personal data in comparison to the Commission's draft, which triggered much concern from the public health community, including EPHA, regarding the continued ability to make best use of personal data for health research purposes.

The Parliament subsequently voted to remove the consent exemption for research in its first reading. This would mean that health researchers would be required to re-contact all former study participants for each new research that is carried out on existing data in order to obtain their consent. And although the amendments include an exemption for the use of pseudonymised health data in research without consent, this exemption is extremely narrow, i.e. it would be very difficult to use in practice (see 1.4).

Thankfully, the **Council** reintroduced important provisions that were contained in the Commission text, and the current version provides a much better basis for discussions, and crucially it is more health research friendly than the Parliament's. It remains to be seen whether it could be weakened again during the trilogue discussions as there is an ongoing discord between national Justice Ministers.¹⁰

On the down side, by providing for significant leeway and flexibility for the Member States, the original aim of a consistent and coherent set of data protection rules that apply to all EU Member States appears to be impossible to achieve. Beyond health and research issues, multiple amendments were introduced that, in the eyes of European digital rights organisations, serve to erode privacy protection and regulatory consistency.¹¹

¹⁰

http://www.theregister.co.uk/2015/06/15/grumpy_ministers_grudgingly_agree_a_compromise_on_new_data_protection_law/

¹¹ <http://techcrunch.com/2015/06/15/european-ministers-agree-to-disagree-on-data-protection-reform/>



Consequences of European Parliament's amendments for public health

The Parliament's amendments calling for **explicit consent for each use of personal data** have far-reaching consequences for the re-use of valuable data in health research. Consequently, if health research is undermined, they constitute a serious threat to public health in general.

Therefore, in early 2014 EPHA joined the **European Data in Health Research Alliance (EDHRA)**¹² which endeavours to ensure that research can continue in the same way it does today. The main goal of the EDHRA online campaign is to ensure that health and scientific research are exempt from the obligation to seek specific consent for the use of personal data.

Consent is at the heart of discussions about data protection and research. Without any doubt, it is an important principle in research and – wherever possible – researchers must and indeed do seek consent from data subjects before using their personal data. However, in some specific instances, it is not possible to do so.

Crucially, the Parliament's amendments stipulate that any use of pseudonymised health data must fulfil the criteria of 'high public interest' and the proof that such studies cannot be carried out by using other methods. Both these conditions could make research difficult or impossible to carry out in practise.

For example, given our increasingly mobile world, it could be very difficult or even impossible in some cases to track down individuals who have moved house or country or who have changed their name. The additional burden to re-contact former participants before each new study would thus render many studies, especially large ones, unworkable in practice or highly expensive. It would delay them and increase the time needed to translate results into concrete benefits for patients and society at large, and to advance disease-specific knowledge.

Furthermore, many patients do not wish to be contacted on several occasions. This can be perceived as uncomfortable, cumbersome or intrusive, which in turn could prompt them to refuse giving their consent to additional studies. Data subjects could feel trailed by researchers creating the sentiment that their privacy is not respected, and it could trigger concerns about leaving additional data traces.

¹² <http://www.datasaveslives.eu/>



As pointed out by MEP Catherine Stihler (S&D, UK) on the EDHRA campaign website, the Parliament’s position could also have unintended effects on the studies themselves: sometimes asking consent can undermine the results as participation is arbitrary, some groups of people might be harder to reach than others, and ultimately this will introduce bias which can compromise the robustness of the study.

Example – Case study: EPIC

(source: European Data in Health Research Alliance website, www.datasaveslives.eu/)

What is it?

The European Prospective Investigation into Cancer and Nutrition (EPIC) is the largest study of diet and health ever undertaken, including half a million people across 10 European countries. It is building our understanding of how diet, lifestyle and environmental factors influence health and disease.

Why is it under threat?

EPIC participants have given broad, not specific, consent for the use of their personal data. This allows researchers to link together data about the same person that is stored in different databases, for example cancer registries, to help build an accurate and complete dataset. The Parliament’s amendments would prohibit the use of identifiable health data without specific consent, which could prevent this linkage and undermine the studies. In addition, the amendments could make the use of data from the study difficult or impossible. Where possible researchers will use pseudonymous data, where individuals’ identities are masked. However, EPIC may not pass the strict requirements set by Parliament for the use of pseudonymous health data without specific consent as it could “possibly be carried out otherwise” by re-contacting all participants for consent. This would however create an unsustainable burden for the participants and researchers. It is also unclear whether EPIC would meet the “high public interest” test as this sets an extremely high, but ambiguous, bar.



2. Public health interest in using data

Health data – need for a balanced solution

In its advocacy surrounding the GDPR, EPHA has called upon the EU legislators not to decide on a simplistic one-sided approach but to find a well-balanced solution that respects the privacy and interests of patients and future patients, as well as those of health and scientific researchers for whom access to personal data is the lifeblood of 21st century research.

Crucially, researchers use personal data to advance their understanding of disease, and this underpins our progress on health. There is thus a need to ensure that crucial data which has been collected can be used and shared.

At the same time, it is of utmost importance that personal data is kept safe. This is why vital and effective safeguards have been created within the research sector, for example ethics committees who oversee personal data use and other mechanisms whose explicit role is to keep personal data safe. What is more, the personal data used in research is pseudonymised rather than identifiable. The Parliament's position does not take into account that these safeguards have long been put in place and that they are working well.

Thankfully, the Council's position rectifies this by reintroducing the exemption proposed by the Commission, adamantly stressing the need for appropriate safeguards to ensure that individuals' data are used safely and securely, and that any exemptions are not misused, thereby going beyond the Commission's proposal.¹³

It follows from these two angles that the crucial challenge is to strike a feasible balance between the right of individuals to access and protect their personal data, and the necessity to make relevant data available to researchers or other individuals who are using the data for the public interest, e.g. to improve individual health outcomes, pursue public health goals and reduce health inequalities.

Health data and innovation

Across European health systems, the emphasis on self-help and self-responsibility is growing. Furthermore, the EU is still struggling with the effects of the economic crisis, with enormous pressures on public budgets. Additionally, demographics are changing rapidly, with a rising percentage of older people who also have a longer life expectancy. Meanwhile, the health workforce is experiencing significant gaps in recruitment and retention, combined with brain drain to affluent countries and regions.

European governments are thus highly interested in finding new ways to shift responsibilities to the individual or to the market, to make the care system more efficient and less costly, and empower people to become more active in monitoring and managing their own health. In order to create 'modern, efficient and sustainable' health systems, collecting and handling data is becoming an essential part of modern healthcare.

¹³ <http://www.datasaveslives.eu/news-resources/consent-explained/>



As a sub-category of eHealth, mobile health (mHealth) appears to be particularly relevant when it comes to the collection, communication, and storage of health data generated by individuals themselves. It covers “medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices”¹⁴ and can be used for manifold purposes e.g. healthcare delivery, monitoring, health promotion and prevention, electronic transfer, and as an information tool. The European Commission estimates that, by 2017, 3.4 billion people worldwide will own a smartphone and half of them will be using mHealth apps.¹⁵

Through e/mHealth, national and cross-border health data flows could increase dramatically. If personal data protection rules become too strict, mHealth could face obstacles in its development. On the other hand, if they are too lenient, there could be loopholes undermining individuals’ faith in new technology, potentially even causing harm. The Commission’s Green Paper on mHealth has initiated a discussion about the need of soft vs. hard legislation, and about the ‘grey zone’ between medical and ‘wellbeing’ applications.¹⁶

Cloud computing is a technological development that increases cross-border data flows and storage. It opens up questions regarding the territorial scope of the EU regulatory framework. Cloud computing services offer huge amounts of storage space for data by sharing computing resources rather than having local servers or personal devices.¹⁷ When personal data is processed in the cloud, it usually flows through - and is stored in - various countries, which may also be outside the EU. Certain data protection legislation pertaining to providers with no legal entity based in the EU may however not provide an equivalent level of protection; this could in turn provide opportunities for exploiting data for commercial purposes.

The term ‘Big Data’ describes very large data sets that may be analysed in order to reveal patterns, trends, and associations which can, for example, be useful in order to learn more about disease interactions, or to stratify patient subgroups. Europe’s ‘Big Data’ strategy is testimony to the importance placed on data as an integral part of health systems, and it is aligned with related European strategies (Open Data, Cloud Computing, High-Performance Computing, access to scientific data).

Shaping solidarity

Other elements may be taken into account when assessing the value of data research for society and for public health.

The current trend is that social ethics are overall declining. People are becoming more individualistic and tend to be less loyal to one another, as well as to the ideals of cooperation and community.¹⁸ The value of solidarity – so important in health - is hence diminishing. Reasons for which are manifold and include the increasing lack of understanding of the basic social contract due to the growing complexity of legal rules.¹⁹ Furthermore, trust in established systems is decreasing, e.g. due to dysfunctional labour

¹⁴ World Health Organisation “mHealth – New horizons for health through mobile technologies, Global Observatory for eHealth series – Volume 3”, p. 6.

¹⁵ http://europa.eu/rapid/press-release_IP-14-394_en.htm

¹⁶ <http://www.ephha.org/a/6105>

¹⁷ <https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/Dataprotection/QA/QA10>

¹⁸ Stein Ringen, *Social Security, Social Reform and Social Assistance*, 1998, Netherlands.

¹⁹ Paul Schoukens, Dranny Pieters, *Social Security Quo Vadis?* 2006, Leuven, p. 81.



markets and high unemployment rates, but also austerity measures which introduced stricter eligibility rules for health and social care provision.

In such an environment, data sharing could be an element to reverse this trend. It could **strengthen the ethical value of solidarity in society and empower people to become active proponents of public health**. By enabling the sharing of health data with others, better health can be provided which in turn could have an inclusive effect on society.

3. Implementation of GDPR

The effectiveness of any new legislation depends on its implementation and when it comes to data protection in the area of health, harmonisation may not be possible given **Europe's many different health systems** and data protection cultures. Critically, making data protection advantageous for research must never legitimise the exploitation of personal health data for marketing, profiling or other purposes that put patients at risk or compromise their ability to lead healthy and fulfilled lives.

Therefore, it is also very important that individuals are accurately informed about their rights and about key concepts such as explicit consent. The information should be targeted to specific groups, taking different levels of (health) literacy into consideration. Poor health is directly linked to lower access to education and if vulnerable individuals are not informed appropriately about the concept and dangers of data protection, inequalities will grow.

4. Conclusion

Data and new technology are continuously gaining in importance and reshaping society, including the health sector. The amount of health data that can be collected and processed is increasing steadily and it would be detrimental to public health if Europe could not take advantage of the new possibilities that 'Big Data' and other developments afford to researchers and scientists.

Yet progress also brings new risks for privacy protection, something that is difficult to anticipate in a complex and globalised digital environment. Abusing personal health data can have particularly harsh consequences as it could lead to an increase of health inequalities and exclusion. Therefore, a strong and coherent EU framework is needed that balances individual and collective health needs.

In the name of population health, it is vitally important that public interests such as health research are protected in order to ensure the robustness and vitality of studies and their results.



Hence EPHA supports the following points:

- The final text of the Regulation must ensure that health and scientific research is exempt from the obligation to seek consent for personal data use. This exemption should be accompanied by privacy safeguards that supplement the research sector's existing protections;
- The GDPR must contribute to a climate of transparency that is badly needed to support public health, e.g. in order to avoid duplication of clinical trials, shape new innovation models and promote European solidarity;
- The overall outcome shall not be an extreme solution protecting fundamental rights but a fair balance between individual fundamental rights and public interests.

The New General Data Protection Reform is still under negotiation. Trilogue discussions have started on 24 June and the post-meeting remarks by European Justice Commissioner Vera Jourová reveal that intense discussions are still expected on issues such as explicit consent and incompatible further processing of data.²⁰

EPHA and its partners in the EDHRA campaign will continue to advocate for a realistic and practicable exemption for health and scientific research during the trilogue. There is too much at stake for Europe and for health to accept the amendments introduced by the European Parliament.

²⁰ http://europa.eu/rapid/press-release_STATEMENT-15-5257_en.htm

About EPHA

EPHA is a change agent – Europe's leading NGO advocating for better health. We are a dynamic member-led organisation, made up of public health NGOs, patient groups, health professionals, and disease groups working together to improve health and strengthen the voice of public health in Europe. EPHA is a member of, among others, the Social Platform, the Health and Environment Alliance (HEAL), the EU Civil Society Contact Group and the Better Regulation Watchdog.

EPHA's Transparency register number is 18941013532-08.



european public health alliance

www.eph.org

Rue de Trèves 49-51
1040 Brussels
BELGIUM

TEL: +32 (0) 2 230 30 56

FAX: +32 (0) 2 233 38 80

MAIL: epha@epha.org