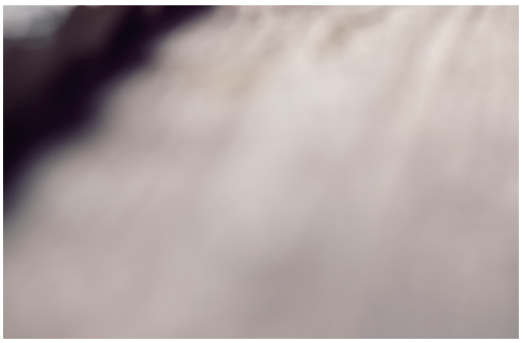
KANTAR HEALTH

CATALYSTS DRIVING
SUCCESSFUL DECISIONS IN
LIFE SCIENCES



HEALTHCARE RESEARCHERS PREPARE FOR GDPR

BY
JESSICA SANTOS

DECEMBER 2017

CONTENTS

GDPR IS A GENERAL DATA PROTECTION REGULATION DESIGNED TO STRENGTHEN CITIZENS' FUNDAMENTAL RIGHTS IN THE DIGITAL AGE AND FACILITATE BUSINESS BY SIMPLIFYING RULES FOR COMPANIES IN THE DIGITAL SINGLE MARKET.

Note: The content of this paper is not legal advice. Please seek qualified local legal advice to determine ways in which GDPR may impact your business.

General Data Protection Regulation (GDPR)[1] is grabbing headlines as the enforcement date (25th of May 2018) approaches. The 2 year implementation period that began 14th of April 2016 aimed to give businesses time to comprehend the regulation and come up with a detailed execution strategy and positioning, but many organizations are still unclear or have different interpretations of GDPR. The 260 pages of the English version consist of 173 recitals (introductory statements) and 99 articles; it is also available in the 24 official languages of Europe.[2] GDPR was drafted with the purpose of creating a consistent approach to data protection for all EU member states and, most importantly, to enhance the rights of European citizens, but its power of significantly higher fines (up to 4% of global turnover) attracts the most attention.

WHAT IS GDPR AND WHAT DOES IT MEAN?

GDPR, or Regulation (EU) 2016/679[3] of the European Parliament and of the Council, is an EU legislation that protects natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC.

The current Data Protection Directive 95/46/EC was enacted in 1995 when the Internet was still in its infancy and most cross border data transfer in analog. The new Regulation is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market. A single law will also do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of approximately €2.3 billion a year[4].

The Directive for the police and criminal justice sector protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities.

GDPR will impose new obligations on organizations, as well, that process the personal data of EU residents. It is a general regulation designed to give citizens more control over their own private information in a digitized world of smartphones, social media, Internet banking, remote data collection and processing, and global transfers, and also sets minimum standards on use of data for policing and judicial purposes.

WHO IS INCLUDED IN THE SCOPE?

GDPR aims to protect all individual EU residents. Therefore, all data controllers and processors offering goods or services (irrespective of payment) or monitoring EU residents' behavior (e.g., tracking on the Internet for profiling) are within the scope, not just those with establishments or use of equipment in the EU (as stated in the Data Protection Directive 95/46/EC). This wider scope includes companies using the Internet to collect and process EU residents' data yet have no establishments in the EU, which are previously outside of the scope. All companies collecting European citizens' data, regardless of whether they are based in Europe or outside, will be required to comply with this legislation.

GDPR MAY PERMIT ORGANIZATIONS TO PROCESS PERSONAL DATA FOR RESEARCH PURPOSES WITHOUT THE DATA SUBJECT'S CONSENT, BUT NOT FOR HEALTHCARE DATA.

WHAT IS THE DIFFERENCE BETWEEN EU DATA PROTECTION DIRECTIVES?

Compared with EU Data Protection Directive 95/46/EC, GDPR strengthens and defines the individual rights to be considered in systems, organizational privacy policies and explicit consent, including:

+ Right of Access: Data Subject Access Requests (DSAR) – e.g. "What do you know about me?"
+ Right to Erasure/Right to be Forgotten – e.g. "Remove me from your database"
+ Right to Rectification – "Amend/correct my details"
+ Right to Restrict Data Processing – e.g. "Stop filming me"
+ Right to Withdrawal of Consent – "I don't want to do this survey anymore"
+ Right of Data Portability – e.g. "'Move my personal data to your competitor X" – very unlikely
+ Strengthened right to prior notification before data collection
+ Right to Reject Automated Profiling - This is a new concept under the GDPR. Profiling is automated processing that is used to evaluate personal aspects of an individual, e.g. being refused insurance based on automated algorithm.

Greater accountability and more detailed compliance responsibilities on BOTH data processors and data controllers are other key differences, together with notifying authorities about data breaches within 72 hours. Pseudonymization is stated as a technique for data de-identification, although pseudonymized data are still within the scope of GDPR.

RESEARCH AS A LEGITIMATE INTEREST FOR DATA PROCESSING

Research is now clearly defined within the GDPR, which was vague under EU Data Protection Directive 95/46/EC, because the EU wants to encourage digital advancement within the EU. Organizations which process EU personal data for research purposes MAY be allowed to: process data without consent; transfer EU personal data to jurisdictions outside the EEA without any transfer mechanisms in place (e.g. model clauses); not grant aforementioned data subjects rights (e.g. request of access or erasure); or avoid restrictions on processing sensitive data, as long as they adopt appropriate safeguards. However, it is unclear exactly what the scope of research is or how far the GDPR's research exemption will extend.

WHAT IS RESEARCH UNDER GDPR?

GDPR stated research under different recitals and each type is treated separately, moreover, the definitions are broad:

Scientific Research (Recital 159): This includes technological development and demonstration, fundamental research, applied research, privately funded research and public health research, with the aim to circulate researchers, scientific knowledge and technology freely. However, although private research for technological development qualifies as research, there may be a requirement that the research be published or made available outside the private entity.

WHETHER HEALTHCARE RESEARCH (E.G. REAL WORLD RESEARCH AND MARKET RESEARCH) CAN USE RESEARCH EXEMPTION IS DEBATABLE.

Public Health Research (Recitals 53 and 54, Articles 36 and 49): "All elements related to health, namely health status, including morbidity and disability, the determinants having an effect on health status, health care needs, resources allocated to health care, health care expenditure and financing, and causes of mortality". Treated as a subset of scientific research under the GDPR, however, it also contains several provisions applicable exclusively to public health records.

Recital 54 clearly noted "public health" should be interpreted as defined in Regulation (EC) No. 1338/2008 of the European Parliament and of the Council, namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality." Furthermore, recital 112 stated "derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport."

Public health research must consult with supervisory authority, or obtain authorization prior to processing, as it may be classified as "high risk".

Historical Research (Recitals 158 and 160): This includes genealogical research, but does not generally apply to deceased people. The exception for archiving in the public interest applies to public and private entities that "hold records of public interest," provided they are under a legal obligation "to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest."

Statistical research (Recital 162): States any collection or processing of personal data necessary for statistical surveys or for the production of statistical results.

WHERE DOES HEALTHCARE RESEARCH FIT?

Will all healthcare research, activities included in the category of scientific research is debatable. Broad interpretation of research can include any data analytics activities from any organization or individuals, which are very common in the big data era; however, there are uncertainties on "appropriate safeguards" and "ethical standard" requirements.

Appropriate safeguard ((Article 89)(1)) is technical and organizational measures to ensure controllers process only the personal data necessary for the research purposes, in accordance with the principle of data minimization (Article 5(c)), which is not clear for research practitioners.

Healthcare research, such as interventional clinical trials or non-interventional studies (NIS), Health Economics Outcome Research (HEOR) or Real World Research (RWR), which has Ethics Committee (EC) approval before execution and publication can be classified as scientific research, but informed consent process is already well-established and treated as an essential steps within, so they are unlikely to remove the consent process or relax its strict guideline, such as Good Clinical Practice (GCP). Most research sponsored or conducted by a public health authority, such as national health services (NHS), can be categorized as public health research.

CONTROLLERS THAT CONDUCT PUBLIC HEALTH RESEARCH MUST CONSULT WITH THE SUPERVISORY AUTHORITY, OR OBTAIN AUTHORIZATION PRIOR TO PROCESSING, AS IT MAY BE CLASSIFIED AS "HIGH RISK".

Questions remain for healthcare market research, business insight research or research sponsored by corporate businesses, such as pharmaceutical companies, which objectives can be brand measurement, examination of unmet needs, patient preference, product improvements, general satisfaction, marketing optimization, and support business decision making as opposed to advancement, discovery or development of knowledge in the medical field, which is mostly conducted by academic institutions. Industry associations, such as EphMRA[5] and BHBIA[6], are publishing guidelines on the position of such research in relation to GDPR. In general, most research will eventually aid better healthcare provision to the general population, and it is recommended to use consent and respond to data subjects' rights.

To benefit the research exemption, several conditions apply, including:

+ Data controllers must provide notice about research at the point of collection.
+ Challenges for researchers will be posed because of the difficulty in identifying ALL research purposes in advance. As research involves exploratory activities, this may be hard to achieve.
+ Researchers must also notify data subjects of their rights under GDPR. Data controllers may not be able to respond to all of them, such as data erasure after database lock or publication.
+ Researchers must confirm period of time data will be stored, or criteria used to determine that period. This requirement of data storage might change based on different legislation, e.g. pharmacovigilance.
+ Researchers must provide consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

However, research MAY be exempt from the notice requirement if they received the personal data from someone other than the data subject, such as where the data came from a publicly available source. Controllers MAY be exempt if "the provision of notice of use proves impossible or would involve a disproportionate effort," which sometimes could be the case in the research context, which are all open for interpretation.

HEALTHCARE RESEARCH STILL NEEDS EXPLICIT CONSENT

While research in general enjoys the recognized position within GDPR, research involving healthcare data still needs explicit consent.

Healthcare data is in the "special categories of personal data", which "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited." (Article 9)

Processing sensitive data is forbidden unless the data subject provides "explicit consent" or it is made public by the data subject. However, a controller MAY also process sensitive data for research purposes, where data was originally collected with consent; processing is necessary for research purposes; it is based on a member state law which is proportionate to the aim (e.g. public interest); respects the essence of the right to data protection, and provides "suitable safeguards". (Article 9(2)(j))

THE UK WILL IMPLEMENT GDPR REGARDLESS BREXIT OUTCOME

Sensitive data may also be further processed for research purposes even if this research was not the purpose for the initial collection, but is "compatible" with the original purpose (Article 6(4)).

HOW WILL BREXIT INFLUENCE THE UK'S POSITION?

The UK Data Protection Authority - Information Commissioner's Office (ICO) published an international strategy on 7th of July 2017 to help protect the UK public's personal information in a global environment and to help it meet overseas data protection challenges, including: increased globalism, changing technology, GDPR and Brexit.[7] It confirms the UK's decision to leave the EU will not affect the commencement of the GDPR.

WHAT ARE HEALTHCARE RESEARCHERS REQUIRED TO DO?

The GDPR implementation date is just around the corner for all organizations. Compliance with the GDPR is clearly a significant business continuity issue.

Given the significant potential fines, no company can afford or risk failing to be compliant with GDPR. Organizations should carry out thorough internal reviews, including:

+ Is our business within the scope of GDPR? Some data controllers or data processors or non-EU companies that are out of the scope under EU Directive should well be covered now.

+ What products and services do we offer? Do they include data analytics, profiling, pseudonymous data, or processing data in a sensitive category? If so, changes in practice will be needed.

+ What type of data are we typically processing? If it's healthcare data, what variables are essential and nice to have?

+ How do we interact with third parties, including joint controllers, processors and vendors? Is any data transfer involved between these third parties? Will cross border data transfer to "inadequate" countries be involved? If so, what are the mechanisms used for the data transfer? Contracts with third parties need be reviewed, especially on liability clauses. Are there any restrictions on data portability?

+ Who is looking after privacy and compliance within the organization? Do we have a data protection officer? It is required within GDPR. Companies can hire internal staff or appoint an external source.

+ Have any privacy impact assessment, privacy by design, privacy policy and general compliance procedures, including data breach notification procedures, been carried out recently? Are your systems and application up to GDPR requirements?

+ Have there been any interactions or consultation with the data protection authorities (DPAs)? There will be no more DPA registration under GDPR, but interaction and cooperation with DPA will increase.

+ What is the legal ground for data collection and processing? Consent is no longer the center of privacy compliance, although it is still necessary for healthcare data processing, and it shouldn't be a tick box exercise. Do we have any restriction on secondary data usage? If so, is the purpose compatible with the consent?

+ How do we interact with the data subjects' requests? Can they access their data or make a request for erasure, objective and deletion? How are their requests handled? Who is managing this? A delegated person or team to handle data subjects' requests is highly recommended.

+ Do we have privacy training in place? Content will need to be updated to GDPR, and individual accountability must be stressed

CONCLUSION

In general, GDPR is welcomed in the 21st century as the current EU Data Protection Directive no longer addresses all privacy issues. Most organizations will need to make some changes to their practice, and European citizens will enjoy their enhanced or newly granted rights to their personal data. Without uniformed interpretation on all recitals and articles, healthcare researchers can still start an implementation plan, and especially review privacy notices, prepare data inventory, and work towards DPIA compliance.

European Data Protection Supervisor[8], the EU's independent data protection authority, provides regular updates and advises on GDPR development. GDPR is no longer lack of awareness; it's entering the final leg of the race before the implementation date on 25th of May 2018.

REFERENCES

1. GDPR - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1462359521758&from=EN
2. GDPR In Different Languages http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_5419_2016_INIT
3. BHBIA - https://www.bhbia.org.uk/guidelines/gdprupdates.aspx
4. EphMRA - http://www.ephmra.org/news/General-Data-Protection-Regulation-GDPR---Update
5. ESOMAR - https://www.esomar.org/news-and-multimedia/news.php?pages=1&idnews=195
6. IAPP - https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-5-profiling/
7. https://www.linkedin.com/pulse/stop-press-gdpr-published-ojec-ardi-kolah-ll-m
8. www.privacylaws.com/Publications/enews/International-E-news/Dates/2015/12/Political-agreement-reached-on-the-EU-DP-Regulation-and-Directive1/

OTHER SOURCES

+ https://iapp.org/conference/gdpr-comprehensive-brussels/
+ https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/?mkt_tok=eyJpIjoiWW1ZNE0yTmlaR1k1TjJOaSIsInQiOiJwandyUzRZMkh0a3FKK3owaDhLOFZxbkN3TkVVNm1tUTFpWWZRNWdRdEh2eW1QZW5IVGRKT1M3TnpMNTA5THBmK1NSV29OZmJmcm56d2pMbkNVVlwvWTB4NDJod0JkOEtLY0xvS0ZXVVdUbDg9In0%3D
+ https://edps.europa.eu/sites/edp/files/publication/15-07-30_strategy_2015_2019_update_en.pdf
+ https://bigdata.fpf.org/wp-content/uploads/2015/12/Tene-Polonetsky-Beyond-IRBs-Ethical-Guidelines-for-Data-Research1.pdf

ABOUT THE AUTHOR

JESSICA SANTOS, PH.D.

Dr. Jessica Santos is the Global Compliance and Quality Director at Kantar Health, the largest custom market research company focused on the life sciences industry. She is primarily responsible for providing oversight and support across the 40+ Kantar Health global offices in the areas of regulation, interaction with clients, suppliers and others within Kantar Health, Kantar and WPP. Dr. Santos is responsible for maintaining, anticipating and coordinating all activities with regard to compliance laws/regulations, industry guidelines, pharamcovigilance and client contracts, defining and driving the execution of Kantar Health's Quality Strategy – our approach to measuring and improving our quality efforts.

Dr. Santos is an experienced statistician, analyst, methodologist and market research scientist. She gained her reputation through her publications and professional committee work in the industry. She is a frequent speaker and contributor in major conferences and has a Ph.D. in Marketing, an MRS fellowship and Chartered Marketer status.

Dr. Santos is a member of UK Research Ethics Committee, EphMRA, BHBIA and PMRG Government Affairs Committee, reviewer and co-chair of ISPOR, and MRS Professional Development Advisory Board and Examiner.

FOR MORE INFORMATION

Please contact info@kantarhealth.com, or visit us at www.kantarhealth.com.

WHY KANTAR HEALTH?

Kantar Health is a leading global healthcare consulting firm and trusted advisor to many of the world's leading pharmaceutical, biotech and medical device and diagnostic companies. It combines evidence-based research capabilities with deep scientific, therapeutic and clinical knowledge, commercial development know-how, and brand and marketing expertise to help clients evaluate opportunities, launch products and maintain brand and market leadership. Our advisory services span three areas critical to bringing new medicines and pharmaceutical products to market – commercial development, clinical strategies and marketing effectiveness.