European Psychiatry 54 (2018) 57–58

Contents lists available at ScienceDirect

European Psychiatry

journal homepage: http://www.europsy-journal.com

Viewpoint

New European privacy regulation: Assessing the impact for digital medicine innovations

The use of smartphone based data streams in relation to mental health research is steadily gaining traction in the field [1]. This approach, also known as *digital phenotyping*, yields continuous behavioural data which shows promise in uncovering new perspectives on human behaviour [2]. However, calls have recently been addressing the need for increased awareness regarding the privacy of the participants [3]. These concerns coincide with the new European *General Data Protection Regulation* (GDPR) that came into effect 25 May 2018 [4]. In most cases, the GDPR will fundamentally impact how research should go about handling highly sensitive (medical) data, since the GDPR comes with some new responsibilities and obligations for both controllers[1] and processors[2]. One of these obligations requires organisations to carry out a Data Protection Impact Assessment (DPIA). This article will assess the impact of such a DPIA on research in practice

1. About the GDPR

The road to compliance with the GDPR proves to be a challenging path for small scale and tech-driven research initiatives. First, limitations regarding technical and legal knowledge gaps need to be overcome. Second, being a technology driven initiative, proper security standards need to be met and maintained in order to ensure that participant data is handled responsibly. This calls for an interdisciplinary approach to research projects operating in this space. Thereby drawing from various additional specialisations, such as biology, law and informatics.

The GDPR lays down the rules relating to the protection of personal data, which is defined as "any information relating to an identified or identifiable natural person". Although the GDPR specifically mentions that identification can take place via identifiers such as name, identification number and location data, identification is not limited to these identifiers. The GDRP does not only set out rules for dealing with personal data, it also offers a tool that can help to implement mandatory practices as laid out in the GDPR: a Data Protection Impact Assessment.

2. Data protection impact assessment

Research data management concerns different stages, namely preparation, data collection, data processing, data analysis, data preservation, access to data and publication and re-use. Since a DPIA helps to visualise the impact of the intended data processing, the DPIA should take place at the end of the preparation phase, or the beginning of the data collection phase. A DPIA is not always mandatory, however, in many instances carrying out a DPIA is still advisable since it will help to both build and demonstrate compliance with the GDPR [7]. For example, a DPIA might help to comply with the requirements of data protection by design and by default.

The GDPR does not define the concept of a DPIA in detail, but sets a number of minimum requirements instead. These minimum requirements, such as an assessment of the necessity and proportionality of the processing operations in relation to the purposes, result in the situation where both the content of the assessment and the way in which a DPIA is carried out is left to the discretion of the controller. The advisory body known as the European Data Protection Board (EDPB) and previously known as the Article 29 Working Party specify that the controller can choose the methodology, as long as the methodology is compliant with the criteria provided in their guidelines.

Concerning the question of when a DPIA is obligated, the GDPR gives some general guidelines. For example, if new technologies are used and the processing is '*likely to result in a high risk to the rights and freedoms of natural persons*' the controller is obliged to carry out a DPIA before the processing starts. The term 'new technologies' is not defined by the GDPR, but is described by the recitals of the GDPR as '*in accordance with the achieved state of technological knowledge*'. Furthermore, three situations in which a DPIA has to be carried out are described in paragraph 3 of article 35 GDPR. Although these three situations are meant as a non-exhaustive list, it does offer some support to the controller if a decision has to be made whether or not a DPIA is needed. Paragraph 8 of article 35 GDPR mentions that if codes of conduct are in place, compliance to these codes have to be taken into account, in particular for the purpose of a DPIA. Therefore, researchers could really benefit from the development of such a (European) code of conduct.

[1] The controller determines what data is collected, how this is done and for which purpose (article 4(7) GDPR).

[2] Processors never determine the purpose and means of data processing, they merely process the data collected by the controller on behalf of the controller and under the instructions of the controller (article 4(8) GDPR).

http://dx.doi.org/10.1016/j.eurpsy.2018.07.003

3. Practical implications of the DPIA

Scientific research is, by nature, innovative and therefore often inclined to push the existing limits of knowledge. As a result, for studies requiring the use of personal data, a DPIA is most probably needed and can enhance transparency. This article uses the BEHAPP programme as introduced next, as an example to show how the GDPR, focussed on the DPIA, affects digital phenotyping research in practice.

4. BEHAPP

The BEHAPP programme is centred around the use of passively collected smartphone data to help quantify human behaviour in terms of communication and exploration [5]. The supporting software, BEHAPP V2, has been developed by the University of Groningen (Faculty of Science & Engineering), a non-profit academic organisation. One of the major design goals of BEHAPP V2 is that it is built as a research platform allowing for multiple simultaneous and configurable studies. This has resulted in various initiatives that are currently employing BEHAPP in their respective lines of research helping to evaluate clinical relevance of digital phenotyping tools in practice. For example, BEHAPP is implemented to identify novel digital biomarkers for social withdrawal in patients suffering from schizophrenia, Alzheimer's disease, and Major Depression in the PRISM study [6], a large EU funded Innovative Medicine Initiative project. In the BEHAPP programme scientists from the Faculty of Science and Engineering work closely together with, among others, scientists from the Faculty of Law. This interdisciplinary approach has proven helpful in light of the GDPR in general and a DPIA specifically.

In this case, the BEHAPP working context is especially interesting, since the programme is both the producer of the app and a joint controller of the data collection. In the latter case this means that article 26 GDPR applies, since that article deals with the situation of joint controllers. Article 26 GDPR determines that joint controllers have to determine their respective responsibilities in a transparent matter. In the case of BEHAPP, the consortium agreement or the data management plan could be used for this. On the other hand, the privacy statement of the app should also make notice of the situation of joint controllers. Since participants are furthermore divided in several groups, for example focus groups and patient groups, this impacts the question of transparency.

For BEHAPP awareness of the GDPR comes at a relatively late stage with the service already in active use by different studies. Nonetheless, the initiative is currently going through its first DPIA cycle and based on the initial review, BEHAPP is now expanding and improving on its policies detailing privacy and information security. Transparency is key and depending on who will be using the service (e.g. Schizophrenia patients or healthy controls) different tailor made documents have to be developed to secure understanding of data use by the participant.

Furthermore, the design reflects principles taken from concepts such as data protection by design and by default. For example, participant records are pseudonymised through a practice also known as *coding* so participants can only be referred to through a unique identifier and no directly identifiable information is stored in the system, with the exception of location data, which is collected as part of the measurements taken by the smartphone application.

Lastly, since privacy protection is a continuous process, going forward in line with GDPR this means that efforts must continue to improve data protection. The GDPR demands technical and organisational measures are taken to ensure data protection. From a technical perspective this is established by applying increased isolation measures on sensitive data and by applying encryption. From an organisational perspective researchers are trained on responsible use and handling of sensitive data.

5. Concluding the cycle

In the case of BEHAPP, this DPIA is a first-time experience for all parties involved. It has shown that an interdisciplinary approach is essential to responsibly create and operate a tech-driven research initiative. A DPIA can help bring deficiencies to light which otherwise may not have surfaced. The cycle enforces all parties to continuously remain critical on technical developments while aligning these efforts to data protection frameworks like the GDPR. At the same time it is important to remain mindful of the (often) limited capacity of small scale and tech-driven research initiatives. This is why we plead for a (European) code of conduct, which could really benefit researchers.

References

[1] Torous J., Staples P, Barnett I, Onnela J, Keshavan M. OPEN A crossroad for validating digital tools in schizophrenia and mental health. NPJ Schizophr 2018;1–2, doi:http://dx.doi.org/10.1038/s41537-018-0048-6.
[2] Insel TR. Digital phenotyping: technology for a new science of behavior. JAMA 2017;318:1215–6.
[3] Marsch LA, Wallace AG. Opportunities and needs in digital phenotyping. Neuropsychopharmacology 2018;1–2, doi:http://dx.doi.org/10.1038/s41386-018-0051-7.
[4] General data protection regulation. 2016. . (Accessed 5 June 2018) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=EN.
[5] Eskes P, Spruit M, Brinkkemper S, Vorstman J, Kas MJ. The sociability score: app-based social profiling from a healthcare perspective. Comput Human Behav 2016;59:39–48, doi:http://dx.doi.org/10.1016/j.chb.2016.01.024.
[6] Kas MJ, Penninx B, Sommer B, Serretti A, Arango C, Marston H. A quantitative approach to neuropsychiatry: the why and the how. Neurosci Biobehav Rev 2017, doi:http://dx.doi.org/10.1016/j.neubiorev.2017.12.008.
[7] Article 29 Data Protection Working Party. 248 Rev01 2017. ec.europa.eu/newsroom/document.cfm?doc_id=47711 (Accessed 5 June 2018).

Trix Mulder[a,*]
[a]*Security, Technology & e-Privacy Research Group, Faculty of Law, University of Groningen, PO Box 716, 9700 AS Groningen, The Netherlands*

Raj R. Jagesar
Groningen Institute for Evolutionary Life Sciences, Faculty of Science and Engineering, University of Groningen, PO BOX 11103, 9700 CC Groningen, The Netherlands

Aline M. Klingenberg
IT-Law, Faculty of Law, University of Groningen, PO Box 716, 9700 AS Groningen, The Netherlands

Jeanne P. Mifsud Bonnici
Security, Technology & e-Privacy Research Group, Faculty of Law, University of Groningen, PO Box 716, 9700 AS Groningen, The Netherlands

Martien J. Kas[**]
Groningen Institute for Evolutionary Life Sciences, Faculty of Science and Engineering, University of Groningen, PO BOX 11103, 9700 CC Groningen, The Netherlands

* Corresponding author.

** Corresponding author.
E-mail addresses: t.mulder@step-rug.nl (T. Mulder), m.j.h.kas@rug.nl (M. Kas).

Received 12 June 2018

Available online 16 August 2018