Himachal Pradesh National Law University, Shimla (India)

Journal Articles *ISSN:2582-1903* *Shimla Law Review*

Volume-III (2020)

ELECTROENCEPHALOGRAPHY (EEG)-BASED BRAIN DATA: Under the Lenses of the General Data Protection Regulation

István Böröcz & Paul Quinn

Contents

Volume III	*ISSN: 2582-1903*	April 2020 - March 2021

ELECTROENCEPHALOGRAPHY (EEG)-BASED BRAIN DATA: Under the Lenses of the General Data Protection Regulation

István Böröcz[*] *& Paul Quinn*[**]

*[**Abstract:** Electroencephalograms (or EEGs), used either in scientific research, health care or for well-being purposes are capable of recording inter alia our attention, emotions, arousal, motivation, cognitive states, mental workload, or drowsiness. Such information can give insight to how the brain reacts to various events and thus reveal information about our mind and also our personality. To facilitate the legal understanding of EEG data, this paper discusses when EEGs can represent personal data and looks at attempts to use them inter alia for identification or authentication, without the combination of other data. Although the authors argue that based on the opinion of the Article 29 Working Party on personal data,[1] EEG data might qualify as personal data on its own, due to enormous variability inherent in EEGs several additional factors need to be taken into consideration when EEG data is to be processed. Furthermore, the contribution analyses whether EEG data can qualify as biometric data, data concerning health, or other categories of special data.*

The variability of EEG data means that the question of whether it alone can constitute personal data is never simple. A complex analysis of the particular context in question, together with the technical facets of a particular EEG is always necessary, which will create headaches for not only those wishing to use EEGs going forward, but those tasked with regulating them.]

I

Introduction

The first electroencephalograms (EEGs) were made more than hundred years ago. Although starting its life as a scientific quirk or curiosity, the use of EEGs in a number of areas has become ordinary practice. This includes diverse areas of

[*] Researcher at Vrije Universiteit Brussel (VUB) Research Group on Law, Science, Technology & Society (LSTS). *Email: isborocz@vub.be.*

[**] Professor at Vrije Universiteit Brussel (VUB) Research Group on Law, Science, Technology & Society (LSTS). *Email: paul.quinn@vub.be*.

[1] Article 29 Data Protection Working Party, Opinion 04/2007 on the concept of personal data, WP136.

scientific research, health care and more recently a new generation of commercial well-being applications. An EEG is capable of recording *inter alia* our attention, emotions, arousal, motivation, cognitive states, mental workload, or drowsiness. Such information can give insight for knowing how the brain reacts to various events and thus, reveal information about our mind and also our personality.

The range of important information that can be discerned from EEGs raises important questions concerning privacy and data protection. The paper explores the potential application of the EU's General Data Protection Regulation (GDPR) to such data. Since EEGs can be used to discern information about the health status of individuals, it seems likely that in instances where they relate to identifiable individuals, they are likely to constitute sensitive data. The question remains, whether EEGs themselves (i.e., not accompanied by meta data that aid to identify a data subject) are able to constitute personal data. This question turns on the identifiability of individuals from their EEGs. The answer to this question is important because it is common in many domains (*e.g.*, scientific research and a range of commercial contexts) to assume that EEGs in isolation constitute anonymous data and are therefore not subject to the rigours of the GDPR.[2]

To facilitate the legal understanding of EEG data, the authors provide a brief description of the functioning of the brain and what exactly EEG data is from a biological and technical perspective (section II). Section III discusses when EEGs can represent personal data and also examines possibility and practices, *inter alia*, the issues of identification or authentication, without combining the data generated by EEGs with other data. The authors argue that based on the 'opinion of the Article 29 Working Party on personal data',[3] EEG data might qualify as personal data on its own. Due to enormous variability inherent in EEGs, we identify three factors which needs to be taken into consideration when EEG data is to be processed. These factors are, 'the adequacy of the technology and the uniqueness of the data subject; the sophistication of the processing method; and the dimension of time. Each of these plays an important role in determining whether an EEG can by itself be thought to constitute personal data. Section IV analyses whether EEG data can qualify as biometric data, data concerning health, or other categories of special data.

Section V, reflects on the unique nature of EEG data. Its variability means that the question of whether it alone can constitute personal data is never simple). A complex analysis of the particular context in question, together with the technical facets of a particular EEG is always required. This can be contrasted with other

---

[2] *See* Loren Gush, *Those 'mind-reading' EEG headsets definitely can't read your thoughts*, THE VERGE (Jan. 12, 2016) *available at*: https://www.theverge.com/2016/1/12/10754436/ commercial-eeg-headsets-video-games-mind-control-technology or see the Muse Headband at https://choosemuse.com/

[3] *Id*.

forms of data, *e.g.*, genetic data, for which the personal status of the data is much easier to determine. This will create headaches for not only those wishing to use EEGs but also for those tasked with regulating them.

II

What is an EEG?

A. Technical Features

Electroencephalography is a neurological examination method used for clinical purposes that has been used in some or other ways for almost a hundred years.[4] It was used the first time by German psychiatrist Hans Berger in 1924.[5] An EEG can be defined as a passive, non-invasive, primarily medical,[6] device which records electrical activity of the brain through electrodes placed on various points of the scalp. In the domain of health care, the evaluation of such records contributes to the detection of brain disorders, in particular seizures, head injuries, encephalitis, brain tumours, dementia, coma, etc.[7] Its physical traits and the quality of the records make it an exceptional and widely used neuroimaging tool used beyond health care for various purposes in connection with neuroscience and, as depicted in the introduction, well-being.

The non-invasive nature of EEG (e.g., invasive neurological examination methods require the opening the scalp, wiring electrodes directly in the brain or placing them on its surface) is seen as one of its most attractive features.[8] This avoids the safety, cost and invasiveness-related issues of using a more invasive technique.[9] Such an advantage has made EEG appealing in areas such as scientific research and commercial well-being services where the use of invasive techniques would not be acceptable.

---

[4] Erik K. St. Louis & Lauren C. Frey, ELECTROENCEPHALOGRAPHY (EEG): AN INTRODUCTORY TEXT AND ATLAS OF NORMAL AND ABNORMAL FINDINGS IN ADULTS, CHILDREN, AND INFANTS (2016).

[5] Richard Jung, & Wiltrud Berger, *Fünfzig Jahre EEG. Hans Bergers Entdeckung des Elektroenkephalogramms und seine ersten Befunde 1924–1931*, ARCHIV FUR PSYCHIATRIE UND NERVENKRANKHEITEN 227 (1979), at 279–300.

[6] Article 2 (1) of the Regulation (EU) 2017/745 of the European Parliament and the Council (Apr. 5, 2017) on medical devices (MDR), medical device '*means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the… specific medical purposes…*'

[7] *Supra*, note 4, St. Louis et. al.

[8] The MDR defines invasive device as *"any device which, in whole or in part, penetrates inside the body, either through a body orifice or through the surface of the body."* (article 2 (6) MDR).

[9] MDR recital (2).

Another advantage of EEG compared to other, similar technologies, is that it has an outstanding temporal resolution (i.e., capable to record electric pulses under milliseconds), facilitating excellent evaluation of dynamic cerebral functioning.[10] Such capability renders the EEG an ideal technology to study the precise time-course of cognitive, emotional and behavioural processing. Furthermore, EEGs are relatively cheap, and they are portable (as opposed to other widely used neuroimaging tools, such as functional Magnetic Resonance Imaging, or fMRI).[11] In contrast to excellent temporal resolution an important disadvantage however is the low spatial resolution of EEGs. In general, this method is only capable of recording neural activity accurately near the scalp. This can be compared with fMRI, which detects changes in the brain associated with blood flow (hemodynamic response) as it is coupled with neuronal activity.[12] Thus, it provides for a significantly better spatial resolution (though its temporal resolution is low). Furthermore, the equipment is spacious and expensive.

What data can an EEG record?

An EEG is not capable of measuring thoughts or feelings directly. Rather, it measures electrical impulses of the brain, which can be associated with certain observed moods of feelings etc. When first introduced in the first half of the twentieth century, EEG was plotted on paper. Nowadays, data is displayed digitally as a continuous flow of voltages.[13] It must be noted that while the approach of Berger facilitated only a qualitative analysis, [14] digital signal processing allowed quantitative analysis, thus *inter alia* forming feature vectors such as spectral frequency decomposition or multivariate autoregressive modelling(e.g.,, to assess physiologically relevant connections between the measured signals).[15]

EEG recordings are carried out through electrode arrays placed on the scalp. These are usually metal disks or pellets that connect with the skin with or without a

---

[10] *Supra*, note 4, St. Louis et. al.

[11] Ernst Niedermeyer, and F H Lopes da Silva, ELECTROENCEPHALOGRAPHY: BASIC PRINCIPLES, CLINICAL APPLICATIONS, AND RELATED FIELDS (2005); Steven J Luck, AN INTRODUCTION TO THE EVENT-RELATED POTENTIAL TECHNIQUE (2014).

[12] Nikos K. Logothetis, Jon Pauls, Mark Augath, Torsten Trinath, and Axel Oeltermann, *Neurophysiological investigation of the basis of the fMRI signal*, Nature (412) 150 (2001) doi: 10.1038/35084005; Richard B. Buxton, INTRODUCTION TO FUNCTIONAL MAGNETIC RESONANCE IMAGING (2009).

[13] iMotions, Electroencephalography- The Complete Pocket Guide, available at: https://imotions.com/guides/electroencephalography-eeg/ (last visited 11 Jun., 2021)

[14] *See* Britton et al.

[15] Yvonne Höller and Andreas Uhl, *Do EEG-Biometric Templates Threaten User Privacy? Full Paper*. in IH&MMSec '18: 6th ACM Workshop on Information Hiding and Multimedia Security, June 20–22, 2018, Innsbruck, Austria. ACM, New York, USA, *available at*: https://doi.org/10.1145/3206004.3206006

typically saline-based conductive gel, paste or cream, comprising various sensor numbers ranging from 5 to 300+ electrodes.[16] For faster application, EEG electrodes can be mounted in elastic caps, meshes, or rigid grids, ensuring that the data can be collected from identical scalp positions across sessions or respondents. The electric potential generated by a single neuron is extremely small and hence cannot be noticed by the electrodes. Therefore, EEG activity is always a summation of the synchronous activity of thousands or millions of neurons with similar spatial orientation and the further amplification thereof. Once the sum of the neurons generates an electric field which propagates throughout the brain tissue and the scalp, it can be recorded, digitized, and displayed.

These values are a variety of a number of base frequencies, reflecting certain cognitive, affective, or attentional states, stemming from the respective areas of the cerebrum.[17] It must be noted, however, that the specific frequencies are dependent on individual factors, stimulus properties and internal states. Therefore, experts classify these frequencies based on specific frequency ranges, or frequency bands: Delta band (1-4 Hz): brainwaves in this range have the slowest and highest amplitude and can be associated with the formation and arrangement of memories, acquired skills and learned information.[18] Theta band (4 – 8 Hz): theta waves can be recorded during daydreaming or sleeping states. In awake state, theta waves might be a sign of attention deficit hyperactivity disorder (ADHD), lack of organisation or impulsivity.[19] Alpha band (8 – 12 Hz): alpha waves correlate with sensory, motor and memory functions. They dominate during moments of quiet thought, and similar meditative states. Mental or bodily activity with eyes open suppress these waves. Beta band (12 – 25 Hz): this frequency is associated with a normal waking state of consciousness when cognitive tasks (ranging from both fast -idle complex thoughts) are carried out. Gamma band (> 25 Hz): gamma waves can refer to high levels of cognitive functioning.

Data from EEGs is primarily useful in the detection of brain disorders such as seizure disorders, brain tumours, encephalopathy, or dementia. Outside the medical field it can be used in authentication/identification, meditation, education or creating immersive and emotion-adaptive 'neuro-environments'.[20] 'Muse' is for example an EEG-based well-being device available on the market, which interprets

---

[16] *Supra* note 13.

[17] *Id*.

[18] *Supra* note 11, Niedermeyer & da Silva.

[19] See - *Understanding Brain waves*, NEUROFEEDBACK ALLIANCE, *available at*: http://neurofeedbackalliance.org/understanding-brain-waves/ (last visited 11 Jun., 2021).

[20] *MindSpaces - Art-driven adaptive outdoors and indoors design project*, funded by the European Union's Horizon 2020 programme in the framework of STARTS initiative (Science, Technology & the Arts). Grant agreement number: 825079. *Available at*: http://mindspaces.eu/ (last visited 11 Jun., 2021).

mental activity to provide guidance to the user, in particular in connection with meditation. Through an app, the user can learn about his own mind, heart, breath, and body. Interestingly, such practices were foreshadowed years ago, long before the computing power needed to make such use of EEG data existed. [21] The complexity of data that can, in theory, be gathered has also given rise to discussion concerning the possibility to identify individuals from their EEGs: '*EEG data appear to be highly unique to an individual and thus should be considered extremely sensitive. The ability to identify subjects in data sets may give the ability to match a short recording of the EEG data with data stored in the large sets, and, if the various types of data are linked, also to link to other information about the user...*'[22]

III

What is EEG data under the GDPR?

EEG data are often accompanied by various forms of meta data that may relate to the identity of the individual. A clear example of such data may be unique identifying numbers relating to patients in a medical record. In such instance, where a patient can be identified using meta data there is little doubt that the EEGs represent personal data. This paper however is focused on the question of EEG data themselves – *i.e.* do they constitute personal data in isolation, in the absence of such meta data. This question is not only interesting from an academic sense but increasingly a practical one also. This is because it is often *assumed* that EEG data held in isolation is anonymous and therefore not subject to regulation as personal data.[23] In view of the advancements in computational power and analytical ability, however, such an assumption is increasingly coming into question . Determining the validity of such an assumption is important given that if such an assumption is not correct, the possibility for significant privacy harms may arise. The discussion below analyses this assumption and intends to answer the question whether EEG data (in isolation) can be thought of as personal data .

---

[21] *Supra* note 4, St. Louis et. al.

[22] Arkadiusz Stopczynski, Dazza Greenwood, Lars Kai Hansen, Alex Sandy Pentland, Privacy for Personal Neuroinformatics, arXiv preprint arXiv:1403.2745 (2014), *available at*: https://arxiv.org/pdf/1403.2745.pdf (last visited 11 Jun., 2021).

[23] For example, the privacy policy of the Muse EEG device explains that sharing of Sensor Data, Processed Data and Activity Data might be possible based on the consent of the user on a de-identified basis with third parties involved in research related to improving the scientific understanding of the brain/body or to improving products and/or delivering better experiences and services. *See geneally*, End User License Agreement, *available at*: https://choosemuse.com /legal/ (last visited 11 Jun., 2021)

The human body as information and the notion of personal data

Article 4 (1) of the GDPR identifies personal data as *"any information relating to an identified or identifiable natural person"*. The Article 29 Working Party (hereinafter WP29) in its Opinion 4/2007 on the concept of personal data the definition opined on each of the four elements identified here in ways that are potentially relevant in the context of EEGs. These are:

Any information: As the WP29 outlined, the legislator envisaged a broad concept of personal data, requiring the broad interpretation of "any information". This includes both objective and subjective information, regardless of its format and way of storage. When referring to brainwaves of an actual, living individual, recorded either on paper or digitally, it can be assumed that it meets the criterion of "any information".

Relating to: This element requires that the information should be "about" an individual. Although such requirement seems obvious, data might relate for example to events, objects, or processes. In order to relate to an individual, the information must have a content, purpose, or a result. The first one is provided when information is about a particular person. The second one is present when information is used to treat or influence the status or behaviour of an individual. The third one is referred to when the information is likely to have an impact on the individual's rights and interest. As these are alternative requirements, each of them is enough to fulfil the "relating to" requirement. The authors of this paper would argue that in case of brain data, each of them can be present, depending on the purpose of the processing in question. For example, in case of a medical profile, EEG data serves as content, when providing information during a meditation session it serves as a purpose, when used for authentication it enshrines a result. Given this, the authors of this paper would argue that the second element can also be assumed to be met.

Natural person: in principle, personal data refers to living individuals. Respectively deceased persons are not subject of data protection law, but their personal data might be subject of other forms of privacy law.[24] At the time of recording EEGs will self-evidently relate to natural persons given that they can only be taken from living individuals. As section 3.2.3 below discusses, the question of the possibility of using EEG data after much time has elapsed (and when it is possible the individual in question may be dead, may well be a moot point given that a significant amount of time elapsing arguably makes EEG data less reliable).

Identified or identifiable: an individual is identified when he or she can be distinguished from all other members of a group. Such a determination is to a large

[24] For example, some national laws provide protection of personal data of deceased person until a certain extent, such as the Danish, Hungarian, or Italian Data Protection Acts.

extend probabilistic in nature and does not equate to a requirement of 100 percent certainty. Rather it is better to envisage identifiability as a threshold requirement above which identification can be thought of as being reasonably likely. Identification can occur directly or indirectly. In terms of the former, a piece of information itself can distinguish a person (e.g. name). For indirect identification (as in isolated EEGs data where such information is not available) a combination of information that is unique to a particular individual is required. In the modern technical age it is also necessary to consider what means are available to make such a determination or as the WP article 29 states *"account should be taken of all the means reasonably likely to be used"*.[25] In doing so it is necessary *inter alia* to consider the costs of and the amount of time required for identification as well as the available technology at the time of the processing and technological developments.[26] The latter means that the data controller should take into account the possibility of identification in the foreseeable future, where new technologies or processes may become available that aid identification.

In terms of EEGs identification usually occurs when the data is combined with further information (e.g. a medical profile, containing the results of the EEG scan and further identifiers of the patient). In the past it was not generally considered likely that EEGs in isolation could be used to identify specific individuals. The validity of such assumptions is becoming increasingly questionable, however. This is arguably demonstrated by some of the purpose's EEGs are now being used for. Technology developers and neuroscientists are now for example aiming to achieve direct identification of an individual through EEG data (although the range of application is still very limited). That would mean that individuals can be distinguished based on their measurable brain activity. The section below will discuss this element in further detail.

As the above discussion indicates the first three of the aspects described above are relatively uncontentious. The fourth i.e. identifiability however is a complex affair. Until recently the answer was that in most cases that isolated EEG data could not be used to identify specific individuals. As section 3.2 below discusses however such an assumption is being called into question. Whilst it would be incorrect to state that isolated EEG data always or often constitutes personal data; it seems that it is possible that it may do so in certain contexts.

Aspects of EEG that will affect the chance of direct identification

The nature of EEG data means that it is not always clear whether such data in isolation can be considered personal data or not. Three important factors must be considered in any context when determining whether such data are indeed personal

---

[25] Recital 26 GDPR.

[26] *Id*.

data. These are the sophistication of the neuroimaging tool; the context and the method used to context the EEG data is collected in; and the changes in EEG data than occur with the passage of time.

Sophistication of the technology and the uniqueness of the data subject: As depicted in the first section, the properties of particular EEG devices vary enormously. The application of the electrode arrays with or without conductive electrode gels can for example affect the quality of the recording. Dry electrodes are more prone to distortions brought about by movement, whereas wet electrodes are more resistant, yet more timely to apply. Another relevant difference lies in the number of the electrode arrays, which can range from five to several hundred depending on the quality of the equipment. Naturally, the number affects the placing of the electrodes as well in order to avoid overlapping concerning the recorded areas. In 1994 the American Encephalographic Society introduced (the now widely adopted) 10-20 standard. [27] This established a standard for testing methods. Prior to that if electrodes were placed in different positions, they were likely to record different data, making the comparative analyses difficult and inconsistent. Given this, the goal of the 10-20 system is to indicate the actual distances and positions of the electrodes from each other; they are placed at 10% and 20% points longitudinally and latitudinally. In addition, other standards re available, including the so-called 10-10 and 10-5 systems are based on similar principles and results in higher resolution.[28] The shape of the head,[29] the skull's and scalp's thickness,[30] as well as anisotropy, and inhomogeneity have considerable effects on EEG data that are recorded.

Whereas neuroscientists are likely to be aware of such changes, non-trained users of EEG-based well-being devices may not be. The differences in the equipment being used by varied users can be stark. In the former context a professional EEG with 320+ wet electrodes may be deployed, mounted by neuroscientists, carefully taking into account the individual traits of the individual involved. This can be contrasted with the type of system used in the consumer or well-being context. The currently available 'Muse S' has for example seven dry electrodes. These will usually be

---

[27] American Electroencephalographic Society, *Guideline thirteen: guidelines for standard electrode position nomenclature*, (11) AMERICAN ELECTROENCEPHALOGRAPHIC SOCIETY. J. CLIN. NEUROPHYSIOL., 111 (1994).

[28] Valer Jurcak, Daisuke Tsuzuki, Ippeita Dan, *10/20, 10/10, and 10/5 systems revisited: Their validity as relative head-surface-based positioning systems*, 34(4) NEUROIMAGE, 1600 (2007); *See also* Robert Oostenveld's blog *available at*: https://robertoostenveld.nl/electrode/ (last visited: 11 Jun., 2021).

[29] B. Neil Cuffin, *Effects of head shape on EEG's and MEG's*, 37(1) IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING 44 (1990) doi: 10.1109/10.43614. PMID: 2303269.

[30] Mika Lehtinen, Kimmo Forsmanx, Jaakko Malmivuo, Hannu Eskola, *Effects of skull and scalp thickness on EEG*, 34 (Supp. 1[2]) MEDICAL & BIOLOGICAL ENGINEERING & COMPUTING (1996), *available at*: http://www.isbem.org/conf/1996/1996icbe/2-4-5-10.pdf (last visited: 11 Jun., 2021).

mounted by users without any particular expertise. Whilst this does not mean that data recorded by Muse is 'bad' per se or inaccurate by default, it is necessary to be aware that significant differences between EEGs, the biological differences between users means that there will be enormous various in the resolution and quality of the data concerned. This means that certain forms of EEG data are more likely to be identifiable than others.

EEG context: The second factor to be considered is the context in which EEG data is recorded. Multiple studies demonstrate that EEG data is highly unique to an individual and (in theory) can serve as a *biometric identifier*. Such studies are often conducted using EEG data that has been recorded in a highly specific context. In 2005, for example, an Italian research demonstrated that an individual's EEG profile in the 8 to 15.5Hz frequency range during non–rapid eye movement (NREM) sleep is unique.[31]

In March 2020 Nishimoto *et. al.* published an article which described their use of EEG as a basis for authentication via brain signals.[32] They collected EEG signals from twenty research participants in four rounds. They reinstalled the EEG cap before each round and facilitated the feature extraction with unsupervised learning methods, common dictionary learning and t-distributed stochastic neighbour embedding.[33]

They found that the *'brain activity (EEG) signals include personal features, which are consistent throughout different times of the day, even after reinstalling the EEG caps, and throughout different days, even with possible changes in the physiological states of the subjects'*. Their results achieved a level of forty percent accuracy (Figure 1). The study proves when and how the EEG data can be used for personal authentication (identification).

---

[31] Their sample group consisted of 10 research participants who had participated in a slow-wave sleep deprivation study. Over 6 nights, their profile remained invariant (Figure 2). Furthermore, their subsequent study in 2008 showed that certain personal features relating to the EEG profile during NREM sleep are genetically determined and are heritable. Read more at: Luigi De Gennaro, Cristina Marzano, and Fabiana Fratello et.al, *The Electroencephalographic Fingerprint of Sleep Is Genetically Determined: A Twin Study*, 64(4) ANNALS OF NEUROLOGY 455 (2008).

[32] Takashi Nishimoto, et.al., *EEG-based personal identification method using unsupervised feature extraction and its robustness against intra-subject variability*, 17(2) JOURNAL OF NEURAL ENGINEERING 026007 (2020).

[33] *Id*.

Figure 1. De Gennaro et al. Op.cit.

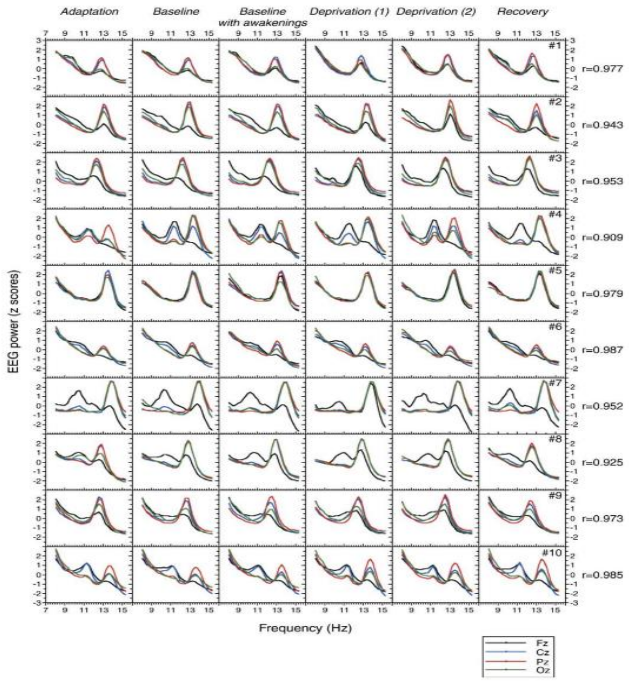
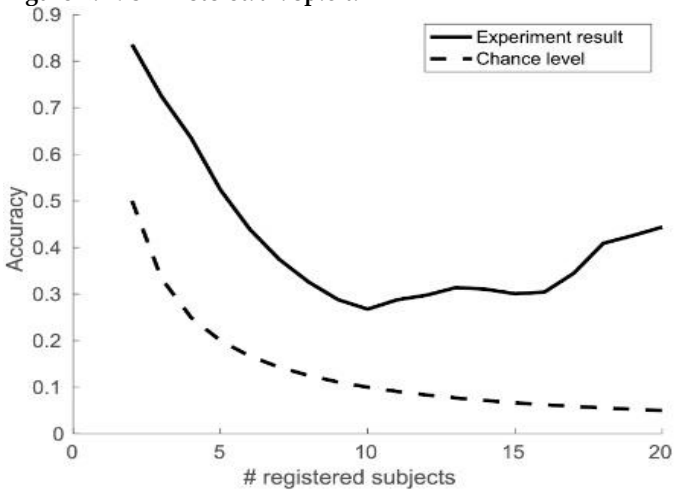


Figure 2. Nishimoto et. al. op.cit.



Using another method, researchers have achieved a far higher figure. Revett *et al*.,[34] Poulos *et al*.,[35] or Paranje *et al*.,[36] claim to have achieved an identification accuracy of eighty or even hundred percent in their research. The applicability of such research may be limited in practical terms since it is related to EEG data that were taken in a resting or sleep state.

What individuals are doing or thinking about whilst their EEG data are being recorded is of immense importance. This was highlighted by Stopczynski *et al*. with reference to the 'P300 paradigm'.[37] This is linked to the notion of the Event-Related Potential (ERP). ERP is a pattern of voltage change, induced by an auditory or visual stimulus within a known timeframe. As explained by Martinovic *et al*., '*the most prominent ERP component which is sensitive to complex cognitive processing is the P300, because it can be detected as an amplitude peak in the EEG signal at ≈ 300 ms after the stimulus*'.[38] Martinovic *et al*. relied on P300 to reveal actual information via EEG, such as the first digit of a PIN, month of birth or the recognition of known people. Although the success rate was twenty to thirty percent (with the exception of sixty percent in one of the experiments), the methodology proved to be working. Similar P300-based tests have been developed for lie detection purposes or in the Guilty-Knowledge test as well.[39] Whilst such research is useful in demonstrating the potential of EEG data to be used for identification purposes, it also demonstrates that this is more likely where the EEG data was recorded under constant conditions. This may mean ensuring that individuals are preforming the same activities or even trying to think about similar things. Where this is not the case, identification of specific individuals may be more difficult. Such requirements may be complicated by the potential effects of neuro modulators (drugs, alcohol, coffee, etc.) which may influence neural function and thus the EEG data that are obtained from an individual.

---

[34] Kenneth Revett & Sergio Tenreiro de Magalhães, COGNITIVE BIOMETRICS: CHALLENGES FOR THE FUTURE. IN: GLOBAL SECURITY, SAFETY, AND SUSTAINABILITY 79–86 (2010).

[35] Marios Poulos, Maria Rangoussi, Nikolaos Alexandris, *Neural network based person identification using EEG features*, Acoustics, Speech, and Signal Processing *in* (2) PROCEEDINGS., 1999 IEEE INTERNATIONAL CONFERENCE ON. IEEE, 1117–1120.

[36] Raman Paranjape, Jeffrey Mahovsky, Luigi Benedicenti & Zoltán J. Koles, *The electroencephalogram as a biometric*, Electrical and Computer Engineering in (2) CANADIAN CONFERENCE ON IEEE 1363–1366 (2001).

[37] *Supra* note 22, Stopczynski et. al.

[38] Ivan Martinovic, et.al., *On the feasibility of side-channel attacks with brain-computer interfaces*, PROCEEDINGS OF THE 21ST USENIX CONFERENCE ON SECURITY SYMPOSIUM (Security'12, 2012) USENIX Association, USA, 34, *available at*: https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf (last visited: 11 Jun., 2021).

[39] Vahid Abootalebi, Mohammad Hassan Moradi & Mohammad Ali Khalilzadeh, *A new approach for EEG feature extraction in p300-based lie detection*, (94) COMPUTER METHODS AND PROGRAMS IN BIOMEDICINE 48 (2009).

The passage of time: The third important factor to consider is that the passage of time can evoke changes in EEG patterns. The brain is a highly plastic structure. It is capable of being altered by the experiences individuals have. This means that the EEG data that an individual provides may also alter with the passage of time. Physiological changes occur in the brain as a result of interactions with the 'environment'. This entails *inter alia* responding to experiences, learning skills, or recovering from injury etc. The phenomenon is referred to as 'neuroplasticity.' We can distinguish between four main types of neuroplasticity: *neurogenesis*, when new neurons are created (e.g., in the young brain); *synaptogenesis*, when new neural connections are established; *long-term potentiation* when the synapses are strengthened (e.g., through learning); and *long-term depression* when the synapses are weakened (e.g., memory loss or disorders).[40] EEG has shown itself to be a useful tool for exploring the concept of neuroplasticity in the context of scientific research.[41] The concept itself means, however, that the likelihood of identification of a specific individual, from EEG data, is likely to reduce with time. The result is that even in instances where an EEG could be considered as constituting personal data, this may no longer be the case after a certain amount of time has passed.

IV

Further Categories of Personal Data

The discussion above relates mainly to the question of whether EEG data, in isolation, can ever be considered to be personal data or not. In cases where it is the question then arises 'is EEG sensitive data or not'? This question is important for two reasons. *Firstly*, the use of sensitive data arguably represents high risk to the fundamental rights and freedoms for the individual data subjects.[42] *Secondly*, as a consequence of the first point, the GDPR attributes a regulatory burden on those are tasked with the responsibility. The GDPR renders specific protection to personal data which are, '*by their nature, particularly sensitive in relation to fundamental rights and freedoms'*.[43] Article 9(1) of the GDPR defines sensitive data as, '*data revealing racial*

---

[40] *See Neuroplasticity*, EMOTIV. *Avialable at*: https://www.emotiv.com/glossary/neuroplasticity/ (last visited: 11 June 2021) and Arno Villringer and Burkhard Pleger, *Plasticity of the human brain - "We never use the same brain twice"*, *available at*: https://www.mpg.de/971989/H_09PlasticityHmnBrainbasetext.pdf (last visited: 11 Jun., 2021).

[41] Giovanni Assenza, Vincenzo Di Lazzaro, *A useful electroencephalography (EEG) marker of brain plasticity: delta waves*, 10(8) *NEURAL REGEN RES.* 1216 (2015). doi:10.4103/1673-5374.162698.

[42] On the concept of 'risks to rights', including discrimination, see Niels van Dijk, Raphaël Gellert, and Kjetil Rommetveit, *A Risk to a Right? Beyond Data Protection Risk Assessments*, 32(2) COMPUTER LAW & SECURITY REVIEW 286 (2016).

[43] Recital 51 GDPR.

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'.

Many of the categories outlined in article 9 could have, at least, a theoretical relevance for a meaningful discussion of the personal data character of EEG data. It can be surmised, for instance, that EEGs can, in theory, reveal information that may be pertinent to political opinions, religious beliefs or even a person's sexual life (imagine an EEG that was taken whilst an individual being exposed to images or information related to one of these themes). In the future, more advanced forms of EEG technologies with increased analytical power may allow practices that would today be associated with the notion of 'mind reading'. Such notions are at present only theoretical speculation and, are at best, a far-off prospect. As such, they will not be explored further in this paper. More realistically applicable sensitive data categories are the concepts of 'health data' and 'biometric data'. The application of such categories to EEG data that relate to an identifiable individual is discussed in the coming sections.

The higher protective regime of the GDPR

The GDPR imposes extra requirements upon data controllers who process sensitive (or special) forms of personal data. First and foremost, the category of sensitive data is a closed and explicit list.[44] These requirements can be broken down into a number of different categories.

First, the GDPR contains specific legal bases that are applicable if sensitive data is to be processed (*i.e.* different to those available for non-sensitive forms of personal data). In general, these legal grounds are more restrictive and less available (i.e. only capable of applying within narrowly defined circumstances) than the legal bases that are available for controllers who wish to process non-sensitive data.[45] The classic example is that of the legal base 'explicit consent', which is purportedly more onerous than the legal base of 'informed consent' available for non-sensitive data. The existence of such legal bases arguably serves a 'barrier function', limiting the processing of sensitive data in certain contexts.

Second, the GDPR aims to restrain automated decision-making using sensitive data only where explicit consent has been obtained.[46] In the era of big data and AI driven

---

[44] Member States can no longer create further categories of sensitive data, as they could under Directive 95/46/EC (though the GDPR now includes the most common ones that Member States had themselves added e.g. genetic data). R Gertz, *Is It 'Me' or 'We'? Genetic Relations and the Meaning of 'Personal Data' under the Data Protection Directive*, 11(3) EUR. J. OF HEALTH L. (2004).

[45] *See* Article 9 of the GDPR.

[46] Such processing is also subject to additional special safeguards adopted by the data controller

decision making, these restrictions seek to reduce the availability of sensitive data for such processes to those context where it is possible to gain such a clear form of consent.

Third, the GDPR also creates a number of administrative requirements that apply even after the 'barrier protection' outlined above is applicable. These requirements include the need for a Data Protection Officer (DPO), under article 37(1)(c), and to perform a Data Protection Impact Assessment (DPIA), under article 35(3)(b) where the processing of special categories of data is 'on a large scale'.

The *fourth* important factor is that, with regards to 'genetic data, biometric data or data concerning health', EU Member States are permitted to 'maintain or introduce further conditions, including limitations' concerning processing.[47] This goes against the general nature of the GDPR which, as a regulation in general, has an important harmonising effect. The result is that for these types of sensitive data EU Member States can maintain a complex and heterogenous web of laws where they go beyond the requirements of the GDPR. This complexity represents an added burden on data controllers, in particular, for those that wish to operate on a cross border basis.

The factors described here provide significant insights to resolve issues such as whether or not EEG data in a particular context is sensitive data. Where it is, data controllers will have to comply with the extra requirements that come with such a determination. In the following paragraphs we will analyse two most likely forms of sensitive data and their potential application.

Biometric data

The GDPR defines biometric data as, *'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'.* The definition consists of three elements: (i) information should be a result of a specific technical processing, (ii) information should relate to the physical, physiological or behavioural characteristics of a natural person, and (iii) such information should allow or confirm the unique identification of that natural person. Specific technical processing as such may refer to a wide range of techniques, but in opting for such a formulation the GDPR has opted for a technology neutral definition, in line with its approach outlined in Recital 15. The second element refers not only to data grasped from first-generation biometrics (e.g. fingerprint or iris scanners) but second-generation biometrics as well e.g., sensors capturing gait, voice, body odour, breath, or even potentially brain data such as

(Article 22(4)).

47 Article 9(4) of the GDPR.

EEG.[48] The choice of wording in the GDPR's definition is capable of applying, both, to identification and verification activities.[49]

From the point of view of EEG data, in this paper, the mention of physical or physiological traits (i.e., bodily characteristics) and behavioural characteristics are of particular importance. Whereas, the former is perceived as the 'usual' type of biometric data relating to definite physical traits, such as fingerprints, iris scans or facial images; the latter category is significantly broader. [50] According to the definition, any behavioural characteristic, which allows or confirms the unique identification of a natural person qualifies as biometric data. 'Behaviour' as a notion can be understood as '*the computed response of the system or organism to various stimuli or inputs, whether internal or external, conscious or subconscious, overt or covert, and voluntary or involuntary*'.[51] This is apparently applicable to human brain data and the brain, involving the reception of inputs from the various sensors in the body, their processing and the sending of commands to various parts of the body to react them, either consciously or subconsciously. When observing brain activity, such processes can be traced, recorded, and interpreted. As discussed above, under section III, numerous researches claim to be able, through the analysis and interpretation of EEG data, to use brain data for authentication and even for identification. In this sense, brain data can be understood as biometric data in the GDPR. Importantly, it is only when data such as EEG is processed specifically for the purpose of identification of individuals, that the data is considered of biometric and a sensitive nature. This is outlined by article 9 in defining the various categories of sensitive data. When referring to biometric data, the definition refers to data used 'for the purpose of uniquely identifying a natural person'.[52] This distinction means that the

---

[48] Emilio Mordini & Dimitros Tzovaras (eds.), SECOND GENERATION BIOMETRICS: THE ETHICAL, LEGAL AND SOCIAL CONTEXT 9 (2012).

[49] As emphasised by Alessandra Calvi and Simone Casiraghi, in Jasserand's understanding „allowing" refers to identification, i.e. the one-to-many process whereby the system compares the captured template with all the available templates to determine the individual's identity, whereas „confirming " can be understood as verification, i.e. one-to-one process whereby an individual claims an identity and the system compares the captured biometric template with the stored template corresponding to the claimed identity. Read more at Alessandra Calvi and Simone Casiraghi, *Biometric Data in the EU (Reformed) Data Protection Framework and Border Management: A Step Forward or an Unsatisfactory Move?* in PERSONAL DATA PROTECTION AND LEGAL DEVELOPMENTS IN THE EUROPEAN UNION (Maria Tzanou (ed.), 2020); and Catherine Jasserand, *Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data,* 3(3) EUR. DATA PROTECTION L. REV. 297 (2016).

[50] Danny Ross, *Processing biometric data? Be careful, under the GDPR, 2017*, *available at*: https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/ (last visited: 11 Jun., 2021).

[51] *See Misbehaviour*, THE ENCYCLOPEDIA OF WORLD PROBLEMS & HUMAN POTENTIAL *available at*: http://encyclopedia.uia.org/en/problem/135126 (last visited: 11 Jun., 2021).

[52] Article 9(1) GDPR.

purpose of collection and use of the biometric data in question is important in determining whether the data in question is sensitive for the purposes of the GDPR. Where there is no intention to use them for purposes of identification, they do not constitute personal data.

Data concerning health

According to the GDPR, any information which reveals details about the health of a specific individual is classified as sensitive data. Recital 35 of the GDPR further elaborates on the notion as follows:

> *'Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject'.*

This open definition allows the inclusion of a potentially enormous amount of data, especially considering the shrinking computational distance between various forms of raw data and potential conclusions about individual health status.[53] This relates not only to data that reveals medical conditions or illnesses but also to probabilistic predictions (*e.g.* that an individual as a higher chance of developing conditions such as diabetes or cancer) and even information that reveals an individual is healthy.

This expansive nature of the concept was outlined in a letter by the WP29 to the European Commission, in 2015. The WP29 clarified the scope of the definition of health data in connection with lifestyle and well-being apps. According to the letter, personal data are health data (or data concerning health under the terminology of the GDPR), when:

1. *The data are inherently/clearly medical data*
2. *The data are raw sensor data that can be used in itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person*
3. *Conclusions are drawn about a person's health status or health risk (irrespective of whether these conclusions are accurate or inaccurate, legitimate or illegitimate, or otherwise adequate or inadequate).*[54]

---

[53] Computational distance can be understood as *the level of scientific, economic, and technological effort required, when combined with other (personal or non-personal) data, to infer sensitive data from apparently non-sensitive information*. *See,* Paul Quinn & Gianclaudio Malgieri, *The Concept of Sensitive Data – Fast becoming a Paper Tiger?*, in German L. J., forthcoming; Gianclaudio Malgieri, and Giovanni Comandé, *Sensitive-by-Distance: Quasi-Health Data in the Algorithmic Era* 26(3) INFO. & COMM. TECH. L. 229 (2017).

[54] *See Annex - Health data in apps and devices, available at*: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf (last visited: 11 Jun., 2021).

EEG data can fit into all of the categories of health data above. In health care, EEG data serves primarily as a support to establish a diagnosis.[55] Forming part of the patient's file and becoming part of his or her medical history, EEG data, has a clear medical nature. EEG data, as raw sensor data, is today the most common format used by neuroscientists and developers of EEG-based devices. As the criterion implies, EEG data is medical data, regardless whether it can be used for direct or only indirect identification, if it is possible to draw a conclusion based on it about the actual health status or health risk of a person. Considering the intrinsic sensitiveness and shrinking computational distance, as emphasised by Malgieri and Quinn,[56] this 'possibility' widens the scope of applicability of the special protective regime of the GDPR in connection with data concerning health as technology advances.

Of the three categories described above, the third category relates to probably the most complex, especially given the variable nature of EEG data as discussed in section II. Whilst some forms of EEG, collected in the health care setting, may be of a sufficient quality to deduce information concerning the health status of a patient, this may not be the case for other forms of EEG collection. EEG-based well-being devices, for example, collect and process less accurate data.[57] Such data may not only be processed with the help of analytics and/or artificial intelligence and may use forms of 'inferential analytics'. Inferential analytics entail the non-intuitive and unverifiable inferences and predictions about the behaviour, sensitive attributes, preferences, and private lives of individuals.[58] Whilst the accuracy of such analyses may often be questionable, they may, nonetheless, be sufficient to meet the definition of health data, which seemingly include inaccurate predictions about an individual's heath status. This flows from the reasoning of the WP29 which has stated that, '*[m]ore often than not, it is not the information collected in itself that is sensitive, but rather, the inferences that are drawn from it and the way in which those inferences are drawn, that could give cause for concern*'.[59] This is logical, in view of the fact that incorrect inferences and assertions about an individual's health status can also lead to negative results (e.g., missing real medical conditions or harms in terms of individual privacy).

---

[55] *Supra* note 4, St. Louis et. al.

[56] Paul Quinn & Gianclaudio Malgieri, *The Difficulty of Defining Sensitive Data–the Concept of Sensitive Data in the EU Data Protection Framework*, BRUSSELS PRIVACY HUB RES. PAPER (2020).

[57] The 'Muse S' technology is using only 7, dry arrays, placed only on the sides of the head, ignoring important biological factors such as the thickness of the skull or the skin.

[58] Sandra Wachter & Brent Mittelstadt, *A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI*, 2 COLOM. BUS. L. REV. 494 (2019).

[59] Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation, p. 47, WP203.

Given the broad nature of health data as defined within the GDPR, it is therefore likely that many forms of EEG data could be considered as forms of 'health data'. EEG data is often created in the contexts where analysis is being made about individual health status for a wide variety of reasons: ranging from health care to lighter forms of wellbeing. Thus, it is clear that many forms of EEG data will constitute sensitive data where it refers to identifiable individuals.

V

Representation of EEG Data as Personal Data & other Forms of Biological Data

EEG data demands contextual analysis

In section III, of the paper, we have demonstrated that the quality of EEG can vary enormously. It can range from the research and health care contexts where the equipment used may be of a high quality to various commercial and well-being contexts where the quality of the data may be on a much lower level. This is logical given that the need for accuracy and consistency in the former types of contexts is much more important. Even where data is of high quality, other factors may affect the possibility of identification, including the consistency of the method used. EEG data may need to be taken in circumstances where subjects are performing the same activity or trying to think about the same thing. Where this is not the case, comparing EEGs, even from the same person, may be like 'comparing apples and pears'. A further factor is the important dimension of time which, given the plastic nature of the human brain, can mean that whilst EEG in certain contexts may be able to be linked to certain individuals at a particular time, this may not be the case after further time has elapsed. All of these factors can play a role in determining whether EEG data is personal or not and indeed what type of sensitive data it may (or may not) be.

This 'grey' nature of EEG data can be compared with other forms of data that may be collected upon analysis of physiological characteristics and which have a more certain character in terms of their likelihood to be personal data. This contrast is most notable and illustrative with genetic data. This type of data is, , by its nature, qualitatively very different from EEG data. Most importantly, the genetic code of individuals is more or less constant throughout their lives. With the exception of issues relating to cancerous cells or epigenetic factors there is almost no variation from one moment to the next, even after many years. Furthermore, the quality of genetic data does not vary according to the technique used to assemble it. Whilst some modern methods may be faster than others, none produce data with results that may be considered unreliable (if they did they would essentially be useless).

Results are furthermore not influenced by what individuals are doing or how or where samples are taken from (*e.g.*, blood or saliva samples).[60] This is reflected in the way data protection frameworks are applied to the use of genetic data. It is commonly understood, for example, that any sizeable quantity of genetic data can never be considered anonymous, even in the absence of accompanying meta data(e.g., patient records). The life-long reliability of such data, together with the potential to identify data subjects through the use of potentially complementary data available elsewhere, means that to consider genetic data as ever being anonymous would be a fallacy.. This stands in stark contrast to EEG data which in many cases, at present, probably cannot be considered to be personal data where it exists alone(i.e., not accompanied by identifying meta data).

In legal terms, the consequences of this 'grey' nature of EEG are significant and can be grouped under two main categories. *First*, EEG need not always in isolation be considered personal data (as is commonly accepted is the case for genetic data, for instance). This means that it may be possible to collect, store and process EEG data without having to comply with data protection rules. It may be important in areas such as scientific or commercially motivated research where the need to gather informed consent or comply with other basic requirements of data protection could be onerous.[61] Importantly, the very nature of EEG data, as outlined above, entails that at least in certain contexts, research can be conducted on such data without the need for adherence to data protection law, unless of course it is processed alongside identifying meta data.

The *second* important implication, however, is that in order to know whether EEG data is or is not personal data, it is necessary to conduct an analysis that is highly contextual. General assumptions are not possible given that the quality of such data can vary enormously, as can the time, since the EEG data were created. It is necessary to consider all of these factors to determine whether such data could be considered personal. The need for such consideration negates, to a certain extent, the potential freedom that flows from the fact that many forms of EEG data may not be considered as personal data. This is because despite the likelihood that EEG data is anonymous in nature, it will often be necessary to carry out analysis to confirm whether this is the case. This will place a burden on those wishing to use EEG data, even where it turns out to be the case that such data is indeed anonymous.

---

[60] Paul Quinn and Liam Quinn, *Big genetic data and its big data protection challenges*, 34(5) COMPUTER L. & SECURITY REV., 1000 (2014).

[61] Paul Quinn, *The anonymisation of research data—a pyric victory for privacy that should not be pushed too hard by the EU Data Protection framework?* 24(4) EUR. J. OF HEALTH L., 347 (2017); Pam Carter, Graeme T Laurie and Mary Dixon-Woods, *The social licence for research: Why care data ran into trouble*, J. OF MED. ETHICS (2015), doi:10.1136/medethics-2014-102374; Michael Friedewald and Dara Hallinan, *Open consent, biobanking and data protection law: can open consent be 'informed' under the forthcoming data protection regulation?*, 11(1) LIFE SCI. AND SOC. POL'Y. 1 (2015).

The grey nature of EEG data also results into the conclusion that it will be recognised differently under the GDPR, according to the particular context involved. The protection the GDPR offers to individuals from whom the EEG data may originate may differ (or may not exist at all). As depicted in the table below, it ranges from forms of EEG data that are not recognised by the GDPR as being personal data (*i.e.*, that they are anonymous) to instances where EEG data could be recognised as a sensitive form of personal data, thus, enjoying an elevated level of protection.

Table 1: Protective regimes of EEG data under the GDPR

EEG data	*Category*	*Level of protection offered by the GDPR*
EEG data that is of an anonymous nature.	Not personal data	None
Any EEG data relating to an identified or identifiable natural person	Personal data	Baseline
Relates to (non-sensitive) behavioural characteristics of a natural person	Personal data	Baseline
Results *from a specific technical processing* relating to physical, physiological, or behavioural characteristics of a natural person, and which is capable to allow or confirm unique identification, for the purposes of uniquely identifying a natural person	Special category of data	Higher level
Processed for medical purposes	Data concerning health	Higher level
Raw sensor data that can be used in itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person	Data concerning health	Higher level
(Accurate or false) conclusion drawn about health status	Data concerning health	Higher level
Reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing data concerning a natural person's sex life or sexual orientation	Special category of data	Higher level

VI

Conclusion

EEG data is important in a number of domains. This includes health care, scientific research, and a variety of commercial contexts. The quality of the data involved can vary greatly from one context to another. The types of apparatus used in the healthcare or scientific research context for recording EEG data may, for example, be much more complex and accurate than those used in commercial or well-being applications. Similarly, the techniques used in different contexts may vary greatly. Such variation may be important in determining whether in a particular instance EEG data can be considered personal. Whilst in many instances, such as in the context of a patient's medical dossier, the answer to this question may be obvious. In other instances, it may not be(e.g., where research data is held in isolation for research purposes). This is because in certain contexts it may be possible to link EEG data to specific individuals whilst, in others, it may not be. Further factors that can influence the nature of EEG data (and the possibility that it could be inked to specific individuals), are the activities that individuals were involved in at the time of having an EEG taken and how much time has elapsed since the data was recorded. The first of these is important because EEG data is related to the activity the human brain is engaged in. That means, it will change according to what a person is doing or thinking about. The second variation arises because the human brain is to a certain extent 'plastic' in nature, changing over time and according to lived experiences. This factor means that even where EEG data may have been capable of constituting personal data at a certain point in the past this may no longer be the case with the passing of time.

This variation of EEG data and its innate 'grey' nature mean that the question of whether it can constitute personal data (i.e., alone in the absence of other identifying meta data) is complex and highly context dependent. This is unlikely in other forms of data driven from biological parameters such as genetic data. In many cases (and at present, in most instances) EEG data alone will likely not fall into the category of personal data. This is because it will not be possible to identify patients without further available identifying meta data. Whilst there is research to suggest that EEG data can be used in a fingerprint like manner to identify individuals, this has been under carefully controlled experimental conditions in which other factors where kept constant. Such conditions are not present in the majority of contexts that involve the storage and collection of personal data. In such conditions, where EEG data, to be processed in isolation (*e.g.,* for scientific or commercial research) and without additional meta data, may often be considered to be anonymous. There are increasing number of researches that demonstrate, however, the possibility for identification. This is becoming possible in view of more powerful computer processing and analytical software. This and the increasing availability of

potentially complementary data online, points towards the eminent possibility for identification of individuals from their EEGs will, rapidly increase in the immediate future. As a result, the possibility that such data constitutes personal data should be considered by those generating and using such data even where this is not obvious (*i.e.*, in the absence of directly accompanying meta data). If EEGs are personal data it is also necessary to consider whether or not they constitute sensitive forms of data, which, as we have discussed, means that they are likely to bring with them a higher regulatory burden.