International Working Group on
Data Protection in Technology (IWGDPT)

Working Paper on
"Emerging Neurotechnologies and data protection"

Published 15th May 2025[1]

Table of Contents

[1] This paper was discussed at the 73rd IWGDPT Meeting on 18th 19th June 2024 and adopted, after final discussion, at the 74th IWGDPT Meeting on 18th 19th November 2024. The written procedure followed after the latter meeting.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

1. Introduction

Traditionally, we have often associated privacy with a sense of physical boundaries, of space and distance and some degree of active control as to how we monitor and enforce this. Yet in recent years we have seen these distinctions and boundaries blurred as increasingly accessible means of gathering intrinsic and intimate data have emerged. We now see biometric technologies that claim to offer behavioural and emotional analysis through observation of physical responses; approaches that are deeply troubling in the potential for harms and risks that they raise.

Yet the emergence of neurotechnologies represent a ground breaking intersection between science, engineering and medicine beyond even this. Whilst their recent proliferation has been largely contained to the health and research sector, it's possible, but also feared, that they may soon become part of our daily lives in the years to come. Use may enter – and in some cases, already has entered – our workplaces and our homes, for example under the guise of providing more personalised services.

These technologies could conceivably be embedded in the next generation of our consumer devices and wearables such as earbuds, headphones and augmented reality headsets. If they were rolled out in consumer devices and became more cost-accessible, other use cases would be likely to emerge and we can anticipate their possible use in employment sectors from office-based roles to high-risk environments such as the use of heavy machinery.

While the accessibility of neurodata comes with positive uses, it also raises new ethical questions around human agency, human dignity and identity, augmentation and enhancement, beyond privacy and consent. After all, what could be more intimate than our very minds and potentially our thoughts and autonomy? Effective data protection and privacy standards, intertwined with the need to respect other fundamental rights, such as the right to mental integrity and human dignity, will be a critical aspect in preventing misuse of information that may lead to new forms of discrimination or reinforcing those that already exist, the undermining of

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

our ability to provide meaningful consent and possibly impacting fundamental notions of personhood and identity.

The very specific and sensitive nature of these data, which may not be by default, health or biometric data under regimes such as the GDPR, raises the question of, first of all 'if', and then how, they should be used and which specific safeguards should be put in place.

The data processing in the context of deployment of these technologies needs to be assessed having regard in particular to the data protection principle of necessity and proportionality.

The goal of this paper is to provide a global perspective on some of the most pressing data protection and privacy implications of the collection and processing of neurodata, by way of emerging neurotechnologies. It will explore questions relating to lawful basis and consent, the use of neurotechnologies on children, security and technical requirements for neurodata. We seek to set out initial concerns and considerations for first practical steps before building out to future questions and issues.

This paper sets out high level definitions of neurodata and neurotechnologies, as well as brief overviews of key terminology, data flows and current uses as well as an overview of the current regulatory context. Then, a combination of horizon scanning, expert engagement and desk-based research has been used to highlight critical issues and challenges. It then examines:

- The lawfulness of neurodata processing and the use of consent as a lawful basis for this processing, taking into account that some uses of neurotechnology should be considered as implying unacceptable risks in breach of fundamental rights and freedoms;
- The intersection of neuromodulation and data protection legislation;
- The use of children's neurodata and;
- Privacy and security concerns regarding neurodata.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Disclaimer

This paper has been written from a foresight perspective. In this context, it should be noted that just because something is technologically possible does not mean that it has to be done, nor that it is ethically acceptable and/or lawful. We briefly explore some plausible use cases in this paper, some of which would first require a human rights assessment to decide whether such data processing could be allowed in any context (under any legal regime), if it implies unacceptable risks, since in breach of fundamental rights and freedoms, including the right to mental integrity.

Indeed, the possible use of neurotechnologies beyond the medical and scientific research sectors raises crucial concerns from a human rights perspective that lie beyond the immediate scope of this paper. The data processing in the context of deployment of these technologies needs to be assessed having regard in particular to the data protection principle of necessity and proportionality, taking into account all fundamental rights at stake (notably, human dignity, mental integrity, freedom of thought, non-discrimination, presumption of innocence, etc.).

In this context, and as mentioned further on in the paper, there is ongoing work in international institutions, such as the Council of Europe, OECD, the Global Privacy Assembly etc., but also in the context of the regulation of artificial intelligence (in the EU with the AI Act[2], and worldwide) to interpret and clarify the human rights framework could contribute to this process.

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), OJ L, 2024/1689, 12.7.2024, available at https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

2. Defining Neurodata and Neurotechnologies

Drawing upon the definitions set out in the ICO tech futures: neurotechnology report[3] (and in turn UNESCO and OECD definitions) we consider neurodata as:

"*first order data gathered directly from a person's neural systems (inclusive of both the brain and the nervous systems) and second order inferences based directly upon this data*".

This helps us to define the scope for this paper. We will consider information drawn from both the brain and the neural system, as well as morphological data (data allowing identification as well as classification) but exclude neurodata inferred via biometric technologies and their data. We then define neurotechnology as:

"*devices and procedures, both invasive and non-invasive, that directly record and process neurodata with the aim of gathering data, controlling interfaces or devices, or modulating neural activity*".

This definition does not directly include approaches that 'emulate' neural activity at this time. This is due to the significant overlap with algorithmic processing that mirrors neural activity without being directly drawn from the source. However, if appropriate, we will consider this in specific circumstances, such as smart prosthetics linked to AI processing.

What this paper does not consider is broader sources of **biometric or biological data**.[4] In other works, forms of personal data that are derived from parts of the body that are not the brain or the nervous systems. While biometric technologies are available that claim to gather data for behavioural or emotional analysis, this may be considered third order neurodata for the purposes of this paper; data drawn from biological responses to neural activity. This paper focuses on first and second order

[3] ico-tech-futures-neurotechnology-0-1.pdf
[4] For an examination of the intersection of biometric data and neurodata see Beyond neural data: Cognitive biometrics and mental privacy (cell.com)

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

neurodata; information derived directly from the brain and nervous systems and inferences made from this data.

While neurodata and biometric data are closely linked in terms of their intrinsic and intimate nature, the focus on neurodata has been chosen in order to limit the scope of the paper and to highlight issues specific to these technologies.

There are a wide variety of technologies and techniques that allow the gathering and analysis of neurodata. However, a comprehensive survey of these is not required here. What is important is to consider the aspects of neurotechnologies that are particularly relevant to data protection and privacy concerns. The ICO[5] identified the following aspects:

- **Implantable neurotechnologies** are surgically implanted to directly contact the brain and to date, provide the most accurate and detailed data on a person's brain patterns at the risk of invasive surgery, and long-term scarring possibly that may reduce device effectiveness. Continued access to laboratory conditions is also required, further limiting the uses of devices on the near horizon.

- **'Semi-invasive' neurotechnologies** focus upon epidural or subdural placement near the cortex reducing, although not eliminating surgical risks as surgery to open the skull is still required. An example of an exception to this is Synchron's stentrode[6] which is threaded through the jugular vein to the brain. The area of minimally invasive technology is one of dynamic growth and will likely see many new developments in the intermediate future.

- **'Non-invasive' (wearable) neurotechnologies** are placed on / outside the body, such as through a patch or headband device. They offer the opportunity to gather both non-medical and medical data across a variety of sectors with often less risk associated with surgery

[5] Neurotechnologies: Key definitions | ICO
[6] The Technology | Synchron

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

through the skull or spine and relatively lower costs in terms of equipment.

The distinction between implanted and wearable devices is an important one, both technically and medically. However, it is also important to note that 'non-invasive' devices can still interact in quite intimate ways with the brain. Another way to distinguish between devices is through their capabilities to record and analyse neurodata received and those that stimulate or modulate neuropatterns. Essentially, both invasive and non-invasive technologies can be considered under the following divisions:

- **Read devices** such as a medical functional magnetic resonance image (fMRI) scanner, designed to image the brain activation patterns or electroencephalogram device (EEG) which can detect electrical activity of the brain.

- **Read-write devices** such as headsets designed to assist with mental health or wellbeing. The write aspect of these devices can be further broken down onto two aspects; neuromodulation and neurostimulation. Neuromodulation relates to processes seeking longer-term change in brain activity, such as with the treatment of a neurodegenerative condition. Neurostimulation seeks to provide a shorter-term effect.

There are also a variety of ways to further differentiate neurotechnologies that may influence the way data can be processed and the level of involvement given to a person using a particular device. These include:

- **Active devices** act upon a deliberate task or stimulus such as finger movement, mental arithmetic or music imagery to generate a neural response.

- **Reactive devices** act upon an external cue such as music, imagery, pain or even a question in order to record a specific response.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

- **Passive devices** record subconscious, unprompted and more generalised responses from a person such as fatigue levels, attention span or arousal.

Synchronous and asynchronous devices are another point of differentiation; with synchronous devices reading on a predefined schedule and asynchronous devices allowing the users of a neurodevice to interact and communicate with the system. Linked to this definition are **closed loop** and **open loop** systems.

- **Closed loop neurotechnologies** operate on an autonomous basis, reacting or inputting on the strength of their programming and algorithmic processing.

- **Open loop systems** are 'open' in the sense that the people wearing or implanted with the device can choose when to make an intervention of action via a device.

Contemporary uses and data flows

As has been set out above, while neurotechnologies can differ widely in how they're deployed and in how they can process data, there are sufficient similarities to make a high level overview of the data flows valuable:

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

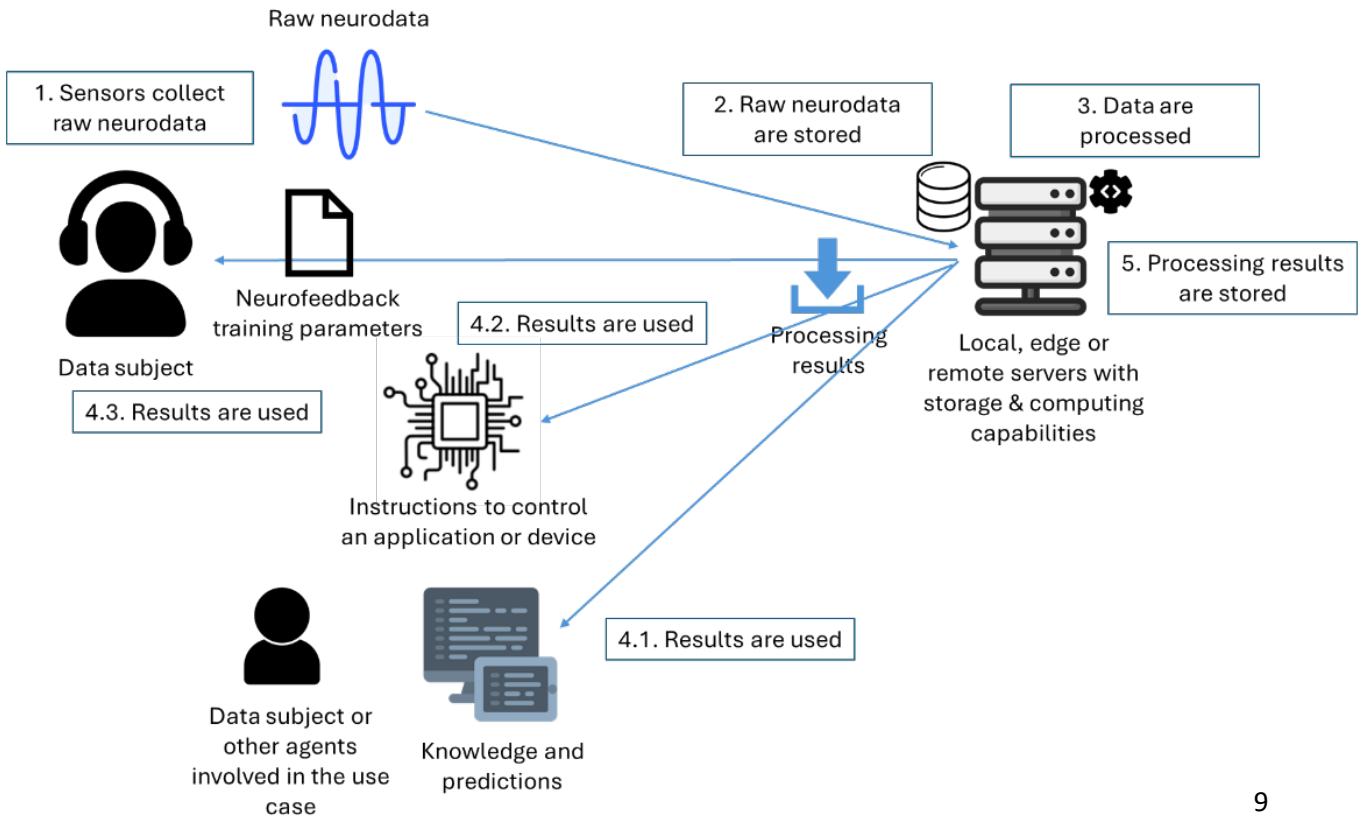

Image courtesy of EDPS/AEPD report[7]

The medical applications for neurotechnologies can be traced back to early neuroprosthetics such as cochlear implants. Yet contemporary, if not cutting edge, medical treatments can now include neural bridges designed to restore mobility to those that have experienced spinal trauma[8] and predictive brain-to-speech technologies for non-vocal patients[9].

Beyond the medical however, cutting edge deployments of neurotechnology have also included:

[7] TechDispatch #1/2024 - Neurodata | European Data Protection Supervisor (europa.eu)
[8] A review of disability EEG based wheelchair control system: Coherent taxonomy, open challenges and recommendations - PubMed (nih.gov)
[9] Scientists translate brain signals into speech sounds | National Institutes of Health (NIH)

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

- classroom monitoring and pupil development in China[10];
- military applications such as the remote use of drone swarms[11];
- neuro controls for games[12]; and
- productivity tracking in corporate workspaces[13].

However, while already deployed across various regions, there is a high potential that the non-medical examples provided above would not be in compliance with fundamental rights, since they may entail questionable exploitation of neurodata and subsequent inferences[14].

3. Legal context

While data protection regimes such as the GDPR do not explicitly define neurodata as a particular category of personal data or special category personal data, Article 4 of the GDPR does set out that 'mental identity' is a core aspect of personal data. No explicit definitions are provided under the GDPR with regards to the limits or boundaries of what may constitute mental identity taking into account other complex and culturally embedded philosophical contexts.

However, Article 3 of the European Charter of Fundamental Rights (the Charter) sets out 'the right to respect for his or her physical and mental integrity'[15].

[10] China Has a Controversial Plan for Brain-Computer Interfaces | WIRED
[11] Design of an EEG-based Drone Swarm Control System using Endogenous BCI Paradigms — Korea University
[12] Mind-Controlled VR Game Really Works | MIT Technology Review and EEG-based BCI and video games: a progress report | Virtual Reality (springer.com)
[13] Neurotech at Work (hbr.org)
[14] TechDispatch #1/2024 - Neurodata | European Data Protection Supervisor (europa.eu): "The use of artificial intelligence ('AI') systems may also make technically possible exploitation of neurodata for purposes such as law enforcement, screening of migrants and asylum seekers, as well as by private entities for instance for **workplace or commercial surveillance**. In this context, it is important to underline that that certain uses of neurodata pose unacceptable risks to fundamental rights and are likely unlawful under EU law."
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The UNESCO International Bioethics Committee argues in its Report on Ethical Issues of Neurotechnology that explicit consent will always be required to write neurodata. However, as discussed later in this document, consent as a basis for the processing of neurodata (rather than for associated medical procedures) may prove to be complex at the best of times and inappropriate at others. Moreover, it is important to stress that data processing that is in breach of human dignity (notably, due to its invasiveness, and/or to possible inferences and profiling of the persons concerned) or of applicable laws (for instance, sectorial laws specifying which types of data can, or cannot, be processed) cannot be considered lawful, regardless of the explicit consent of the data subject.

Further approaches to neurodata governance and rights emerged in 2018 when proposals were made to amend the Brazilian General Personal Data Protection (GPDP) law, which is already based upon a right to free development of personality, and to include neurodata specific sections in Spain's Digital Rights Charter. In 2019, the OECD issued a Recommendation on Responsible Use of Neurotechnology.[16] It offers a beginning to what many in the industry seek; an international standard for research, innovation and deployment in and around neurotechnologies. Key recommendations are phrased as broad principles highlighting priorities for inclusivity, responsible innovation, building trust and safeguarding data.

The first explicit piece of legislation directly regarding neurodata passed in the amendment to Article 19 of the Chilean Constitution. Following consultation with international experts, the explicit right to neuroprotection was signed into law, preceding the development of a neuroprotection bill. This bill sets out five essential rights discussed briefly below[17] including the right to personal integrity, free will, mental privacy and fair and equal access to technologies that can enhance or alter neurological states. It should be noted that the bill specifically refers solely to medical uses of neurotechnology. Uses are forbidden in situations where vulnerable communities are placed at risk or when a person's behaviour may be altered without explicit consent.

[16] Emerging technologies | OECD
[17] Mind the Gap: Lessons Learned from Neurorights | Science & Diplomacy (sciencediplomacy.org)

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The reception of the bill has been varied. Some groups have welcomed both the legislation and the constitutional reform, while others have argued that the new law undermines existing rights and opportunities for those it seeks to protect and could inhibit innovative research into neurological conditions.

In the US, two new laws regulating "neural data" passed in Colorado[18] and California[19], each clarifying that "neural data" is "sensitive data" under the states' underlying consumer privacy laws. This is a different approach than that being taken in other countries to create new "neurorights," instead expanding existing privacy law to cover a new category of data (neural data).

Another parallel area of legislation that may come to have a significant impact on the development and deployment of neurotechnologies is the EU's AI Act. Requiring that algorithmic processing be evaluated on a risk-based approach, Article 5(1)(a) of the AI Act states that the following AI practice shall be banned:

'the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm'.

[18] Protect Privacy of Biological Data | Colorado General Assembly
[19] Bill Text - SB-1223 Consumer privacy: sensitive personal information: neural data.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

4. Neurorights

There are also increasing calls for the consideration of specific (and fundamental) **neurorights**[20]. The Neurorights Foundation in particular has sought to advocate for the following five rights to be created, some of which raise some specific connections to existing rights and obligations under existing data protection laws:

- The right to **mental privacy**. The generation and processing of neurodata relates to both conscious and subconscious patterns, beliefs and responses. This potentially includes information that we are either unaware of or may never chose to voluntarily disclose. Given that data is gathered directly from neural patterns, this choice is removed; presenting two critical issues. Firstly, highly sensitive information may be unwillingly and reflexively revealed. Secondly, inaccurate data may be revealed leading to complexities around rights of correction as well as social, societal and psychological impacts arising from a 'slip of the mind'. While the reading of semantic data[21] (such as a specific memory response to a scent for instance) is not yet possible, the accuracy of implanted technologies can already provide significant insight.[22]

- The right to **mental integrity** (also defined as the right to **psychological continuity**). While at an early stage of development, neurotechnologies are currently able to modulate neural patterns and affect processes such as concentration and multi-tasking. Longer-term development may lead to the ability to impact mental states in an increasingly precise and focused manner. Laboratory tests have already demonstrated the ability to implant hallucinations within the brains of mice, eliciting responses to these images.[23]

[20] https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU(2024)757807_EN.pdf provides an overview of the most recent publications in this area.
[21] A complex or abstract response or emotional state triggered by a specific stimulus.
[22] 1680a429f3 (coe.int)
[23] Hallucinations implanted in mouse brains using light (nature.com)

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

- The right to freedom from **neurodiscrimination**, which occurs when systemic bias arises from the use of algorithms to analyse neurodata or from future research. This may identify particular patterns of thinking, mental health states or behaviour that could further generate means to discriminate against neurodivergent people. Discrimination of neurodivergent persons (as 'ableism'[24]) can also be the outcome of a technologically possible, although unethical and most likely unlawful, use of neurodata at the workplace or in the context of recruitment.

- The right to **fair access to neuroaugmentation** for all. While raising significant ethical and legal issues, this right does not fundamentally pertain to privacy and personal data at this level.

- The right to **cognitive liberty** (literal freedom of thought rather than the manifestation of thought as currently expressed by European and UN human rights legislation).

The intersection of human rights and mental rights continues to be debated across the neurotechnology community. There appears to be an emerging call by some for an approach based upon the need for a clearly defined and wide-ranging piece of legislation to formally establish the above. This is driven by the argument that neurodata is key to a sense of self and that the integrity and privacy of neuroprocesses should be fundamentally maintained. Others argue that while the issues raised are critical, further risks are posed by 'rights inflation'; excessive legislation that ignores the existing powers already available to regulatory and legislative regimes.[25]

[24] **Ableism** is discrimination and social prejudice against people with physical or mental disabilities. Ableism characterizes people as they are defined by their disabilities and it also classifies disabled people as people who are inferior to non-disabled people. On this basis, people are assigned or denied certain perceived abilities, skills, or character orientations. Although ableism and disablism are both terms which describe disability discrimination, the emphasis for each of these terms is slightly different. Ableism is discrimination in favour of non-disabled people,

[25] "Neurotechnologies and Human Rights: Do we need new rights? " The report of the Council of Europe and OECD round table is published - Human Rights and Biomedicine (coe.int)

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Council of Europe and UNESCO's international bioethics committee independently concluded that instead of novel human rights, existing human rights law and regulations to neurotechnology should be tailored to specific contexts. The EPRS also noted that the debate:
"*should be reframed to meet interests and rights of European citizens, reach the expectations of democratic European states and underlying European values*"[26].

In August 2024, the Council of Europe also released its report on neurotechnology and its place within convention 108+ offering further context and policy options[27]. In the EU, in addition to privacy and data protection (Article 7 and 8 of the Charter of Fundamental Rights of the EU), fundamental rights such as human dignity (Article 1 of the Charter) and physical and mental integrity (Article 3 of the Charter) as well as freedom of thought (Article 10 of the Charter) provide a 'defence' against certain uses of neurodata that would jeopardise these rights.

5. Lawfulness of neurodata processing

Once its purpose has been specified, and provided that the processing of neurodata is compliant with fundamental rights, and in particular with the principle of necessity and proportionality of any interference with the fundamental right to privacy and to the protection of personal data, neurodata processing can be lawful[28] only if and to the extent that, among other conditions, the appropriate legal basis is relied upon by the controller. These legal basis include: the processing is necessary for the performance of a contract, it is necessary for compliance with a legal obligation, it is necessary in order to protect the vital interests of the data subject or of another natural person, it is necessary for the performance of a task carried out in the public interest or it is necessary for the purposes of the legitimate

[26] https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU(2024)757807_EN.pdf
[27] 1680b12eaa (coe.int)
[28] Note that the grounds for lawful processing may vary by jurisdiction.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

interests pursued by the controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject). Processing can also be done which is necessary for the protection of Lawful Rights and Interests; Establishment, Exercise, or Defence of Legal Claims.[29] Finally, if the data subject has given fully informed consent to the processing of their neurodata for the specified purposes.

In the light of the high risk for the rights and freedoms of the person concerned, such processing should in principle only occur for certain well-specified use-cases, for instance for health or scientific research purposes, always with appropriate safeguards in place and of course, subject to all other data protection conditions and limits including purpose limitation[30].

There are several serious concerns regarding consent as a basis for processing neurodata, yet this is an approach that many developers are considering for neurodata processing in different contexts. Power imbalance, data scoping, and issues around data subject capacity to give consent are all serious barriers to obtaining valid consent.[31]

Due to these concerns and the highly sensitive[32] nature of data processed by neurotechnologies, we now examine why consent is so challenging for

[29] For example, see NPC-Advisory-No.-2024-02-Personal-Data-Processing-Based-on-Section-13-f.pdf in the Republic of the Philippines.

[30] See EDPS-AEPD Techdispatch, TechDispatch #1/2024 - Neurodata, at page 16: "It would be alarming for any controller, other than a provider of healthcare, to use neurodata to detect or infer an individual's health information (in particular very sensitive information that is possibly not yet known to that individual themselves, e.g. about psychological disorders or a neurogenerative disease).", available at https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata_en

[31] See, e.g., "ICO tech futures: neurotechnology," ICO Report, "Regulatory Issues" Issue 3 (accessed May 12, 2024), https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ico-tech-futures-neurotechnology/.

[32] We note that there are many different legal standards globally for considering neurodata a special category that would require additional legal protections that may affect consent, which some neurotechnology cases may avoid. However, we believe for the purposes of this discussion that it is fair to refer to neurodata as "sensitive" in that it must always be very cautiously handled, processed, and protected due to its combination of involuntary generation, opportunity for highly personal and revealing inferences, and connection to biodata since it is read from signals in the brain and nervous system.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

neurodata processing and whether circumstances exist that would allow consent to be considered an appropriate lawful basis for this processing. It is worth clarifying that we are referring to consent for the processing of personal data and not to medical consent or other types of informed consent.[33]

Focus: Challenges to consent

The complexity of both neurotechnology and the data it processes creates intrinsic challenges to consent as a legal basis for processing. As set out under the GDPR and other regulatory frameworks, valid consent must be freely given, informed, specific, and unambiguous.[34] For ease of structure, we will look at the challenges specific to each element of consent.

Freely given: Consent must be voluntary, without coercion or negative consequences derived from refusal. Consent may only be freely given in circumstances where there is no power imbalance at play. While there are many considerations to keep in mind when assessing whether consent has actually been "freely given," there are some circumstances in which "freely given" consent is near impossible. This, in addition to concerns on the necessity and proportionality of the interference of the data processing with the fundamental rights and freedoms of the person concerned, will largely rule out consent-based neurodata processing in scenarios such as employment, education, the military, or justice, to mention only some significant examples.

First, certain settings contain power dynamics that come into play for the individual when they are asked to give consent. Employment is an especially challenging area because the power imbalance between employee and employer means that consent would likely not be valid under regimes such as the GDPR. Individuals who may not be comfortable with

[33] In some data protection regimes, consent to a medical procedure may be read as implied consent to processing of personal data, but in others, such as GDPR, another legal basis for processing is likely to be required.
[34] These factors of valid consent come from the GDPR but are echoed in many other regulations worldwide.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

using neurotechnology (and especially may be uncomfortable with their employer having access to their neurodata) will likely feel that refusing to give consent will lead to repercussions at work. Likewise, use of neurotechnology in education may leave students feeling they are unable to withhold consent without facing grading penalties (in cases of adult students – there are far more issues around consent when the students are minors). In both of these examples, the consent cannot be considered freely given if it may have been given only to avoid negative repercussions. The same occurs when the individual is forced to consent in order to use a product or service, as an essential requirement for access. This power imbalance further adds to concerns on necessity and proportionality and on the impact of the data processing on human dignity, mental privacy, freedom of thought and non-discrimination.

It must be emphasized that, depending on the context, the use of neurodata and neurotechnologies might be subject to broader legal provisions stemming from sectoral laws. For instance, in a working environment, it is very likely the use of such technologies might entail a preliminary check on risks related to potential remote control of workers. This is often strictly regulated and admitted only under specific and well framed circumstances.[35]

Second, medical use cases have been proposed to help address some mental health or behavioural issues. In those cases, there may be serious barriers to consent based on capacity (as in cases of severe mental illness where the data subject may not be of sound mind such that they are capable of giving consent)[36] or circumstance. Other examples would remain fundamentally unacceptable, such as the use of neurotechnologies on prisoners that demonstrate aggression where the data subject may be coerced into consenting by being told it may reduce a sentence or allow them certain privileges).[37]

[35] For example, in Italy, remote control of workers is allowed only for issues relate to the safety of working environment or the protection of a property, and if this is done in collaboration with workers organizations
[36] *See, e.g.*, Zuk, P., Torgerson, L., Sierra-Mercado, D., & Lázaro-Muñoz, G. (2018). Neuroethics of Neuromodulation: An Update. *Current opinion in biomedical engineering*, *8*, 45–50. https://doi.org/10.1016/j.cobme.2018.10.003.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Informed: Data subjects must be fully informed about the purpose, duration, risks, and benefits of neurodata processing. They should understand how their data will be used, and inappropriate expectations should be avoided. But it is exceptionally difficult for data subjects to be fully informed when it comes to neurotechnology and neurodata processing.

The technology itself is incredibly complex and individuals without high technical expertise are unlikely to fully grasp the nature of the technology or data flowing through it. In addition, experts in the field of neurotechnology are still determining what can be gleaned or inferred, meaning researchers, doctors, or companies behind the neurotechnology may also not be capable of fully disclosing the range of data that may be collected or drawn from the information. When scope and possibilities are unknown even to experts, how can we expect data subjects to be fully informed of these matters?

To obtain an informed consent, data controllers must explain the neurodata processing in such a way as to make it understandable to the data subjects, including the scope of data that may be collected, what can be gleaned from that data, risks present in neurodata processing, and a basic description of how the technology works as well as technical risks.

Data controllers should be cautious of information fatigue and avoid the use of excessively technical or specialized language. The question is: is there a real chance to provide concise, transparent, intelligible and easily accessible information about what data is collected, how it is processed, and all the risks and benefits in such a context? And how can we be sure that average data subjects truly understand the information provided to them about data processing? It can be difficult to figure out the best way to provide all the necessary information to data subjects.

To address this challenge, it is recommended to perform user testing to receive feedback on the accessibility, understandability, and ease of use of the proposed transparency approach. Because this technology is so complex and still evolving, one way to ensure that data subjects actually

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

understand the technology would be to have them describe their understanding to an evaluator (this may not be possible in all settings but should be in many medical and therapeutic settings) or answer some questions about the technology digitally to demonstrate understanding where this form of assessing data subject understanding would be more appropriate.

It is also important to document this approach to fulfil accountability obligations, showing how the selected approach effectively conveys the information for this specific processing.

Specific: The specificity of consent refers both to the specific data being processed and the specific purpose it may be processed for. The specificity of data is particularly difficult due to the nature of neurodata. Neurodata is involuntarily and subconsciously created by data subjects. Individuals may not be able to control what elements of neurodata will be picked up by neurotechnology. Crucially, data subjects may often be unaware of the volume and nuances of their neurodata. For example, let's say a data subject is using neurotechnology for gaming. They may believe they are just consenting to collection of neurodata related to the desired movements of the game, reaction time, etc. In reality, the neurodata may contain broad brain patterns and responses that derive from many other areas (focus, mental illness, emotional state, the physical health of the brain, etc.), as well as inferences that can be drawn from neurodata to reveal much more sensitive and personal information. This indicates the crucial importance of data minimization and **data protection by design and by default**, consisting in this case in the collection of only data strictly necessary (without inferring data on health state or mental illness of the 'player' in the context of gaming), to be deleted as soon as no longer necessary. The aim is to protect data subjects, notably **children/teenagers**, from a possibly new and harmful typology of **commercial surveillance** (based on the exploitation of neurodata) in the context of 'gaming'. Such 'gaming experience', for instance if accompanied by emotion recognition via neurodata, can also become harmful to the players due to induced **addiction**.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

This leads us to the scenarios where specific purposes are not clearly delineated in consent. In the example above, consent may have been given to process neurodata for game mechanics or to assist the data subject in "improving performance." However, a term like "improving performance" could be much broader than the data subject believes. For example, would tracking long-term patterns improve performance? Information extrapolated from the neurodata may be much more revealing and sensitive than a user would believe when they merely intended to allow the game to function. Therefore, this information should not be extrapolated from the 'player'.[38]

It is incredibly difficult to be specific about the scope and nuances of neurodata since our understanding of what is and can be revealed in it is constantly evolving. However, this very ambiguity must be described to data subjects to ensure they understand the scope of what they may be revealing with their consent. This can be partially addressed by mandating that neurodata controllers be extremely specific about what exactly they will seek to glean from the neurodata, exactly how that data will be used and who it will be shared with, and strictly limit themselves to solely the processing activities clearly described and agreed upon within the consent.

Given the very high risks for the rights and freedoms of the data subject, neurodata should only be collected for the functioning of the device (device functionality) and be deleted as soon as no longer needed for such functionality in strict compliance with the principle of data protection by design and by default.[39]

[38] See Reality Check: How to Protect Human Rights in the 3D Immersive Web, by Mariana Olaizola Rosenblat https://bhr.stern.nyu.edu/publication/reality-check-how-to-protect-human-rights-in-the-3d-immersive-web/ The Report, at page 20, recommends "Commit to a moratorium on the use of body-based data for psychographic profiling. Hardware and software platforms should make a commitment to erase all body-tracking data— including inferential or "abstracted" data derived from eye, face, and limb movements—once it is no longer needed for device functionality. The risks of storing such data greatly outweigh any commercial or other justifications for its use. Erasing body-based data will help prevent the creation of predictive behavioral models, which require aggregation and analysis of data over time."

[39] See EDPS AEPD Techdispatch, **TechDispatch #1/2024 - Neurodata,** at page 16, on conditions and limits for the processing of data such as 'brain fingerprinting'

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Unambiguous: Data subjects must make a statement or engage in a clear affirmative action to provide consent. This means that consent must always be given actively and cannot be assumed or implied. It must be clear that the data subject has given their consent to the specific processing that is taking place. The requirement for consent to be unambiguous is the only element that does not seem to have a neurotechnology-specific challenge. Individuals consenting to processing of their neurodata can and should take documented, affirmative action to show consent. Whether the other criteria can be met remains a problem.

If every one of these criteria would be met, consent as a basis for processing neurodata in those specific circumstances would be valid, provided that in those circumstances human rights are still complied with.

However, in any case, all elements of consent would need to be clearly documented and there should be regular checks or audits performed to ensure that the necessary conditions are consistently met. Particularly in confirming that neurodata controllers are going no further than was specifically consented to in their processing activities, i.e. the data minimization and purpose limitation principles are respected.

Additionally, it must be considered that neurodata will often be especially sensitive data whose processing involves a very high risk to the point of being prohibited by default. For example, under the GDPR neurodata may fall into the special category of personal data related to an individual's health ("*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*") or even biometric data ("*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*"). However, this may not always be the case; since neurodata may be of very different nature. Different application domains and use cases will require different granularity, accuracy, collection frequency, linkage with other contextual information, etc.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

When the processed data are considered especially sensitive, or special categories of personal data under regimes such as the GDPR (data concerning health or biometric data), the legal basis for such processing must be established, but also a condition to lift the prohibition of processing. This condition may be that the data subject has given explicit (as in a reinforced, clear and specific affirmative agreement) consent to the processing of those personal data or that the processing is necessary to protect the vital interests of the data subject (when the data subject is physically or legally incapable of giving consent). It may alternatively be that the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when proportionality, respect to the essence of the right to data protection and measures to safeguard the fundamental rights are provided.

Concerning this explicit consent, two best practices can be recommended:

- A two-stage verification of consent that provides the information progressively and redundantly in the most critical aspects, with explanations that follow different approaches or strategies to be sure that the data subject understands what exactly they are agreeing with.
- Automated revocation of consent at appropriate time intervals. This forces the implementation of consent refreshments, guaranteeing the data subject remains well informed about the processing and still agrees with it.

6. Neuro-stimulation/modulation's relevance to data protection and the regulation of privacy

Neurostimulation and neuromodulation (collectively called neurofeedback) have a wide array of potential applications, ranging from treating neurological disorders to enhancing cognitive abilities. At a basic level, neurostimulation provides a short-term alteration of brain patterns, while neuromodulation provides a longer-term alteration. Although

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

neurofeedback has shown promising results, more research is needed to understand the underlying neural mechanisms, determine the effects of prolonged treatment, and evaluate long-term outcomes. As these technologies carry potential risks, regulatory bodies and different authorities must ensure that only safe and effective devices are marketed and comply with medical device regulations.

Neurostimulation and neuromodulation involve collecting, recording, storing, and analysing neurodata, at least, because these are very personalised processes that only work if the brain's structure, function, or activity is properly known. But they may also involve structuring, altering, or writing neurodata in the feedback part of the processing, modifying brain waves by the obtained knowledge.

Neurodata is personal data, and processing means any operation performed on personal data, whether by automated means, that modification of neurodata related to a specific individual will fall under the applicable data protection law. Therefore, data protection regulatory frameworks must be complied with, as in the rest of the cases in which personal data is processed, regardless of the type of performed operation, which can be reading (generating knowledge) or modifying data to generate or control brain waves.

Neurodata processing lawfulness has been already discussed in the previous section. Examples of claimed legal bases for specific neurodata processing for neurofeedback could include:

- Vital interest: In cases where neurofeedback is crucial for an individual's health (the data subject or a different person), for example.
- Contractual necessity: If neurofeedback is part of a contract, for example, for psychological therapy.[40]

[40] For example, see the services offered by Mindlift in which consent and contractual necessity may both be employed: https://www.myndlift.com/post/quarterback-netflix-what-is-kirk-cousins-using-to-train-his-brain-and-how-neurofeedback-helps

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

- Legal obligation: Compliance with legal obligations, for example, in the case of medical record-keeping.
- Legitimate interest: This could be the case, for example, of certain types of scientific research projects.

Yet many current use cases rely on consent as the legal basis for processing neurodata. As it has been already discussed, obtaining valid consent for the processing of personal data requires meeting specific criteria which can be challenging in the case of neurodata processing. Even more when it involves neurofeedback, given the writing operations performed on the brain.

Let us examine again some of the criteria for valid consent focusing on the specifics of neurostimulation and neuromodulation:

Freely given: This may be a challenge given the purpose of some neurofeedback processing activities derived from write capable devices, such as neurostimulation or neuromodulation, which results in cognitive enhancement or even pain management and psychiatric treatment. First, power imbalance should be identified as a significant threat to free consent in some specific application domains. In this sense, consent may not be a reliable basis for processing when the controller is a public authority (in the healthcare or education domains, for example) due to the power imbalance that often exists between the controller and the data subject; the data subject may have no viable alternatives to accepting the terms of processing set by the controller.

Second, the nature of neurofeedback makes it very difficult to establish that the technology itself does not influence consent. Where a data subject has already participated in neurostimulation or neuromodulation, the technology may have been used to make the data subject more accepting, persuadable, or otherwise manipulated into giving consent when they would not have otherwise. Therefore, consent from anyone who has undergone neurostimulation or neuromodulation must be assessed with extreme caution to ensure this processing has not affected the data subject's inclination to give continued consent.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Informed: This may be a significant challenge given the existing uncertainties concerning neurofeedback and its impacts in the short, medium and long term, which in addition can be very specific for each data subject and their context or circumstances.

Specific: Again, this may be a challenge given the current uncertainties concerning neurofeedback. Specific and clearly differentiated information must be provided for operations that read data from the brain and those that write to it. Although they are part of the same processing, which has a single purpose, the implications, risks or degrees of personalization or reversibility are completely different, and this must be clear to the data subject when giving consent.

In summary, obtaining valid consent in neurofeedback scenarios may be especially complicated. This is even more true in specific scenarios. For example, in the case of people with disability, patients with mental illnesses or brain disorders. It is even possible to consider cases in which the implantation of invasive neurological devices can modify the personality of the data subject and therefore, their priorities or decision-making mechanisms. Even in an extreme case, is the person who consents to the processing of personal data before significant levels neurostimulation or neuromodulation the same as after processing? This is unlikely to be a binary situation, but at what point might a regulator consider a person's mental identity to have been modified beyond the limits of consent? Is the consent provided when the data subject was, in some respects another person, still valid?

The requirement of fairness under the different regulatory frameworks demand to always consider the reasonable expectations of data subjects, the effect that the processing performed for neurofeedback may have on them and their ability to exercise their rights in relation to that processing. For example, the data subject should have the right to withdraw their consent at any time. In these cases where consent is withdrawn, the effects of neurostimulation or modulation may continue to occur afterwards. That is, it must be clear to the data subject that the withdrawal of consent does

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

not imply the revocation of the alterations that may have occurred in their brain.

Concerning the transparency principle, due to the high risks involved in processing neurodata for neurostimulation and neuromodulation, it is essential to deploy additional transparency mechanisms and best practices. The data processing scope and consequences should be known and understood beforehand. Data subjects should not only have access to the strictly necessary information required under regulatory frameworks, but also to explanations in clear language about the most significant potential outcomes of the processing. In other words, what kind of impact may the specific data processing described have on a data subject? This explanation should not merely contain harmless and predictable "best-case" examples of data processing. Instead, it should present an overview of the types of processing that could have the most substantial impact on the fundamental rights and freedoms of data subjects. This information should be provided without prejudice (in addition to) the transparency and information obligation for the controller pursuant to data protection laws.

In this sense, it is essential to conduct thorough assessments of the impact of the processing of personal data on the rights and freedoms of the data subject (as fundamental rights' impact assessment, in addition to a data protection impact assessment pursuant to data protection law) before deploying data processing for neurostimulation and neuromodulation, regardless of the type of data or the legal basis that applies. The publication of these assessments, or at least of some parts, may foster trust in the processing and help achieve the required transparency levels.

The reliability of the inferences based on neurodata for both read only and read-write devices is also a subject of debate and scrutiny. There are concerns about how neurodata are collected, assessed, interpreted or written back to the brain. Two of these concerns are related to using devices and interfaces that incorporate very innovative technologies that are not sufficiently tested outside lab environments and relying on inadequate or incorrect statistical methods and models (not mature enough or including some kind of bias, for example).

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

A lack of accuracy in the processing of neurodata implies an infringement of the accuracy principle. But in the case of neurostimulation or neuromodulation inaccuracy of the data processing may affect the rights and freedoms of the data subject in many different and critical ways, starting with their right to integrity. The irrevocable implications that infringing the principle of accuracy may have in these cases of use could be considered unacceptable.

Additionally, it is crucial to implement robust protection measures which meet the principles of data protection by design and data protection by default to minimize risks to individuals' rights and freedoms. Adherence to specific codes of conduct elaborated to specify the application of the data protection law with regard to neurostimulation and neuromodulation may help meet all these principles and demonstrate transparency and accountability.

7. The application of neurotechnologies on children and young people

An additional layer of protection is required when processing children's personal data because they may be less aware of their rights, threats, and their potential consequences as risks for their rights and freedoms.
In certain situations, obtaining free, informed, and specific consent (when the processing is based on consent) can be a significant challenge. The age at which consent can be provided depends on each country, but it is usually between 13 and 16 years old. Below that threshold (children), it is necessary to collect parental consent. Above that threshold (young people), even when consent information is given in language that is clear and plain for them, they still may not understand the possible highly prejudicial and long-term effects that neurodata processing can have.

Data controllers should consider the public they are targeting with their products and services and be mindful of the varying applicable national laws. Since the processing of neurodata is high-risk, these controllers must

verify that those who consent to them, as data subjects or as parents, are old enough to do so (over the age threshold) and, when it is the case, holders of parental responsibility.

Furthermore, neurotechnologies may have long-term impacts that could particularly affect children and young people, given that their brains are still developing and are therefore more vulnerable at its moment of maximum plasticity. These are other key challenges concerning this population group.

They are a potential target audience for many application domains spreading the most: education, entertainment (video games, virtual reality), and neuromarketing. Therefore, they are more likely to become target of surveillance, develop addictions to online experiences, and be profiled for life, as well as led to make choices without having the maturity necessary to put them into question. The use of neurodata in this context, for instance in case of marketing of products or services, would further increase the impact on children and therefore be unacceptable. For example, according to legislation in the European Union[41], already the 'basic' (that is, not leveraging neurodata) profiling of children for the purpose of marketing (targeted advertisement) is prohibited.

In any case it is also worth mentioning that the accuracy of the processed neurodata can also be a problem, since in the case of children and young people, neurodata processing involves data on the structure, function or activity of an organ that is constantly evolving, something that does not happen with adults.

[41] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), OJ L 277, 27.10.2022, p. 1–102, available at https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

8. Privacy and security design considerations for neurotechnologies

Having set the overall context around the privacy challenges of neurodata, we now turn to an initial consideration of approaches to data security and data protection by design and default as well as wider risk mitigation. To frame this discussion, we will separate our considerations into two groups – those associated with the neurotechnology which facilitates the collection of neurodata, and those associated with the processing of neurodata.

8.1 Security Design Considerations – Neurotechnology

In 2009, Denning et al.[42] introduced the term "neurosecurity", defining it as "the protection of the confidentiality, integrity and availability of neural devices from malicious parties with the goal of preserving the safety of a person's neural mechanisms, neural computation, and free will." The authors recognized that while at that time neurosecurity was not a significant concern (as most technologies did not leave research environments), within "5-20 years" security and privacy safeguards would need to be considered early in the design phase of neurotechnologies.

Confidentiality, integrity and availability - the "CIA Triad" – will each be important in the context of neurotechnology and neurodata. Protection of **confidentiality** requires securing access to data throughout its lifecycle, including during the collection, transmission, processing, and storage phases. This will involve both information security considerations (with respect to, for instance, confidentiality on-device and in-transit) and privacy considerations based on the intended processing of the data (which we will address further in the next section).

Integrity and **availability** of a neurodata signal must also be given consideration based on context. Failures in availability will not always lead

[42] Dennin, T., Matsuoka, Y, and Kohno, T. "Neurosecurity: security and privacy for neural devices." Journal of Neurosurgery, Volume 27: Issue 1. Available at: https://thejns.org/focus/view/journals/neurosurg-focus/27/1/article-pE7.xml

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

to measurable harm to an individual; for instance, if the signal is being used to monitor attention being paid to a task, that gap in data may impact an overall analysis but not have immediate impact. However, where a neurodata signal is being used to control a prosthetic or mobility device, any interruption could result in outcomes ranging from inconvenience to serious injury. Loss of Integrity of a neurodata signal can have similar effects. For instance, Zhang et al. have shown (in a lab setting) that noise introduced to EEG signals could change the output of a device that allows a severely disabled person to spell words using their thoughts, with consequences ranging "from merely user frustration to severe misdiagnosis in clinical applications."[43]

Fortunately, significant research[44] has been undertaken with respect to securing implantable medical devices from which neurotechnology developers can draw (noting that failures of security safeguards for other implanted devices – such as pacemakers or insulin pumps – could have equally dire consequences as safeguard failure for neurotechnology). Potential neurotechnology-specific security schemes have also been proposed.[45]

Proposed measures to ensure the confidentiality, integrity and availability of neurodata will generally be familiar to those in the cybersecurity community, and include access controls, encryption of wireless signals combined with effective key management strategies, and mechanisms for secure software and firmware updates. Special consideration will also need

[43] Zhang, X. et al. "Tiny noise, big mistakes: Adversarial perturbations induce errors in Brain-Computer Interface spellers." National Science Review, Volume 8: Issue 4. Available at: https://academic.oup.com/nsr/article/8/4/nwaa233/5903729

[44] See, for instance: Camara, C., Peris-Lopez, P., and Tapiador, J. "Security and privacy issues in implantable medical devices: A comprehensive survey." Journal of Biomedical Informatics, Volume 55. Available at: https://www.sciencedirect.com/science/article/pii/S153204641500074X; Kwarteng, E. and Cebe, M. "A Survey on Security Issues in Modern Implantable Devices: Solutions and Future Issues." Pre-print. Available at: https://arxiv.org/ftp/arxiv/papers/2205/2205.00893.pdf

[45] See, for instance: Maiseli, B et al. "Brain-computer interface: trend, challenges, and threats." Brain Inform, Volume 10: Issue 1. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10403483/; Marin, E. et al. "Securing Wireless Neurostimulators." Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (March 2018). Available at: https://dl.acm.org/doi/10.1145/3176258.3176310; Xia, K. et al. "Privacy-Preserving Brain-Computer Interfaces: A Systemic Review." In *IEEE Transactions on Computational Social Systems*, Volume 10: Issue 1. Available at: https://ieeexplore.ieee.org/document/9808103

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

to be given to ensuring the integrity of the model being used to interpret first-order neurodata, as well to the need for neurotechnology (and in particular, implanted neurotechnology) to be both resilient against attack during normal operation and accessible at time of emergency (for instance, if a patient is incapacitated and unable to grant access to a device). Finally, should use of a neurotechnology device involve modulation, it will also be vital to ensure the integrity of messages being sent to the device (as well as neurodata read from it).

While we do not further highlight specific confidentiality, integrity and availability solutions in this paper, this is not done to downplay the importance of this work. This is a critical field of research and development, and we encourage the reader to engage it further.

For purposes of this paper, we will conclude by recommending that **neurotechnology developers integrate security measures appropriate to the level of sensitivity of the data being collected (taking into account type and granularity of data) and the purpose for which it will be used.**

In order to achieve this effectively, the devices that collect neurodata (sensors) or that stimulate/modulate brain waves, the neurodata themselves (stored, in transit or being processed) and the software that processes them (models, etc.) must be protected. And to do so, their particularities and specific weaknesses/vulnerabilities must be taken into account.

8.2 Privacy Considerations – Neurodata

As noted, effective information security will address the confidentiality of data – the "C" of the CIA Triad – on-device and in-transit. However, we must also consider the appropriate application of privacy principles to neurodata throughout its lifecycle including protection by design and by default as for example set out under the GDPR, Article 25.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

Groups such as the OECD's Council on Responsible Innovation in Neurotechnology[46] and the Future of Privacy Forum (in collaboration with IBM)[47] have explored the application of these principles, often with a focus on ensuring individuals' control over neurodata. The recommendations from these groups have included enhanced transparency and the promotion of opportunities for individuals to decide what, how, and to whom neurodata is shared through granular controls on devices and within companion apps, as well as simpler controls such as the ability to stop collection of neurodata when appropriate.

However, much of the determination of appropriate privacy controls (and, indeed, security controls) will rest on the sensitivity of neurodata. While a contextual analysis may be required, we recommend that **developers and regulators acknowledge that *both* first-order and second-order neurodata be considered as potentially sensitive.**

The sensitivity of first-order neurodata arises from potential inferences that can be drawn, now or in the future. Like genetic samples in years past, it may not immediately be clear the extent to which first-order neurodata is, or will be, data leading to the identification of individuals, or what inferences could be extracted from analysis of it. To some degree, the risk is unknown. However, it is probable that developments in interpretation of neurodata will continue to advance (particularly as neurotechnology sees broader adoption), and that first-order neurodata should generally be understood as warranting additional protection - a special category of data under the GDPR, or sensitive personal information under other legislative instruments.

The sensitivity of second-order neurodata, on the other hand, will be based both on the intended use of the inferred or interpreted information and the potential impacts or harms associated with its intended use or unintended

[46] "OECD Recommendation on Responsible Innovation in Neurotechnology". (December 2019) Available at: https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm
[47] Future of Privacy Forum and IBM. "Privacy and the Connected Mind: Understanding the Data Flows and Privacy Risks of Brain-Computer Interfaces." (November 2021) https://fpf.org/wp-content/uploads/2021/11/FPF-BCI-Report-Final.pdf

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

loss. Here, privacy risks are known (or knowable), and organizations are able to act accordingly.

Taken together, this means that wherever possible and appropriate:

- Given the unknown risks associated with first-order neurodata, where it is necessary to process it for a defined purpose, it should be deleted as early in the process as possible. For instance, it may be preferable to process information on-device if possible, retaining only the second-order neurodata. It is preferable to design a privacy program to manage the *known* risks of second-order neurodata. Of course, both first- and second-order neurodata remain subject to data deletion requirements.
- Where the processing of neurodata is necessary, access to that data should be limited and permitted only with strict controls (both technical and organizational) in place.

Finally, privacy-enhancing technologies should also be considered – though their appropriate role and use in this area remains a matter for future research.

9. Sector use-cases and scenarios

Neurotechnologies are already being adopted across a number of different sectors, with growing interest for new and novel uses.

It is anticipated that the health and research sector will continue to be a prominent user of neurotechnologies for the treatment of an increasing variety of physical and mental health conditions, with practical applications ranging from therapeutic (such as deep brain stimulation), to neuroprosthesis and brain machine interfaces.

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The consumer healthtech and wellness markets demonstrates a new and growing area for neurotechnology to develop, with wearable devices offering existing hardware with relevant proximity for sensors.

Portable neurotechnology devices such as wireless helmets are used in educational[48] and entertainment[49] environments to improve students' performance and learning outcomes or to maximize users' enjoyment of leisure. These kinds of devices are also being used for neuromarketing, trying to understand or predict consumer behaviour (motivations, preferences) and decision-making processes. Any devices that are brought to market must be compliant with existing legislation and should embed privacy by design and should consider approaches such as edge computing and local data storage for example.

The fact that such devices are placed on the market does not imply that the processing of personal data entailed by such devices is lawful. On the contrary, as mentioned having regard to neuromarketing, such data processing is highly possible to be in breach of necessity and proportionality, of data protection, but also of consumer law, due among others to the possible manipulation of the persons concerned ('end-users').

A sector which presents novel privacy and data protections questions is how white-collar workplaces may routinely deploy neurotechnology in the future for uses ranging from health and safety monitoring to cognitive enhancement or even in recruitment. This represents a new and concerning form of employee tracking, raising particular ethical and legal concerns, and, as in the case of neuromarketing, also highly likely to be considered by the CJEU and the European Court of Human Rights (ECHR) as incompatible with the respect for fundamental rights.

[48] Davidesco, I., Matuk, C., Bevilacqua, D., Poeppel, D., & Dikker, S. (2021). Neuroscience research in the classroom: portable brain technologies in education research. *Educational Researcher*, *50*(9), 649-656, available at https://journals.sagepub.com/doi/10.3102/0013189X211031563

[49] Navarro, D., Sundstedt, V., & Garro, V. (2021). Biofeedback methods in entertainment video games: A review of physiological interaction techniques. Proceedings of the ACM on Human-Computer Interaction, 5(CHI PLAY), 1-32, see also at https://dl.acm.org/doi/10.1145/3474695

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

In addition, there are emerging applications of neurotechnology in safety[50] (monitoring to prevent accidents) or robotics[51] (controlling machinery and processes with free hands).

10. Recommendations

10.1 Recommendations for regulators

This paper has presented a series of global views on some of the most immediate privacy and data protection challenges relating to neurodata and the uses of neurotechnologies. As noted, the recent Council of Europe report on the intersection of C108+ and neurodata has highlighted the fact that caution is needed when calling for entirely new rights and regimes in areas covered by the GDPR to mitigate the privacy and data protection risks posed by neurotechnologies. In many instances, the tools and approaches we need already exist; what is required is clarification of key definitions and how authorities use their existing tools to promote a privacy first approach to these rapid and remarkable developments. This paper has sought to build upon this view with its global survey.

It is also clear that many of these explorations have raised further questions and challenges which require additional engagement. Areas for future consideration and analysis may include:

[50] Ramos, P. M., Maior, C. B., Moura, M. C., & Lins, I. D. (2022). Automatic drowsiness detection for safety-critical operations using ensemble models and EEG signals. *Process Safety and Environmental Protection*, *164*, 566-581, see also at https://www.researchgate.net/publication/361470687_Automatic_drowsiness_detection_for_safety-critical_operations_using_ensemble_models_and_EEG_signals

[51] Aljalal, M., Ibrahim, S., Djemal, R., & Ko, W. (2020). Comprehensive review on brain-controlled mobile robots and robotic arms based on electroencephalography signals. *Intelligent service robotics*, *13*(4), 539-563, available at https://link.springer.com/article/10.1007/s11370-020-00328-5

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

- A greater examination of the fundamental intersection of the human right to dignity and the uses of neurotechnology and gathering of neurodata to better understand how and when these may be compatible.

- A closer examination of neurotechnologies on a jurisdictional basis. This document has raised important questions, but greater understanding is needed for specific privacy regimes in order to support an effective global approach.

- Acknowledgement that some data protection regimes are placing an increased emphasis on consent as the key mechanism for using neurodata and exploring what challenges might this create in a global context. How might regulators facilitate fair and appropriate use of this data across different regimes while respecting the will of the person concerned?

- A closer review of the call for explicit neurorights, taking into account the fundamental rights and freedoms already recognised (e.g., by the Universal Declaration of Human Rights or Charter of Fundamental Rights of the European Union; by the European Convention on Human Rights); a review of how regulators might engage with debates around new and revised legislation regulating neurotechnologies.

- Defining key legal and conceptual terms that intersect with data protection and privacy concerns. This may include mental identity, mental integrity, concepts of personhood and ideas of freedom of thought.

- Exploration of future definitions of high and unacceptable risk uses taking inspiration from the approach established by the EU AI Act. Are there likely to be entire sectors or groups where neurodata should not be processed? If there are, are these likely to be seen as areas of fundamental prohibition for processing?

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

- Further engagement with AI processing and regulation on a global basis to better understand the likely impact of this fast-moving sector on uses and risks relating to neurodata.

10.2 Recommendations for developers and organisations looking to deploy neurotechnologies and process neurodata

Such organisations should:

- Assess the necessity and proportionality of the processing in relation to the purposes of processing, regardless of the legal basis.

- Ensure transparency and accessibility of the highly complex and technical processing or personal data posed by neurotechnologies.

- Provide specific and clearly differentiated information for operations that read data from the brain and those that write to it.

- Perform user testing to receive feedback on the accessibility, understandability, and ease of use of the proposed transparency approach.

- Identify power imbalance as a significant threat to free consent in some specific application domains.

- Assess consent from anyone who has undergone neurostimulation or neuromodulation with extreme caution to ensure this processing has not affected the data subject's inclination to give continued consent.

- Verify that those who consent to them, as data subjects or as parents, and, when it is the case, holders of parental responsibility, are old enough to do so (over the age threshold).

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

- Integrate security measures appropriate to the level of sensitivity of the data being collected (taking into account type and granularity of data) and the purpose for which it will be used.

- Implement privacy by design and by default mechanisms.

- Acknowledge that *both* first-order and second-order neurodata are potentially sensitive data.

Further Reading

UNESCO
Ethical issues of neurotechnology: report
https://unesdoc.unesco.org/ark:/48223/pf0000383559

Unveiling the neurotechnology landscape: scientific advancements innovations and major trends
https://unesdoc.unesco.org/ark:/48223/pf0000386137

United Nations
UN Human Rights Council Advisory Committee Report (August 2024)
g2413328.pdf

OECD
Neurotechnology Toolkit
https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/emerging-technologies/neurotech-toolkit.pdf

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

Council of Europe
Common Human Rights challenges raised by different applications of neurotechnologies in the biomedical field
https://rm.coe.int/report-final-en/1680a429f3

Europe scientific report: *The privacy and data protection implication of the use of neurotechnology and neural data from the perspective of Convention 108+*
https://rm.coe.int/expert-report-neuroscience/1680b12eaa

EPRS
European Parliamentary Research Service Report (July 2024)
EPRS_STU(2024)757807_EN.pdf

Panel for the Future of Science and Technology (STOA) - European Parliament
The protection of mental privacy in the area of neuroscience - Societal, legal and ethical challenges
https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2024)757807

Australian Human Rights Commission
Protecting Cognition: Background Paper on Neurotechnology and Human Rights
https://humanrights.gov.au/our-work/technology-and-human-rights/publications/protecting-cognition-background-paper

UK Information Commissioner's Office
ICO tech futures: neurotechnology
https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ico-tech-futures-neurotechnology/

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org

The Working Group is being supported by Data Protection Commissioners and independent experts from countries all over the world in order to improve privacy and data protection in technology

EDPS-AEPD
TechDispatch on Neurodata
https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2024-06-03-techdispatch-12024-neurodata_en

The Neurorights Foundation
Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies
https://www.perseus-strategies.com/wp-content/uploads/2024/04/FINAL_Consumer_Neurotechnology_Report_Neurorights_Foundation_April-1.pdf

The Royal Society
iHuman: Blurring lines between human and machine
https://royalsociety.org/-/media/policy/projects/ihuman/report-neural-interfaces.pdf

Secretariat
Federal Commissioner for Data Protection and Freedom of Information (BfDI)
Graurheindorfer Str. 153
D-53117 Bonn
Phone +49 / 228 99/ 7799 1404

E-Mail:
IWGDPT@bfdi.bund.de

Internet:
www.iwgdpt.org