Strasbourg, 5 March 2025 T-PD(2025)1

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

(CONVENTION 108)

Draft Guidelines on Data Protection in the context of neurosciences

www.coe.int/dataprotection

Introduction

The rapid advancement of neurotechnologies has introduced unprecedented opportunities and challenges in understanding, monitoring, and influencing human brain activity. Neurotechnologies encompass a broad spectrum of tools and systems, from brain-computer interfaces and neural implants to neuroimaging and neuromodulation devices. These technologies hold transformative potential for neuroscience, clinical applications, and human enhancement. However, they also raise profound ethical, legal, and societal concerns, particularly regarding the collection, processing, and protection of neural data, and the protection of privacy of the individuals whose data are processed.

Neural data—information derived from the human nervous system, such as brain activity patterns and neural signals—poses unique regulatory challenges. Unlike other categories of personal data, neural data is inherently sensitive, as it may reveal deeply intimate insights into an individual's thoughts, emotions, preferences, or even identity. The processing of such data carries great promises for improved understanding of the human brain as well as for advancing science and medicine. At the same time, it poses significant risks, including unlawful interference with individuals' privacy, breaches of data protection, unauthorized surveillance, and manipulative practices. These risks necessitate a re-evaluation of existing human rights frameworks to ensure they are equipped to address the novel issues posed by neural data in the digital age.

Existing international instruments, such as the Council of Europe Convention **for the Protection of Individuals with Regard to the Processing of Personal Data (ETS. No 108, "Convention 108")** and its modernized version, (Protocol CETS No 223 amending Convention **for the Protection of Individuals with Regard to the Processing of Personal Data, "**Convention 108+"), provide a robust foundation for safeguarding privacy and personal data of individuals. These instruments enshrine the human right to privacy and offer commonly acceptable and transposable standards for the protection of personal data, notably by prohibiting unauthorized use, access, disclosure, and misuse. Convention 108+ furthermore explicitly emphasizes principles such as lawful processing, necessity and proportionality of the processing, purpose limitation, data minimization, data quality and the implementation of appropriate safeguards to ensure the protection of personal data, even in complex and evolving technological contexts. However, the unique characteristics of neural data necessitate additional normative efforts to interpret and adapt these principles to neurotechnologies.

These Guidelines interpret and apply the principles enshrined in Convention 108 and Convention 108+ to neural data and the processing of personal data in and by neurotechnology ensuring that privacy rights remain appropriately safeguarded and guaranteed in the context of neuroscience and neurotechnologies. These Guidelines reflect the realities of the digital age and address specific challenges associated with neural data processing, such as the heightened sensitivity of the data, the risks of re-identification from anonymized neural data, processing of personal data for legitimate purposes and the implementation of the purpose limitation principle in such context. The Guidelines aim to inform how to embed data protection considerations in line with those instruments into the imperatives of scientific progress and innovation.

For example, under Article 5 of Convention 108+, the processing of personal data is permitted only with the explicit consent of the individual or on another legitimate legal basis established by domestic law. The Guidelines provide an interpretation of this provision tailored to the context of neural data processing, ensuring that data controllers choose easily the appropriate legal basis for the processing of personal data in this context, given also some of the widely acknowledged difficulties to demarcate such data protection consent from the one required for medical, health-related interventions all at the same time ensuring that individuals remain in control over their personal data and free to decide on their mental privacy and cognitive integrity. Furthermore, these Guidelines give practical recommendations how to comply with Article 6 of Convention 108+ which highlights that special categories of personal data, including biometric data and health-related data, which overlap with neural data when these data include biometric identifiers and are used for health-related purposes, requires additional protection. In such cases, the choice of such additional measures could have an essential role for the sake of mental privacy and cognitive integrity in providing the heightened level of protection required, as outlined in the Convention and supported by domestic legislation.

The Guidelines also address broader concerns associated with neural data, including the correlation between brain activity and user preferences, behaviors, and identities. These risks are particularly pronounced in scenarios involving unauthorized data collection, sharing, or analysis, where statistically significant associations or re-identification risks emerge from otherwise de-identified data. Convention 108+ underscores the importance of addressing such risks through secure data-sharing practices, strong cybersecurity measures, and appropriate oversight mechanisms.

[While the processing of neural data should generally align with the principles outlined in Convention 108+, exceptions may arise in cases where neural data does not meet the definition of personal data. For instance, data collected from the peripheral nervous system or data that has been irreversibly anonymized may fall outside the scope of personal data regulations. In these cases, ethical and security considerations remain critical to prevent misuse and uphold public trust in neurotechnologies.]

In conclusion, the Guidelines presented in this document provide a framework for interpreting and applying the principles of Convention 108 and Convention 108+ to the processing of neural data. By addressing the unique challenges posed by neurotechnologies, these Guidelines aim to ensure that neural data processing is conducted in a manner that respects human rights, secure mental privacy, and cognitive integrity and promotes responsible innovation in neuroscience.

1. Definitions

[For the purposes of this recommendation all definitions used in the Guidelines should be interpreted as described in Convention 108+ and the document on Interpretation of provisions elaborated by the Committee.

- The expression **"personal data"** covers any information relating to an identified or identifiable individual. An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time and manpower. In cases where the individual is not identifiable, the data are referred to as **anonymous**;

- The expression **"neural data"** refers to all personal data derived from the brain or nervous system of an individual. This includes, but is not limited to, data obtained through neuroimaging, brain-computer interfaces (BCIs), neurostimulation devices, electrophysiological recordings, and other neurotechnological tools. Neural data, inter alia reveal cognitive, emotional, or behavioral information and may include patterns linked to mental states, decisions, intentions, and predispositions. Neural data can also be used to reveal non-mental information such as motor functions, physical health indicators, and reactions to external stimuli.
- The expression **"invasive neurotechnologies"** refers to technologies that require direct physical interaction with the nervous system, such as through surgical implantation of electrodes, probes, or other devices that penetrate biological tissues (e.g., deep brain stimulation implants, neural implants for BCIs).
- The expression **"non-invasive neurotechnologies"** refers to technologies that do not require surgical procedures or direct penetration of biological tissues to collect neural data. These include tools such as electroencephalography (EEG), functional magnetic resonance imaging (fMRI), transcranial magnetic stimulation (TMS), and wearable neuro-monitoring devices. It is worth considering that although they do not involve implantation, non-invasive neurotechnologies may nevertheless be intrusive.
- The expression **"mental information"** refers to information specifically related to mental processes, such as thoughts, beliefs, preferences, emotions, memories, and cognitive capacities. This includes information derived from neural activity that may indicate mental states, mental health conditions, or individual traits related to behavior or psychological well-being. It also includes information derived from non-neural sources, such as behavioral observations, self-reports, and wearable sensors. Mental data may provide insights into subjective experiences and cognitive states.
- The expression "**neural signature"** refers to unique neural patterns or characteristics that are associated with particular mental functions or states and can serve to identify or infer sensitive aspects of an individual's cognitive identity or mental experiences.
- The expression **"mental privacy"** refers to a subtype of privacy that specifically protects an individual's mental domain from unauthorized access, manipulation, unlawful interference, or exposure. Mental privacy encompasses the right to control the disclosure of one's thoughts, emotions, and cognitive states and aims to safeguard against breaches that could compromise an individual's autonomy, identity, or mental integrity.]

2. Scope

[2.1. These guidelines are applicable to the collection and automatic processing of **neural data**, [unless/in line with] domestic law, [in a specific context outside the health-care or research sectors, provides other appropriate safeguards.

/

2.1 "These Guidelines provide a set of baseline measures that governments, developers, manufacturers, and service providers should follow to ensure that the processing of neural

data does not undermine the human dignity and the human rights and fundamental freedoms of every individual, in particular with regard to the right to data protection.

2.2 Nothing in the present Guidelines shall be interpreted as precluding or limiting the provisions of the European Convention on Human Rights and of Convention 108. These Guidelines also take into account the new safeguards of the modernised Convention 108 (more commonly referred to as “Convention 108+”)]

2.2. A Party may extend the principles set out in these guidelines to cover neural data not processed automatically.

2.3 [While the processing of neural data should generally align with the principles outlined in Convention 108+, exceptions may arise in cases where neural data does not meet the definition of personal data. For instance, data collected from the peripheral nervous system or data that has been irreversibly anonymized may fall outside the scope of personal data regulations. In these cases, ethical and security considerations remain critical to prevent misuse and uphold public trust in neurotechnologies.]

2.4 [These Guidelines should specify the differences, if relevant when neural data are processed in the health-care and/or medical sector or otherwise for general public interest purposes.]

3. Principles

3.1. Respect for Privacy

3.1.1. The processing of neural data shall be carried out with full respect for human rights and fundamental freedoms, in particular the right to privacy, freedom of thought, conscience and religion, and freedom of expression. Special attention shall be given to protecting human dignity and ensuring informational self-determination, in line with the principles of Convention 108+.

3.1.2. Neural data may only be collected and processed on a valid and legitimate legal basis, in full compliance with human rights and fundamental freedoms. Such processing must be conducted with appropriate safeguards, as provided by law, ensuring the protection of individuals' rights and dignity.
Neural data derived from **invasive neurotechnologies** should be collected and processed only by qualified professionals, such as neuroscientists, clinicians, or individuals working on behalf of professionals in neurotechnology-related fields. These individuals or bodies should be subject to strict rules of confidentiality comparable to those incumbent upon health-care professionals.

Neural data derived from **non-invasive neurotechnologies** can be collected and processed by general users, including the data subjects themselves (such as patients, research participants, and healthy individuals), provided that appropriate safeguards and guarantees have been put in place for the protection of personal data and that the rights of the data subjects are respected. When it comes to security safeguards the state-of-the-art measures are to be implemented taken into account the very highly sensitive nature of personal data and that those will not be used by trained professionals but by everyday consumers. Such safeguards should ensure that unauthorized use, access, misuse, or accidental exposure of neural data is prevented They should also provide that users are adequately informed about the implications of data sharing, storage, and analysis that might interfere with individuals’ private life.

3.2. Collection, Processing and Retention of Neural Data

3.2.1. General Principles

Neural data derived from non-invasive neurotechnologies may be collected and processed by general users, including data subjects themselves (such as patients, research participants, and healthy individuals), provided that appropriate safeguards and guarantees are in place to ensure the protection of personal data and respect for fundamental rights. The collection, storage, and processing of neural data must not serve illegitimate purposes or purposes that are incompatible with the purposes of the initial processing, and the data collected should not exceed what is necessary to achieve the intended purpose.

A clear distinction must be made between neural data processing for purposes directly linked to public interest, such as medical research, healthcare, and clinical applications, and processing for other purposes, such as user experience enhancement, performance measurement, statistical analysis, and AI development. Regulatory frameworks should facilitate and support the responsible use of neural data in medicine and research while imposing stricter safeguards and limitations on non-medical applications to prevent misuse, unauthorized access, and potential risks to individual rights.

Given the highly sensitive nature of neural data and the fact that many consumer applications involve everyday users rather than trained professionals, state-of-the-art security measures must be implemented. These safeguards should prevent unauthorized access, misuse, or accidental exposure of neural data while ensuring that users are fully informed about the implications of data collection, sharing, storage, and analysis

3.2.2. Direct Collection and Lawful Basis

Neural data shall, in principle, be obtained directly from the data subject on a valid, legitimate and lawful basis. They may be obtained from other sources only when necessary to achieve the purpose of the processing or if the data subject is not in a position to provide the data, provided this aligns with all principles of these Guidelines. Even when processing serves legitimate purposes, neural data must not be retained beyond what is strictly necessary and should be securely archived, anonymized, or deleted in accordance with applicable data retention and disposal policies.

Neural data may be collected and processed only when a valid legal basis exists, in accordance with applicable laws and safeguards to protect human rights and fundamental freedoms. Processing may occur under one or more of the following legal bases, depending on the specific purpose and the necessity of data use in each context:

- **(a) Explicit and informed consent** – Neural data may be processed if the data subject, their legal representative, or an authority provided for by law has given explicit and informed consent for one or more specific purposes, unless domestic law provides otherwise. This basis applies particularly to cases where data processing is voluntary and not strictly necessary for medical or legal obligations.
- **(b) Medical and healthcare purposes** – Neural data may be processed for preventive medical purposes, diagnostics, therapy, or neurotechnology development, provided that such processing is in the interest of the data subject and is carried out by a qualified professional who initially collected the data or as permitted under Principles 7.2 and 7.3. In such cases, consent may not be required when processing is necessary for medical treatment or healthcare delivery under applicable laws.

- **(c) Compliance with a legal obligation** – Processing may be carried out if it is required by law for specific public interest reasons, including public health, epidemiological research, or other legally mandated purposes.
- **(d) Scientific research and statistical purposes** – Neural data may be processed without explicit consent when necessary for scientific research, provided that appropriate safeguards are in place, such as anonymization or strict access controls, to minimize risks to data subjects.
- **(e) Protection of vital interests** – In exceptional circumstances where neural data processing is necessary to protect the life or physical integrity of the data subject or another person, processing may occur without prior consent, subject to applicable legal safeguards.

Each legal basis applies independently, meaning they are not necessarily cumulative. The selection of the appropriate legal basis should be determined based on the specific purpose of data processing, ensuring that fundamental rights and safeguards are upheld in accordance with applicable domestic and international legal frameworks.

3.2.3. Retention and Disposition Policies

The retention of neural data must adhere to the principles of necessity and proportionality. Such data should be deleted or retained in a form that permits individual identification only as long as necessary to fulfill the purposes of processing. Establishing common standards for neural data disposition, with supervisory authorities playing a key role, can enhance consistency and accountability. Special care must be taken to prevent unnecessary retention and unlawful processing, or processing that is not compatible with the initial purpose.

3.2.4. Inferences and Mental Privacy

While the collection of neural data for research and clinical purposes should be promoted whenever legal requirements are met, restrictions apply to inferences about emotions, memories, intentions, preferences, and cognitive states when these inferences:

- **(a)** They are made without the explicit awareness and informed consent of the data subject, unless expressly permitted by law for specific, legitimate purposes;
- **(b)** They are unrelated to the stated and lawful purpose of data collection and processing; or
- **(c)** They could result in unlawful profiling, coercive influence, manipulation, discrimination, or unjustified mental state monitoring.

The use of neural data to infer highly sensitive mental characteristics—such as political beliefs, private memories, subconscious biases, or other deeply personal attributes—is strictly limited to medical and scientific research purposes and must be subject to rigorous legal and ethical safeguards. Such processing is explicitly prohibited for commercial, advertising, or marketing purposes, even with the data subject’s consent.

Additionally, particular attention must be given to mitigating potential errors and biases that may arise from the interpretation of neural activity, especially when artificial intelligence or other automated tools are used for data analysis. Developers and researchers must implement robust validation, oversight, and transparency measures to prevent misinterpretations and ensure that individuals' cognitive privacy and dignity are fully respected.

3.2.5. Neural Data of Unborn Children

Neural data concerning unborn children, such as data resulting from prenatal diagnosis or the identification of genetic or neural characteristics, should benefit from appropriate protection. Such data should be considered personal data and be subject to strict safeguards to ensure the protection of the rights and interests of the future child.

Unless otherwise provided for by domestic law, the holder of parental responsibilities may act as the legally entitled representative for decisions concerning the processing of such data, while ensuring that the best interests of the future child are upheld. The recognition of the unborn child as a data subject should be determined in accordance with applicable legal frameworks, with particular attention to ensuring that neural data is not misused for discriminatory or predictive profiling purposes.

Experts' proposal

3.2.6. Purpose and Limitations of Neural Data Processing

Neural data collected for preventive care, diagnosis, neurorehabilitation, or scientific research should only be used for these purposes or to enable the data subject to make free and informed decisions. The processing of neural data for judicial or criminal investigations and for public interest in general must be subject to specific legal provisions offering appropriate safeguards, addressing only immediate legal concerns, such as preventing imminent danger [or suppressing a criminal offense] / [preventing imminent real and serious threat to public security or risk to life and bodily harm of individuals]. Profiling of cognitive, emotional, or psychological traits unrelated to the case is strictly prohibited.

3.2.7. Predictive and High-Risk Profiling

The predictive use of neural data, such as for identifying neurological conditions or assessing behavioral tendencies, should be strictly limited to cases of overriding public interest and must be subject to rigorous legal and ethical safeguards. Predictive processing may only be considered under the following conditions:

- (a) For legitimate public health protection measures, such as the early detection of neurological disorders or epidemiological research;
- (b) When necessary to safeguard the vital interests of the data subject, particularly in cases of severe medical risk or life-threatening conditions;
- (c) For scientific or medical research, provided that appropriate safeguards, including anonymization and strict oversight mechanisms, are in place.

Predictive uses of neural data must never be employed for generalized surveillance, coercion, or speculative profiling of individuals for law enforcement purposes. In all cases, regulators must prioritize fundamental rights, including human dignity, privacy, non-discrimination, and social justice, ensuring that neurotechnology applications in both public and private sectors do not lead to unjustified restrictions on individual freedoms.

3.2.8. Neural Data Transfer and Safeguards

The global nature of neuroscience research and collaboration necessitates robust mechanisms to protect neural data during cross-border transfers. Legal grounds for data transfer must be distinguished from safeguards, which should be in place regardless of the transfer's legal basis.

Neural data transfers must comply with Convention 108+ principles, including data minimization and purpose limitation, and be accompanied by appropriate safeguards to prevent misuse, unauthorized access, and privacy risks. These safeguards should include, but are not limited to, encryption, access controls, and strict data handling protocols to ensure data security in transit and at rest.

A lawful transfer of neural data may take place under one of the following legal bases:

- (a) The data subject provides explicit, informed consent, with full awareness of the associated risks and limitations, unless domestic law prohibits reliance on consent in such contexts;
- (b) The transfer is necessary for contract performance, legal compliance, or public interest protection, provided that additional safeguards are in place to uphold individual rights and data security.

Regardless of the legal basis for transfer, all cross-border data exchanges must ensure that fundamental rights, including privacy and human dignity, are not undermined. Data transfers to jurisdictions without equivalent protections should be subject to reinforced safeguards and risk assessments to mitigate potential vulnerabilities.

3.2.9. Mental Data Protection Impact Assessments (MDPI)

Neural data processing poses risks that require proactive assessments. Article 10 of Convention 108+ mandates data controllers to assess the potential impact of data processing activities on the rights and freedoms of individuals before processing begins. This includes evaluating risks such as inaccuracies, biases, and unintended ethical or social consequences.

Furthermore, human rights due diligence and impact assessments should be implemented across public and private sectors, as recommended by the Committee of Ministers (ref). Neurotechnologies, often involving algorithmic systems, require ongoing monitoring, stakeholder engagement, and risk mitigation strategies to minimize adverse impacts on human rights.

3.3. Information of the Data Subject

3.3.1. The data subject shall be informed by the data controller of the following elements regarding the processing of their neural data:

- **(a)** The fact that their neural data are being or will be processed, including the type of data collected or to be collected;
- **(b)** The specific purpose(s) for which the data are or will be processed (e.g., neuroscience research, medical diagnosis, therapeutic interventions, or assistive technologies aimed at supporting individuals with disabilities or neurological conditions);
- **(c)** Where applicable, the individuals or entities from whom the data are or will be obtained;
- **(d)** The individuals or entities to whom the data may be communicated and the purposes of such communication;
- **(e)** The possibility, if any, for the data subject to refuse consent, withdraw it, and the potential consequences of withdrawal;
- **(f)** The identity and contact details of the data controller and, if applicable, their representative, as well as the conditions under which the data subject may exercise their rights, including access, rectification, and objection.

3.3.2. The data subject should be informed **at the latest at the moment of collection**. However, when neural data are not collected directly from the data subject, the latter should be notified of the collection as soon as possible and in an appropriate manner, unless this is clearly unreasonable, impracticable, or redundant if the data subject has already been informed.

3.3.3. Information for the data subject shall be appropriate and adapted to the circumstances, ensuring that the complexity of neural data collection and processing is explained in an accessible manner. Information should preferably be given to each data subject individually.

3.3.4. Before a neuroimaging analysis, brain-computer interface session, or neural monitoring procedure is carried out, the data subject should be informed about the objectives of the analysis and the possibility of incidental or unexpected findings, especially those related to mental states or cognitive traits.

Legally Incapacitated Persons

3.3.5. If the data subject is a legally incapacitated person who is incapable of free decision and domestic law does not permit them to act on their own behalf, the information shall be provided to the person legally entitled to act in the interest of the data subject. The data subject's capacity to understand the information should still be respected to the greatest extent possible.

Derogations

3.3.6. Derogations from Principles 5.1, 5.2, and 5.3 may be made [according to the section on exceptions / in the following cases:

- **a.** Information to the data subject may be restricted if the derogation is provided for by law and constitutes a necessary measure in a democratic society:
    - **i.** To prevent a real danger or suppress a criminal offense;
    - **ii.** For public health reasons;
    - **iii.** To protect the data subject or the rights and freedoms of others.

- **b.** In medical or research emergencies, neural data necessary for immediate medical or safety-related interventions may be collected prior to informing the data subject, provided that the subject is informed as soon as reasonably possible.]

3.4. Consent and Individual Autonomy in Neural Data Processing

3.4.1. Core Principles of Consent

Consent is a fundamental safeguard in the field of neurotechnologies, ensuring that individuals retain control over the collection, processing, and sharing of their neural data. Given the sensitivity of such data, consent mechanisms must be designed to uphold individual autonomy while addressing the unique ethical and legal challenges posed by neural data processing.

While consent is a primary legal basis for processing, it must be supplemented with strong safeguards to prevent misuse, particularly when dealing with vulnerable populations or when exceptions apply for public interest purposes, legal obligations, or medical necessity. Any limitations to consent must be justified under strict conditions of necessity, proportionality, and data minimization to ensure fundamental rights remain protected.

To be ethically and legally valid, consent must be:

- Freely given, informed, explicit, and specific to the defined purpose(s) of data collection and processing;
- Unequivocal, demonstrating a clear and voluntary decision by the data subject;
- Given without coercion, manipulation, or undue influence, ensuring that individuals are fully aware of the implications of their choice and can withdraw consent at any time without negative consequences.

Convention 108+ emphasizes the importance of obtaining valid consent for personal data processing. However, the unique nature of neural data—often involving subconscious brain activity—poses challenges to achieving truly informed consent. Individuals may find it difficult to fully comprehend the scope of data collection, its potential uses, and associated risks.

3.4.2. Ensuring Meaningful Consent in Neurotechnologies

Given the inherent knowledge asymmetry between data subjects and controllers in the field of neurotechnologies, particularly robust mechanisms are necessary to ensure that consent is meaningful and informed. These mechanisms must include:

- Clear communication of the scope and potential implications of neural data collection and processing.
- Safeguards to protect individual autonomy and uphold the integrity of decision-making processes.
- Ongoing opportunities for individuals to review and, if necessary, withdraw consent.

Neurotechnology developers and operators must integrate these safeguards into their systems to ensure that individuals retain control over their neural data and can make decisions based on comprehensive, comprehensible, and transparent information.

3.4.3. Consent for Vulnerable Populations

Special provisions must be established to protect vulnerable populations, including legally incapacitated individuals or those with limited decision-making capacity. In such cases:

- Consent must be provided by the individual's legal representative or an authority specified by law, in accordance with domestic legislation.
- The data subject must be informed of the intention to process their neural data, and their wishes should be taken into account to the extent possible.
- Additional safeguards should ensure the protection of the individual's rights, dignity, and autonomy.

3.4.4. Limitations of Consent as a Legal Basis

Consent is not always an appropriate legal basis for data processing, particularly in situations where **an imbalance of power exists between the data controller and the data subject**, such as when processing is conducted by public authorities or in employment or healthcare settings. **In such cases, alternative legal bases should be carefully assessed to ensure that individuals' rights and freedoms are effectively protected.**

When consent is used as a legal basis under **Article 5(2) of Convention 108+**, it must meet **strict validity requirements**:

- **Consent must be freely given, informed, explicit, and specific** to the purpose of data collection and processing.
- **The data subject must have a genuine choice** and the ability to withdraw consent at any time without detriment.

Regardless of the legal basis for processing, **all data protection principles must be upheld**, including:

- **Necessity and proportionality** – Processing should be strictly limited to what is essential for the stated purpose.
- **Transparency** – Data subjects must be fully informed about the processing and its implications.
- **Data minimization** – Only the minimum amount of neural data necessary for the purpose should be collected and processed.

3.4.5. Legal Bases for Neural Data Processing

Under **Article 5 of Convention 108+**, the processing of neural data is considered **legitimate** when based on:

1. **The data subject's explicit, free, informed, and specific consent**; or
2. **Some other legitimate basis laid down by law**, which may include:
    - Processing necessary for the **protection of the vital interests** of the data subject or another person;
    - Processing required to **comply with a legal obligation** to which the data controller is subject;
    - Processing necessary for reasons of **public interest**, including **scientific or medical research** and **public health protection**, subject to **strict safeguards and proportionality**;
    - Processing necessary for the **performance of a contract** or pre-contractual measures at the request of the data subject.

Given the **sensitive nature of neural data**, consent remains a particularly **appropriate** legal basis in many cases, **ensuring individual autonomy and control**. However, in circumstances where **consent is not feasible or appropriate**, other legal bases may be relied upon, provided that processing:

- **Strictly adheres to the principles of necessity, proportionality, and data minimization**;
- **Complies with strengthened protections for special categories of data**;
- **Ensures fundamental rights are safeguarded, including privacy, human dignity, and non-discrimination**.

3.4.6. Secondary Uses and Renewed Consent

The results of any neural analysis must remain within the boundaries of the objectives for which consent was originally obtained. Any subsequent use of the data—especially for purposes involving secondary inferences—requires renewed consent unless the data is anonymized to a degree that prevents re-identification. Such measures are critical to maintaining trust and respecting the autonomy of data subjects.

3.5. Communication

3.5.1. Neural data shall not be communicated unless in accordance with the conditions set out by the law.
3.5.2. In particular, unless other appropriate safeguards are provided by domestic law, neural data may only be communicated to individuals subject to confidentiality rules equivalent to those incumbent upon health-care professionals or researchers, and who comply with the provisions of this recommendation.
3.5.3. Neural data may be communicated if they are relevant and:

- **a.** If the communication is provided for by law and constitutes a necessary measure in a democratic society for:
    - **i.** Public health reasons;
    - **ii.** The prevention of a real danger or the suppression of a specific criminal offense;
    - **iii.** Another important public interest;
    - **iv.** The protection of the rights and freedoms of others.
- **b.** If the communication is permitted by law for the purpose of:
    - **i.** The protection of the data subject or a relative;
    - **ii.** Safeguarding the vital interests of the data subject or a third person;
    - **iii.** Fulfilling specific contractual obligations (e.g., agreements related to neuroprosthetic devices);
    - **iv.** Establishing, exercising, or defending a legal claim.
- **c.** If the data subject or their legal representative, or an authority provided for by law, has given their explicit consent for one or more purposes, insofar as domestic law does not provide otherwise.

d. Provided that the data subject or their legal representative, or an authority, has not explicitly objected to non-mandatory communication, and if the data have been collected in a freely chosen preventive, diagnostic, or therapeutic context, and if the purpose of the communication (e.g., care provision or service management) is compatible with the purpose of the original data processing.

3.6. Purpose Limitation and Impact Assessments

3.6.1. Neural data should be collected for explicit, specific, and legitimate purposes and must not be processed in ways incompatible with those initial purposes.
As the application of the principle of purpose limitation might become challenging due to the difficulty to selectively filter purpose-specific information from the dynamic flow of neural data,

the adherence to the principle of **data minimization**, ensuring that only the data strictly necessary for legitimate purposes is collected and processed is particularly important.
In the same line **impact assessments** must be conducted before implementation to evaluate the risks and ensure data collection remains proportionate to its stated purpose.

3.6.2. Neural data collection should serve legitimate purposes, such as medical research or treatment, in alignment with constitutional and international legal standards, rather than being driven by expediency or mere desirability.

3.6.3. Legislation governing neurotechnologies should define the system's scope and the specific purposes for processing neural data. This legislation should be presented in an accessible and comprehensible format and be accompanied by a publicly disclosed impact assessment. Such an assessment should evaluate potential impacts on human rights and fundamental freedoms, while identifying safeguards to mitigate risks to privacy and data protection.

3.6.4. Data controllers and entities providing the hardware, software, and services enabling neurotechnologies should, whenever is appropriate, by design and through continuous measures, ensure that only data strictly necessary for legitimate purposes are processed. If the processing becomes incompatible with these legitimate purposes, the data must not be further processed and should be deleted.

3.6.5. The reuse of neural data must be strictly prohibited unless explicitly authorized by law and accompanied by adequate safeguards.

3.6.6. Neural data sharing must be justified, and any processing that leads to disproportionate interference with privacy or other human rights and fundamental freedoms, as defined under Convention 108+, is deemed excessive and constitutes unlawful data processing.

3.7. Necessity and Proportionality

3.7.1. Data processing must be conducted in a manner that is necessary to the legitimate purpose for which it was collected. The neural data collected must be proportionate and sufficient to meet the identified purposes, avoiding excessiveness in relation to those objectives.

3.7.2. Before implementing neurotechnologies data controllers must define the legitimate and purposes for processing personal data. This ensures compliance with the principles of necessity and proportionality and meets the requirements of legitimate processing and purpose limitation under Article 5(4)(b) of Convention 108+. It also prevents data from being processed for vague, imprecise, or incompatible purposes and aligns with the design obligations established in Article 10 of the Convention.

3.7.3. Neural data processing must be strictly **limited** to what is essential for achieving its specified purpose. Moreover, neural data collection and processing must remain proportionate to the intended objective, avoiding unnecessary intrusions into individuals' **mental privacy**. The following must be assessed: a) the **sensitivity** of neural data being processed; b) the potential **risks and impacts** on individuals' rights and freedoms; and c) whether the degree of interference is justified in relation to the **legitimate purpose** pursued.

3.7.4. To uphold the principles of necessity and proportionality, an **impact assessment** must precede the deployment of neurotechnologies. The assessment should evaluate: a) the specific purpose and **legality** of processing neural data; b) whether the data collection is

essential and avoids excessive or irrelevant information; and c) the risks to individuals' privacy and mental integrity, ensuring that safeguards are implemented to mitigate these risks. 3.7.5. Impact assessments should be conducted transparently and shared with relevant supervisory authorities to promote **accountability** and trust.

3.8. Fairness & Transparency

3.8.1 Neural data must be processed fairly and in a transparent manner as outlined in Article 5, paragraph 4(a).

3.8.2. Transparency is a critical aspect when neuro technologies are employed and also ensures that individuals are aware of their rights and understand how to exercise them.

3.8.3. To adhere to this principle, neural data processing must comply with Article 8 of Convention 108+ as interpreted by paragraphs 67 to 70 of the Explanatory Report.

3.8.4. These provisions detail the information that must be provided to individuals to uphold transparency. This information can be presented in multiple formats or layers—such as general overviews on websites or detailed explanations in enrollment forms—to enhance clarity and accessibility. It is essential that the information is user-friendly, comprehensible, and tailored to the needs of specific groups, such as individuals with visual impairments or low literacy levels.

Individuals must be provided with clear information, including:

- The purpose of processing their neural data.
- The consequences of refusing to provide neural data.
- The identity of the neural data controller and processor.
- The recipients of their neural data.
- The methods by which they can exercise their rights.
- Whether their data will be transferred to other countries.

3.8.5 Additionally, individuals should be informed about the techniques used to collect neural data, including whether those techniques are invasive or non-invasive. This information must be communicated to individuals in a manner they can understand, taking into account their capacity to comprehend the details provided.

3.8.6. The principle of fairness ensures that neural data processing activities are conducted ethically and without discrimination. Neural data controllers must not misrepresent the scope, purpose, or risks of data processing. Furthermore, safeguards must protect individuals, especially **vulnerable individuals and groups**, from the unfair exploitation of neural data.

3.9. Accuracy

3.9.1. The neural data processed should remain accurate. Furthermore, to protect individuals' human rights and fundamental freedoms, it is crucial to implement measures ensuring the accuracy of neural data processes. Any inaccuracies must be corrected or deleted efficiently and promptly to prevent serious consequences.

3.9.2. Maintaining neural data quality is critical and should be part of an ongoing cycle of assessment, evaluation, and adaptation to ensure relevance and accuracy over time. Adherence to good data quality management practices promotes interoperability across systems, institutions, and jurisdictions. This helps prevent negative impacts on individuals'

rights and freedoms, eliminates duplication in registered identities, and ensures the efficient management of services reliant on these identities.

3.9.3. According to Paragraph 89 of the Explanatory Report to Convention 108+ and Article 10, which emphasizes additional obligations, data protection requirements must be integrated at the earliest stages of system architecture and design through technical and organizational measures (data protection by design). This proactive approach minimizes risks and enhances the overall reliability of neural data processing systems.

3.9.4. Testing for accuracy is an essential element of a human rights-by-design approach and must be conducted before purchasing or implementing neurotechnologies. This ensures that the systems meet high standards of fairness and effectiveness while minimizing the potential for adverse impacts.

3.9.5. Given the highly sensitive nature of neural data—which can reveal insights into an individual's thoughts, emotions, and cognitive processes—enhanced security measures and safeguards are necessary. Appropriate security measures must be developed to protect neural data from cybersecurity threats, unauthorized access, destruction, loss, alteration, or disclosure and inappropriate use, recognizing the unique vulnerabilities associated with this type of information.

3.9.6. Neurotechnologies might involve processing neural data on a large scale. Ensuring robust data and system security is critical, as failures can result in severe adverse effects on the human rights and fundamental freedoms of individuals, groups, and communities.

3.9.7. To mitigate risks, appropriate technical and organizational measures must be implemented to protect neural data and uphold human rights. Failure to secure neural data effectively constitutes unlawful processing and can lead to unauthorized access, theft, or disclosure, causing harms such as harassment, persecution, fraud, or identity theft. Convention 108 and 108+ highlights the need for robust safeguards to prevent unauthorized access to individuals' personal data. This is particularly relevant in scenarios where decoding techniques could intrude on mental privacy.

3.9.8. Preventing third-party tracking of neural data is equally vital. Measures to ensure security include:

1. Data Minimization by Design: Systems should default to processing only the neural data necessary for each specific purpose.
2. Risk Assessment and Mitigation: Evaluate the sensitivity of the neural data and potential adverse impacts, adopting measures to address identified risks.
3. Incident Management: Implement policies to investigate and manage security incidents, report breaches to affected individuals and supervisory authorities, and address adverse impacts.
4. Access Control: Establish stringent policies, procedures, and technical controls to manage system and data access.
5. Data Encryption: Secure neural data in transit and at rest, ensuring access is restricted to trusted devices.
6. Ongoing Security Review: Regularly assess security measures, address weaknesses, and maintain a log of reviews and corrective actions.
7. Vulnerability Reporting: Provide secure channels for reporting security vulnerabilities confidentially.
8. Effectiveness Testing: Regularly test the effectiveness of security measures and take action to address any shortcomings that could compromise neural data protection.

9. Contingency Planning: Develop plans to handle potential misuse of compromised neural data and ensure continuity of services reliant on neurotechnologies, including backup systems and processes.
10. Mitigation of Third-Party Tracking: Add security barriers to prevent information leaks, and disclose liability waivers and legal frameworks governing third-party breaches.

3.9.9. Regulatory authorities and policymakers should adopt a precautionary approach to neural data protection, acknowledging the growing complexity of neural data processing and its transformative impact. This approach should ensure that emerging risks are proactively addressed and that safeguards evolve alongside advancements in neurotechnology.

3.9.10. Data controllers should implement preventive policies to address the risks associated with the use of neural data and its potential impact on individuals and society, ensuring robust protection of personal data during processing activities.

3.9.11. Neural data controllers and processors must conduct a **thorough risk assessment** to comply with the principles of **lawful data processing and data quality** under **Convention 108+**. This obligation ensures that potential adverse effects on **fundamental rights and freedoms** are identified, prevented, or minimized. The assessment must carefully **balance the protection of these rights with the legitimate interests involved** in neural data use, ensuring **proportionality, necessity, and accountability** in all processing activities.

3.10. Accountability

3.10.1. Core Principles of Accountability

Accountability is a cornerstone of Convention 108+ and modern data protection frameworks, requiring data controllers and, where applicable, data processors to demonstrate that their data processing practices comply with legal and ethical obligations. In the context of neural data, accountability plays an even more critical role, given the sensitive and potentially intrusive nature of such data.. Continuous transparency, regular risk and threat assessments, and adherence to structured governance practices are essential. Organizations must demonstrate their commitment to protecting human rights throughout the lifecycle of neural data processing and ensure that such practices are embedded into their operational and governance structures.

3.10.2. Key Actions to Ensure Accountability

To meet these requirements and maintain accountability, organizations involved in neurotechnology development and deployment should adopt the following measures:

1. **Commitment to a Human Rights-Based Approach**
    - Clearly document and publish a commitment to a human rights-based approach in the collection, processing, and use of neural data.
2. **Human Rights Impact Assessments (HRIAs)**
    - Conduct human rights impact assessments (HRIAs) at each stage of neurotechnology development, from policy formulation to implementation.
    - Publish the results of HRIAs to ensure transparency and provide evidence of how potential risks to human rights have been mitigated.
3. **Stakeholder Engagement and Inclusion**
    - Actively engage with stakeholders, including affected individuals, communities, experts, and civil society organizations.

- Document and act on feedback from stakeholders to address concerns and improve accountability practices.

4. **Policies, Procedures, and Ethical Oversight**
   - Develop and implement comprehensive policies and procedures addressing human rights, data protection, and non-discrimination.
   - Establish governance structures, such as ethics committees, to oversee the development and implementation of neurotechnologies and ensure ethical integrity.
5. **Explainable Artificial Intelligence (XAI) in Neurotechnologies**
   - Ensure that artificial intelligence (AI) systems used in neurotechnologies are designed with explainability as a core principle.
   - Develop mechanisms to provide clear, understandable, and accessible explanations of how AI systems process neural data, make inferences, and arrive at decisions.
   - Employ XAI to support accountability by enabling individuals, auditors, and regulators to understand the rationale behind AI-driven processes and to detect potential biases, errors, or unethical practices.
   - Encourage the integration of explainability into AI design to ensure alignment with the principles of transparency, fairness, and accountability.
6. **Transparency**
   - Provide clear and accessible information to individuals on their rights regarding neural data processing and how they can exercise these rights.
   - Ensure that such information is tailored to address the unique complexities of neural data and its implications.
7. **Training and Capacity Building**
   - Implement robust training programs for all personnel involved in neural data processing to ensure awareness of human rights, data protection, and privacy obligations.
8. **Auditing and Compliance Monitoring**
   - Conduct regular audits of data processing activities to identify potential risks or non-compliance with human rights and data protection standards.
   - Address findings through corrective actions and continuous improvement.
9. **Complaint and Redress Mechanisms**
   - Establish clear, accessible, and effective mechanisms for individuals and communities to lodge complaints and seek redress for violations of their rights.
   - Ensure these mechanisms are transparent and responsive, building trust in the accountability framework.
10. **Procurement and Vendor Accountability**

    - Incorporate human rights criteria into the procurement process, requiring vendors to conduct HRIAs and demonstrate their commitment to human rights.
    - Monitor vendors' compliance with these criteria throughout the contract lifecycle.

11. **Independent Reviews and Oversight**
    - Facilitate independent reviews of neurotechnology systems and their impact on human rights, involving stakeholders such as universities, NGOs, government organizations, and industry experts.
    - Publish the findings of these reviews to enhance transparency and public trust.

3.10.3. Accountability as a Dynamic and Collaborative Process

Accountability in neural data processing is not a static obligation but a dynamic and

collaborative process. It requires continuous monitoring, adaptation to emerging challenges, and proactive engagement with all relevant stakeholders. By embedding robust accountability measures into their practices—including the use of explainable AI—organizations can ensure that neurotechnologies are developed and deployed in a manner that respects and upholds human rights, fosters public trust, and promotes ethical innovation.

3.11. Special Protections for Minors and Vulnerable Groups

3.11.1. Minors and vulnerable groups face unique risks when interacting with neurotechnologies, particularly because of their **developing cognitive functions** and **susceptibility to external influences**.

3.11.2. Due to the unique plasticity of their developing brains, children and adolescents may be especially vulnerable to the potential negative effects of neurotechnologies. Interactive technologies can influence the process of identity formation, impact autonomy, and decision-making capacities, and foster dependency.

3.11.3. As brain-computer interfaces for video gaming become more widespread in the coming years, young users may face unforeseen consequences, including potential long-term psychological or mental health challenges. Advanced surveillance technologies could also be used to infer insights into children's mental states, predict health outcomes, and influence behaviors.

3.11.4. Neurotechnologies have the capacity to exploit or alter cognitive and sensory experiences, thoughts, and emotions, potentially interfering with children's mental and physical integrity. Furthermore, commercial neurotechnologies may expose children to "neuromarketing" strategies designed to prioritize corporate interests over the child's welfare, making these practices highly manipulative.

3.11.5. Children's mental health, autonomy, and cognitive integrity must be safeguarded in neurotechnology development. Given their vulnerability, strict regulations must ban the use of neurotechnologies for marketing, targeted advertising, and commercial profiling of minors.

Neurotechnologies in educational settings must be scientifically validated, privacy-protective, and ethically justified. Special attention is required for informed consent, as children and caregivers may not fully grasp the risks. A child-centered regulatory framework must ensure neurotechnologies support education and well-being without exposing minors to commercial exploitation.

3.11.6. Parents may be misled into believing that certain neurotechnologies can enhance their children's intellectual abilities, potentially leading them to impose these tools on their children despite the associated risks. Clear guidance and regulatory measures are needed to ensure that children's welfare and rights are protected in this rapidly advancing technological landscape.

3.11.7. Moreover, **legislation** should provide for enhanced protections for minors and vulnerable groups, like:

1. **Informed Consent and Assent**:
    - Parents or guardians must provide **explicit, informed consent** for the collection and processing of neural data from minors.

    - In addition, minors should be given the opportunity to provide **assent**, meaning their consent should be **voluntary** and based on an age-appropriate understanding of the risks and benefits.
2. **Age-Appropriate Safeguards**:
    - Data controllers must ensure that neurotechnologies are designed to be **age-appropriate**, and that information about the technology is provided in formats that are understandable for both minors and their guardians.
    - Special attention should be paid to **non-invasive technologies** that minimize physical and psychological risks.
3. **Prohibition of Harmful Practices**:
    - Prohibit the use of neurotechnologies for purposes that may **harm** minors, such as **neuromarketing, behavioral modification**, or **identity manipulation**.
    - Regulate the use of neurotechnologies in contexts where minors may be influenced in ways that could negatively impact their **mental health, well-being**, or **autonomy**.

In addition to minors, **vulnerable adults**—including those with cognitive impairments, mental health issues, or limited decision-making capacity—also require special protections. The risks include:

1. **Exploitation and Coercion**: Vulnerable adults may be more susceptible to **exploitation** through neurotechnologies, particularly in the form of **coercion** or **manipulation** by third parties.
2. **Informed Consent Challenges**: Adults with limited mental capacity may struggle to provide fully **informed consent** for neural data processing, raising concerns about their **autonomy** and **mental privacy**.

Legislation and policies should ensure **vulnerable adults** are afforded the same robust protections as minors:

1. **Informed Consent**:
    - Ensure that **vulnerable adults** give informed consent for neural data processing, and establish mechanisms for ensuring that consent is given freely and **without undue influence**.
    - In cases of diminished capacity, provide safeguards to ensure that consent is **genuine** and that individuals are fully informed of the **risks and implications.**
2. **Special Considerations for Cognitive Impairments**:
    - Take extra precautions when processing neural data of individuals with **dementia, Alzheimer's disease**, or other **cognitive impairments**, ensuring that their mental privacy is respected, and that their data is not used in ways that could be harmful or exploitative.
    - Develop **tailored consent** processes for individuals with mental health conditions or cognitive disabilities, involving caretakers or legal representatives when necessary.

3.12. Supervisory Authorities

Article 15 of Convention 108+ established that each Party shall provide for one or more authorities to be responsible for ensuring compliance with the provisions of this Convention. Because the complexity and challenges of neural data processing, Parties of the Convention shall ensure that the supervisory authorities are provided with the material and technical resources necessary for the effective performance of their functions and exercise of their powers in assessing and controlling the activities of neurotechnologies.

.

Because the nature of neural data, Supervisory Authorities should pay particular attention to:

1. **Mental Privacy Protection**:
    - Ensure that the collection and processing of **neural data** do not infringe upon individuals' **mental privacy**.
    - Provide additional safeguards for the processing of neural data related to **biometric identification, emotional states,** or **cognitive processes**, which have a higher risk of harm or exploitation.
2. **Compliance with Consent and Purpose Limitation**:
    - Verify that **informed consent** is obtained from individuals and that **neural data** is processed only for the **explicit, legitimate purposes** specified at the time of collection.
3. **Handling of Special Categories of Data**:
    - Ensure that neural data, particularly when it falls under the **special categories of personal data** (health data, biometric data), is subject to **additional safeguards** as required by **Article 6 of Convention 108+**.

The Supervisor authorities are responsible for safeguarding human rights and fundamental freedoms while ensuring compliance with data protection obligations as outlined in Convention 108 and Convention 108+.

3.13. Exceptions and Special Circumstances

The principles included in this document -the Guidelines- are relevant to the use and develop of neurotechnologies, assuming that most neurotechnologies involve processing personal data. Data protection principles apply when the identification or re-identification of individuals is possible. However, they do not apply to fully anonymized data that has been processed to eliminate all links to the individual who provided it.

Moreover, certain **exceptions** and **special circumstances** may apply, particularly in cases where processing is deemed necessary for public interest, national security, or other legitimate objectives. It is crucial that such exceptions are carefully considered and applied in a manner consistent with the **fundamental rights** and **privacy protections** established under **Convention 108+**.

Following **Article 9** of **Convention 108+**, there are certain exceptions to the rules governing the processing of personal data, including **neural data**. These exceptions must be interpreted and applied with caution to ensure that they do not undermine the essential protections afforded to individuals. As it is mentioned above, exceptions may include:

1. **Public Interest or Legal Obligations**: In some cases, processing neural data may be necessary for the **performance of a public interest task** or for compliance with a **legal obligation**. These exceptions must be narrowly defined and subject to strict safeguards to avoid overreach or undue interference with individual rights.
2. **National Security or Law Enforcement**: Processing neural data may be justified in exceptional circumstances where it is **necessary for national security**, **the prevention of crime**, or **public safety**. Such processing must be proportionate to the objective pursued and must not disproportionately infringe upon the individual's privacy and mental integrity. However, the use of neurotechnologies should be prohibited as a tool to prosecute accused individual for any crime or as a mean that could affect the right of the accused, the right to defend and due process.

3. **Health and Public Health Purposes**: In certain cases, neural data may be processed without explicit consent for the purposes of **public health** or **medical research** when it is necessary to protect the health of individuals or the general public. Any such processing must be consistent with existing **ethical standards** and subject to appropriate **safeguards**.
4. **Scientific Research**: Exceptions may also apply in cases where neural data is processed for **scientific research** purposes, particularly when it serves **public interests** such as advancing medical knowledge or improving public health outcomes. However, even in these circumstances, strict safeguards must be in place to ensure that the data is anonymized whenever is possible, and that individuals' **privacy** and **mental integrity** are not unduly compromised.
5. **Emergencies and Public Health Crises:** During **emergencies** or **public health crises** (like pandemics), neural data may be processed with greater flexibility to respond to urgent needs. However, even in such situations, the processing should be **time-limited** and **targeted** to the specific needs of the crisis, and **data protection principles** must be upheld to the extent possible.

Finally, even when exceptions might applied, **transparency** and **oversight** mechanisms should be maintained to ensure accountability and prevent misuse. For example, data controllers must provide clear justifications for any processing that falls under an exception. Moreover, **i**n cases where exceptions are invoked, there must be robust **independent oversight** by **supervisory authorities** to ensure that the processing is carried out lawfully and that the individual's rights are adequately protected. Finally, **d**ata processing activities that rely on exceptions should be subject to **regular reviews** to assess whether the processing is still justified and whether the safeguards are sufficient. In some cases, processing should be suspended or limited if it is no longer necessary or if the risks to individuals' rights outweigh the benefits.

4. RIGHTS OF NEURAL DATA SUBJECTS

Article 9 of Convention 108+ establishes a robust framework for individual rights over the processing of personal data, that might be interpreted as included within the context of neural data processing. These rights apply to all individuals, regardless of citizenship, nationality, or residency status, and they must be enshrined in law. The rights can only be restricted if it is a necessary and proportionate measure in a democratic society, for specific and legitimate public interest purposes, and always respecting the essence of fundamental rights and freedoms.

To ensure that individuals can exercise their rights effectively within the use of neurotechnologies, the following rights must be ensured:

1. **Right to Information**:

   Individuals must be informed about:

   - Why their neural data are required,
   - The purposes for which their neural data will be used,
   - The legal basis for processing (e.g., consent, legal obligation),
   - The retention period of their neural data,
   - The entities with which their data will be shared or accessed, and
   - Any use of automated systems to process their neural data, especially if it involves significant legal decisions. Information should be provided in clear, simple, culturally appropriate ways to ensure fairness.

- Individuals are entitled to receive confirmation as to whether their neural data is being processed.
- Individuals have the right to obtain information about the reasons for processing their neural data and the applications or outcomes of that processing.
- Offer clear and comprehensive information to the public and research participants about the collection, storage, processing, and potential use of personal brain data collected for health purposes.

2. **Right of Access**:

   Individuals have the right to access their neural data and obtain a copy, when is technologically possible, of the neural data being processed, free of charge.

3. **Right to Control Neural Data**

   Individuals are entitled to exercise free control and self-determined action over their neural data and mental information.

4. **Right to Rectification**: Individuals can have inaccurate neural data corrected, free of charge and without excessive delay.

5. **Right to Erasure**:

   Individuals can request the deletion of their neural data, free of charge, if the neural data processing contravenes applicable laws (e.g., data protection laws). If data is processed in violation of the convention, individuals have the right to request its erasure. Should the data controller refuse, appropriate remedies must be made available to the individual. Regarding access to neural data and the individual's ability to request its erasure, any regulation should align with established principles governing the processing of health data. In certain situations, individuals should be able to request the deletion of their neural data.

6. **Right to Restrict Processing**:

   Individuals can request the restriction of their neural data processing under certain conditions.

7. **Right to Object**:

   Individuals may object to the processing of their neural data unless the data controller demonstrates a legitimate interest that outweighs the individual's rights or fundamental freedoms.

8. **Right to Not Be Subject to Automated Decisions**:

   Individuals should not be subject to decisions that significantly affect them, based solely on automated processing of their neural data, without having their views considered. Automated processing in respect to non-medical uses needs closer scrutiny.

9. **Right to Present a Complaint**:

   Individuals have the right to file a complaint with a supervisory authority regarding the processing of their neural data.

10. **Right to Judicial and Non-Judicial Remedies**:

    Article 12 of Convention 108+ guarantees the right to seek judicial and non-judicial remedies when their rights are infringed.

11. **Right to Explanation of Automated Decisions**:

    In cases of automated decisions, individuals have the right to explanations that describe how the decision was reached and provide relevant information about the system, including data inputs and outputs.

12. **Right to Neural Data Portability.**

The design of neurotechnologies must prioritize enabling individuals to fully exercise these rights. This requires a system that facilitates transparency, accountability, and fairness in the processing of personal data while ensuring individuals are informed about their rights and the conditions under which they may be limited.

5. RECOMMENDATIONS FOR POLICY MAKERS

Policy makers, including members of parliaments, legislators, government officials, and policy advisors, play a vital role in setting societal values and legal approaches, as well as defining standards applicable to national digital identity schemes.

Policy makers? should:

- **Define clear goals for neurotechnologies**: Ensure that the objectives are well-defined, evidence-based, and proportionate, aligning with the legitimate purposes pursued.
- **Adopt a human-rights-centered national policy**: Prioritize the protection of fundamental rights and freedoms in all policies involving neurotechnologies.
- **Integrate human rights impact assessments (HRIA)**: Extend the scope of data protection impact assessments (DPIA) to explicitly include broader human rights considerations, ensuring these are incorporated into the policy design, implementation, and operation of neurotechnologies. This includes the introduction of a Mental Data Protection Impact Assessment (MDPIA).
- **Establish regulatory forums**: Create platforms for data protection regulators and other supervisory authorities to collaborate, ensuring effective compliance, addressing risks, and developing best practices.
- **Engage stakeholders**: Inform policy and legislative development through meaningful stakeholder engagement. Provide opportunities for stakeholders to contribute to and review policies and laws before their adoption.
- **Publish stakeholder engagement results**: Promote transparency by sharing the outcomes of stakeholder consultations.
- **Regulate neural data processing**: Specify in law that the processing of neural data is permissible only for specific and legitimate purposes, based on a defined legal framework.

- **Strengthen consent requirements**: Ensure that consent for neural data processing is valid only when all conditions for informed, free, and explicit consent are met, safeguarding individual autonomy.
- **Mandate human rights impact monitoring**: Require continuous assessments of human rights impacts throughout the lifecycle of neurotechnologies, from policy development to implementation and operation.
- **Promote privacy and human rights by design**: Develop and adopt methodologies reflecting Article 10 of Convention 108+ and best practices to embed privacy and human rights considerations into the design and deployment of neurotechnologies.
- **Establish redress mechanisms**: Ensure that civil and judicial remedies are available for individuals if any of data subjects rights is not respected.
- **Create independent oversight bodies**: Establish independent entities with the authority to conduct audits and enforce corrective measures.
- **Plan for harm mitigation**: Develop strategies to address risks arising from the compromise of neural data processing, including data theft, denial-of-service attacks, and other forms of cybercrime as outlined in the Council of Europe's Budapest Convention (ETS No. 185) and its protocols. Address the misuse of national identity systems to harm individuals or groups.
- **Criminalize attacks on neural data processing**: Align with the Budapest Convention to criminalize acts such as unauthorized access, selling, or misuse of neural data for financial or other gains.
- **Set clear data retention guidelines**: Legislation should define retention periods and specify the conditions under which neural data may be stored.
- **Protect minors and vulnerable adults**:
    - Regulate neurotechnologies to prevent neuromarketing, behavioral manipulation, and other harmful practices targeting these groups.
    - Require rigorous ethical reviews for research involving neurotechnologies and implement guidelines tailored to the needs of minors and vulnerable adults.
    - Establish clear, age-appropriate informed consent and assent procedures.
    - Introduce special safeguards to ensure the free, informed, and genuine consent of vulnerable adults, protecting them from coercion or undue influence.

By following these recommendations, policy makers can ensure that neurotechnologies are developed and implemented responsibly, respecting human rights and promoting trust in digital identity systems.

6. RECOMMENDATIONS FOR SUPERVISORY DATA PROTECTION AUTHORITIES (SDPAs)

Supervisory data protection authorities (SDPAs) should play an active role in enforcing national and international data protection laws, in alignment with Chapter IV of Convention 108+.
SDPAs' key responsibilities include:

- **Consultation on legislative measures**: Article 15(3) of Convention 108+ requires Parties to consult SDPAs on any legislative or administrative measures involving personal data processing. Policy makers and legislators must ensure SDPAs are involved as key stakeholders, starting from the formulation of national policies on neurotechnologies and throughout the legislative process.
- **Issuing opinions on neural data processing**: SDPAs have the authority to provide opinions on neural data processing operations that pose risks to individuals' rights and freedoms. Such opinions should be issued as part of consultations under Article 15 of Convention 108+ on proposals to introduce or amend neural data processing regulations.

- **Promoting public awareness**: SDPAs must engage in activities to raise public awareness about their role, including issuing periodic reports on their activities related to neurotechnologies. This aligns with their role as advocates for data protection and privacy.
- **Collaborating with stakeholders**: Work with key stakeholder groups to raise awareness about the impact of neurotechnologies on human rights. SDPAs should contribute to policy development, lawmaking, and creating guidance or legally binding codes of practice to mitigate risks.
- **Participating in human rights impact assessments**: SDPAs should be part of decisions involving human rights impact assessments (HRIAs) that expand DPIAs to explicitly integrate human rights considerations into the design, implementation, and operation of neurotechnologies.
- **Engaging in regulatory forums**: Participate in forums alongside other supervisory authorities to ensure compliance, address risks, and develop best practices for neurotechnologies.
- **Ensuring independent oversight**: Ensure external oversight of neural data processing is carried out by SDPAs or with their involvement, maintaining objectivity and accountability.

Strengthening the Role of SDPAs

To enhance their effectiveness in protecting individual rights and ensuring compliance with neural data protection regulations, the following actions are recommended:

1. **Allocate Adequate Resources**:
    - Ensure that supervisory authorities are well-funded, staffed, and trained to oversee neural data processing activities effectively.
2. **Develop Specialized Expertise**:
    - Build specialized teams with expertise in neurotechnologies and mental privacy to address the unique challenges posed by neural data.
3. **Ensure Independence**:
    - Safeguard the independence of supervisory authorities from external pressures, including data controllers, processors, or public entities.
4. **Promote Cross-Border Cooperation**:
    - Collaborate with international counterparts to ensure consistent enforcement of neural data protection laws, particularly in global research and data transfer contexts.
5. **Engage with Stakeholders**:
    - Facilitate ongoing dialogue with researchers, industry players, civil society, and data subjects to ensure regulations remain relevant to emerging technologies and societal needs.

By adopting these measures, SDPAs can effectively safeguard individuals' rights and enhance trust in neurotechnologies.

7. RECOMMENDATIONS FOR MANUFACTURERS AND DATA CONTROLLERS

Manufacturers and data controllers hold critical responsibilities in ensuring that neurotechnologies are designed, developed, and deployed in ways that respect fundamental rights and comply with data protection laws, including Convention 108+. To achieve these goals, the following recommendations should guide their actions:

7.1. Human Rights-Centered Design

- **Embed human rights by design and by default**: Integrate privacy, mental autonomy, and other human rights protections into the design, development, and deployment of neurotechnologies.
- **Conduct Human Rights Impact Assessments (HRIAs)**: Perform HRIAs alongside Data Protection Impact Assessments (DPIAs) to assess and mitigate risks to mental privacy, dignity, and autonomy at every stage of product development.
- **Incorporate Explainable AI (XAI)**: Ensure AI systems used in neurotechnologies are explainable, allowing individuals, auditors, and regulators to understand how decisions are made and ensuring accountability for any outcomes.

7.2. Transparent and Ethical Data Practices

- **Establish robust transparency mechanisms**: Clearly inform users about how their neural data will be collected, processed, shared, and stored.
- **Ensure meaningful consent**: Obtain explicit, informed, and specific consent before processing neural data, with mechanisms for individuals to easily withdraw consent at any time.
- **Limit data collection**: Only collect neural data that is strictly necessary for the specified and legitimate purpose, adhering to the principles of necessity and proportionality.

7.3. Safeguarding Neural Data

- **Adopt state-of-the-art security measures**: Implement advanced cybersecurity protocols to prevent unauthorized access, breaches, or misuse of neural data. This includes data encryption, secure storage, and regular security audits.
- **Ensure data minimization and retention limits**: Retain neural data only for the duration necessary to achieve the intended purpose, with clear deletion protocols to prevent unnecessary retention or misuse.
- **Develop secure systems for cross-border data transfers**: Comply with Convention 108+ provisions and establish safeguards such as encryption or pseudonymization for neural data transferred across jurisdictions.

7.4. Oversight and Accountability Mechanisms

- **Establish internal governance frameworks**: Create dedicated governance teams or ethics committees to oversee compliance with data protection laws and human rights standards in neural data processing.
- **Conduct independent audits**: Engage third-party auditors to assess compliance with ethical standards, legal obligations, and technical safeguards.
- **Facilitate complaint mechanisms**: Develop accessible processes for individuals to lodge complaints regarding data processing and seek redress for violations of their rights.

7.5. Special Considerations for Vulnerable Populations

- **Implement enhanced safeguards**: Develop neurotechnologies with protections tailored to the needs of vulnerable populations, such as minors and individuals with cognitive impairments.
- **Avoid harmful applications**: Prohibit the use of neurotechnologies for neuromarketing, behavioral manipulation, or profiling that targets vulnerable groups without adequate safeguards.

7.6. Collaboration and Stakeholder Engagement

- **Engage with stakeholders**: Actively involve researchers, civil society, policymakers, and end users in the development process to ensure technologies align with societal values and ethical standards.
- **Promote interoperability and standards**: Work with industry and regulatory bodies to establish and adopt common technical and ethical standards for neural data processing.

7.7. Reporting and Accountability to Authorities

- **Provide detailed compliance reports**: Regularly report to supervisory authorities on data processing practices, including compliance with data protection laws and implementation of human rights safeguards.
- **Support oversight mechanisms**: Cooperate with external oversight bodies, such as supervisory data protection authorities (SDPAs), to ensure compliance and improve accountability.

8. ADDITIONAL RECOMMENDATIONS FOR FACILITATING NEUROSCIENCE RESEARCH AND INNOVATION

To ensure that data protection regulations support rather than hinder scientific progress and clinical advancements, the following recommendations are made:

• **Simplification of Ethical and Legal Procedures:** SDPAs should work closely with research institutions and clinical organizations to streamline ethical review and compliance procedures for neuroscience projects involving neural data. This includes developing standardized templates and processes to avoid delays.

• **Expedited Approval for Low-Risk Studies:** Implement fast-track approval mechanisms for studies using non-invasive neurotechnologies or anonymized neural data, provided that adequate safeguards are in place to protect privacy.

• **Researcher Support Programs:** Provide guidance and training for neuroscience researchers on data protection requirements to foster compliance without stifling innovation.

• **Clear Guidelines for Secondary Use of Data:** Establish clear frameworks for the secondary use of neural data in research to expand datasets for scientific discovery while respecting the original consent terms.

• **Collaboration with Research Stakeholders:** Facilitate dialogue between SDPAs, neuroscientists, and healthcare professionals to ensure that regulatory frameworks reflect the practical needs of neuroscience research and do not create unnecessary barriers.

• **Data Sharing Protocols:** Encourage the development of secure data-sharing platforms and protocols that allow neuroscience research institutions to collaborate while adhering to data protection standards.

Facilitation of Cross-Border Studies: Support cross-border neuroscience research by harmonizing data protection standards and promoting international agreements that enable secure data transfer while respecting privacy regulations. This includes establishing mutual recognition agreements for ethical approvals to prevent duplicate reviews.

• **Transparency and Public Trust:** Engage in public information campaigns to raise awareness about the societal benefits of neuroscience research, fostering public trust and participation.