COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

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

INDEX

to be drafted as a final step

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 the most intimate part 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 concerns the most intimate part of the human being, and is therefore 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 reaffirming existing human rights and data protections frameworks to address the novel issues posed by neural data in the digital age.

International instruments, such as the Council of Europe Convention for the Protection of Individuals with Regard to the Automatic 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 Automatic Processing of Personal Data, "Convention 108+"), safeguards 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 provides 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 characteristics of neural data require 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 to ensure 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, including the heightened sensitivity of such data, the risk of re-identification even from anonymized neural data, the need for that the processing of personal data is carried out for legitimate purposes, and the importance of implementing the purpose limitation principle in this context.

Convention 108+ emphasizes the importance of obtaining valid consent for personal data processing. However, the 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.

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 on how to comply with the provisions 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. 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 security measures, and appropriate oversight mechanisms.

While the processing of neural data shall 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 and that has been anonymized in an irreversible way fall outside the scope. 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 shall be interpreted in accordance with the provisions of the Convention 108+ and the documents on Interpretation of its provisions elaborated by the Committee.

- **"Personal data"** shall be understood as defined in Article 2(a) and covers any information relating to an identified or identifiable individual ("data subject").
- 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 and taking into account other data or meta data, reveal cognitive, emotional, or behavioral information and may include patterns linked to mental information such as regarding 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 **"implantable 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-implantable 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-implantable neurotechnologies may nevertheless be intrusive.
- The expression **"mental information"** refers to information relating to an individual's mental processes including but not limited to their thoughts, beliefs, preferences, emotions, memories, intentions and cognitive capacities. Such information may be derived from neural activity, as recorded through neurotechnologies, and may provide insights into mental states, mental health conditions, or other individual characteristics related to behavior, identity, or psychological well-being. Mental information may also be generated through non-neural sources, such as behavioral data, self-reported experiences, psychometric assessments, or data captured by wearable or ambient sensors. Even when not directly linked to brain activity, such information may reveal subjective experiences or internal cognitive states and shall therefore be treated with heightened protection where it is capable of identifying or inferring sensitive attributes of the data subject.
- The expression **"mental privacy"** refers to a specific dimension of the right to respect for private life, as protected under Article 8 of the European Convention on Human Rights and Article 5 of Convention 108+. It encompasses the protection of the individual's mental domain —including thoughts, emotions,

intentions, and other cognitive or affective states— against unlawful or non-consensual access, use, manipulation, or disclosure. The right to mental privacy implies that individuals must retain meaningful control over data and information that pertain to their inner mental life. This includes both direct representations (such as verbalized thoughts or declared preferences) and inferred mental content derived from neural data or behavioral signals. This right is of particular importance in the context of emerging neurotechnologies and artificial intelligence systems that enable the detection, inference, or alteration of neural activity and mental states. Any interference with mental privacy must comply with the principles of legality, necessity, and proportionality, and must pursue a legitimate aim in a democratic society , in line with established human rights jurisprudence. The protection of mental privacy serves to uphold related fundamental rights, including freedom of thought, freedom of expression, and the right to human dignity and mental integrity.

- The expression **healthy individuals** refers to persons who do not have a diagnosed medical or psychological condition for which the neurotechnology is used and who engage with such technologies for purposes including wellness, self-optimization, entertainment, education, or personal research.

2. Scope

[2.1. These Guidelines apply to the collection and processing of neural data in contexts falling both within and outside the health care and research sectors, in accordance with applicable domestic and international law.

2.2 “These Guidelines recall the existing legal obligations of States and other actors under international human rights law, in particular the duty to respect and ensure the rights enshrined in the European Convention on Human Rights and in Convention 108+. They provide guidance on the implementation of these obligations in the specific context of neural data processing, with a view to ensuring that such processing fully respects human dignity and safeguards the human rights and fundamental freedoms of every individual, including, in particular, the right to the protection of personal data.

2.3. These Guidelines are addressed to all relevant stakeholders involved in the design, development, deployment, and regulation of systems and technologies that involve the collection or processing of neural data. This includes but is not limited to: public authorities and policymakers, developers, manufacturers, and service providers of neurotechnologies and related AI systems, health care and research institutions, and any other actors processing neural data, whether in medical, commercial, educational, workplace, security, or other settings.

2.4 Neural data may be processed in a wide range of sectors, including health care, scientific research, education, employment, security, and commercial applications. These Guidelines apply irrespective of the sector, while recognizing that certain contexts—such as medical care or public health—may be governed by more specific legal regimes or sectoral safeguards under domestic or international law. Where neural data are processed in the context of health care, biomedical research, or for general public interest purposes, such processing shall comply not only with these

Guidelines but also with the applicable standards arising from relevant legal frameworks, including the Convention on Human Rights and Biomedicine (Oviedo Convention) and its additional protocols, as well as national legislation ensuring appropriate safeguards for the rights and freedoms of data subjects. These Guidelines do not override such existing safeguards but aim to complement them by addressing the specific risks and normative challenges associated with neural data, including those related to re-identification, cognitive manipulation, and the protection of mental integrity.

2.5. These Guidelines shall be without prejudice to more specific rules or higher safeguards that may apply under domestic law, including in sectors such as health, biomedical research, or law enforcement, provided such rules are consistent with the principles and rights enshrined in Convention 108+ and other relevant international human rights instruments.

2.6. 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 and “Convention 108+”.

3. Principles and Legitimacy of Neural Data Processing

3.1. General Principles

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. Being aware of the profound implications on individuals and society which may derive from the processing of neural data, 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, whether derived from implantable or non-implantable neurotechnologies, shall only be collected and processed in a manner that ensures full respect for the rights and fundamental freedoms of individuals, including the rights to privacy, data protection, mental integrity, and human dignity, as guaranteed under the European Convention on Human Rights and in accordance with Article 5 Convention 108+. The collection, storage, and processing of neural data must comply with the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. The collection and processing of neural data shall be carried in full respect of the rights and fundamental freedoms of the individual, as guaranteed by applicable international human rights law. Such legal grounds may include, where appropriate, the consent of the data subject, the performance of a contract, compliance with a legal obligation, the protection of vital interests, the performance of a task carried out in the public interest, or the legitimate interests of the controller or a third party, provided that the rights and freedoms of the data subject are not overridden.

3.1.3. Any processing must be accompanied by appropriate legal, organizational, and technical safeguards, as prescribed by law, in order to ensure the effective protection of human dignity, mental privacy, and the right to the protection of personal data.

3.1.4. In particular, where neural data are obtained from implantable neurotechnologies, their collection and processing shall be restricted to appropriately trained and authorized professionals, such as neuroscientists, medical practitioners, or duly designated personnel acting under their responsibility. These actors shall be subject to binding professional standards and legal obligations of confidentiality, equivalent to those applicable to health-care professionals, in order to ensure the lawful and ethical handling of such highly sensitive data.

3.1.5. Neural data derived from non-implantable neurotechnologies may be collected and processed by general users, including the data subjects themselves (such as patients, research participants, and healthy and non 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.
Such processing shall only occur where appropriate safeguards and legal guarantees have been implemented, in full compliance with the principles laid down in Convention 108+, in particular those concerning lawfulness, fairness, purpose limitation, data minimization, and data security. Given the highly sensitive nature of neural data, and the fact that such data may be processed by individuals who are not trained professionals, state-of-the-art security measures must be applied, in accordance with Article 7 of Convention 108+. These measures shall be designed to prevent unauthorized access, accidental or unlawful destruction, loss, misuse, alteration, or disclosure of neural data. They shall include technical and organizational safeguards tailored to consumer-grade devices and platforms. Furthermore, users must be adequately and clearly informed, in accessible and intelligible terms, about the potential implications of data collection, storage, analysis, and sharing. This includes information on the risks such processing may pose to the rights to privacy, mental integrity, and human dignity, particularly where profiling, behavioral inference, or third-party access are involved.

3.1.6. 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.

3.1.7. All processing of neural data must comply with the core principles of lawful and fair data processing as set out in Convention 108+ , including accuracy, security, and accountability. Measures should be tailored to the level of sensitivity and potential harm, ensuring that human rights are respected and protected throughout the entire data lifecycle.

3.1.8. The principles set out in these Guidelines apply to the use and development of neurotechnologies where personal data, including neural data, are processed—especially when individuals can be identified or re-identified.

3.2. Collection, Processing and Retention of Neural Data

Necessity and Proportionality

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.

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.

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.

3.2.1. Purpose limitation

Data shall not be processed for purposes that are unlawful, incompatible with the original purpose of collection, or disproportionate in relation to the intended objectives. 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.

A clear distinction shall be drawn between neural data processing for purposes of general public interest—such as medical care, public health, or scientific research—and for other purposes, including commercial use, user experience optimization, behavioral profiling, AI development, or entertainment. In the former case, legal and ethical frameworks should facilitate data use in accordance with established safeguards. In the latter, stricter legal limitations and enhanced safeguards must be applied, including risk assessments, independent oversight, and restrictions on re-use and third-party access.

Given the 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 to prevent unauthorized access, misuse, accidental exposure, or unlawful disclosure. These safeguards shall be proportionate to the risks involved and shall also ensure that data subjects are adequately informed—in a clear, accessible, and comprehensible manner—about the implications of data collection, storage, sharing, and analysis, particularly where such practices may interfere with their mental privacy or autonomy.

Where neural data are obtained from sources other than the data subject, this shall be permitted only when strictly necessary to achieve the legitimate purpose of the processing and where such collection remains consistent with all applicable principles set forth in these Guidelines. In accordance with the principle of purpose limitation under Article 5(4) of Convention 108+, neural data shall only be processed for specified, explicit, and legitimate purposes and shall not be further processed in a manner incompatible with those purposes. Moreover, personal data shall not be retained for longer than is necessary for the fulfilment of the original purpose. Once the purpose has been fulfilled, neural data must be securely archived, anonymized, or erased in accordance with applicable data retention, minimization, and disposal frameworks, ensuring continued compliance with the principles of integrity and confidentiality under Article 7 of Convention 108+.

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.

3.2.2. Direct Collection and Lawful Basis

Neural data shall, as a general rule, be collected directly from the data subject and only on a valid, legitimate, and lawful basis, in accordance with Article 5 of Convention 108+. The legal basis may include, as appropriate, the data subject's consent, compliance with legal obligations, protection of vital interests, or processing carried out in the public interest or in the exercise of official authority.

Neural data may be collected and processed only when a valid legal basis exists, in accordance with applicable domestic laws and with appropriate safeguard to protect human rights and fundamental freedoms. Processing may occur on one of the legal grounds provided by Article 5 of Convention 108+, depending on the purpose of the processing and the necessity of the data in the given context**:**

- **(a) Explicit and informed consent** – Neural data may be processed where the data subject has given their explicit, free, specific, informed and unambiguous consent for one or more specified purposes. In cases where the data subject is unable to provide such consent—such as individuals under guardianship, or those with reduced capacity—consent may be given by their legal representative or by an authority designated by law (such as a court or administrative body authorized to act in the best interests of the individual under applicable domestic legislation). In the case of minors, consent must be provided by a parent or another person holding parental authority or legal guardianship, in accordance with domestic law and with due regard for the evolving capacities and best interests of the child, as enshrined in Article 5 of the UN Convention on the Rights of the Child. This legal basis is particularly relevant for contexts where neural data processing is voluntary, such as in consumer neurotechnology applications, and not required by law or necessary for the performance of a task carried out in the public interest or the delivery of essential services.

- **(b) Medical and healthcare purposes** – Neural data may be processed for preventive medicine, diagnosis, the provision of care or treatment, or the development of medical neurotechnologies, provided that such processing is in the interest of the data subject and is carried out by a qualified professional or another person also subject to a legal obligation of professional confidentiality under domestic law. In such contexts, explicit consent may not be required where the processing is necessary for:
    - the provision of healthcare or medical treatment;
    - the management of health services;
    - or other tasks carried out in the public interest under the responsibility of a health authority, as authorized by domestic law in accordance with Article 6(2)(b) of Convention 108+.

    This applies, for example, in situations where:

    - the data subject is unconscious or otherwise unable to provide consent, but urgent medical intervention is required;
    - public health authorities process neural data to fulfil epidemiological, diagnostic, or safety-monitoring functions in accordance with statutory mandates;
    - consent cannot be freely or meaningfully given due to power asymmetries, e.g. in clinical trials, but other legal safeguards (including ethical review and purpose limitation) are in place.

All such processing must be carried out in accordance with the principles of necessity, proportionality, and data minimization, and must include appropriate legal and technical safeguards to protect the fundamental rights and freedoms of the data subject.

- **(c) Compliance with a legal obligation** – Processing of neural data may be lawful when it is required under domestic legislation for specific public interest purposes, such as the protection of public health, the fulfilment of epidemiological surveillance obligations, occupational safety, or other legally mandated purposes. In such cases, the legal obligation must be clearly defined, necessary in a democratic society, and proportionate to the aim pursued. The legal framework must include adequate safeguards to ensure compliance with Article 5 of Convention 108+ and protect against misuse or disproportionate impact on data subjects.
- **(d) Scientific research and statistical purposes** – Neural data may be processed for scientific research or statistical purposes where such processing is based on a valid legal basis in accordance with Article 5 of Convention 108+, and provided that appropriate safeguards are implemented pursuant to Article 9. While scientific research constitutes a legitimate purpose, it must be accompanied by a legal basis established in domestic law, which may include

the explicit and informed consent of the data subject, or, where recognized by law, processing carried out in the public interest or by a scientific institution acting under a legal mandate. Processing of neural data for research or statistical purposes should not be subject to disproportionate constraints where robust safeguards are in place. Such safeguards include the application of data minimization and purpose limitation principles, the implementation of technical and organizational measures such as pseudonymization or anonymization where feasible, and appropriate oversight mechanisms, including ethical review processes where required. The processing must not be used to make decisions affecting individual data subjects, nor to attempt re-identification, unless this is expressly authorized by law and subject to further justification and safeguards. In all cases, the research purpose must be clearly defined, the rights of data subjects must be respected, and measures must be taken to prevent any risk of misuse, discrimination, or undue interference with privacy.

- **(e) Protection of vital interests** – In strictly limited and exceptional circumstances neural data may be processed without the consent of the data subject where it is necessary to protect the life, physical integrity, or essential interests of the data subject or another person and where no other legal basis is available. This legal basis may apply in urgent medical situations or public emergencies, provided that processing remains proportionate, time-limited, and subject to accountability and review mechanisms under applicable law.

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.

However, paragraphs 1, 2, 3 and 4 of Article 5 of Convention 108+ are cumulative and must be respected in order to ensure the legitimacy of the data processing.

3.2.3. Retention and Disposition Policies

The retention of neural data must be strictly governed by the principles of necessity, proportionality, and purpose limitation, as enshrined in Article 5(4) and Article 6 of Convention 108+. Personal data permitting the identification of an individual shall not be retained for longer than is necessary for the fulfilment of the purpose for which they were collected and processed. Neural data must therefore be either securely erased, anonymized, or archived in a form not permitting identification once the purpose has been fulfilled or the legal retention period has expired. Any continued retention must be justified by a new legal basis and purpose that is compatible with the original one, in line with Article 5(4).

To promote consistency and accountability, States should establish common standards and procedures for data disposition, especially for highly sensitive categories such as neural data. The role of independent supervisory authorities, as defined in Article 15 of Convention 108+, is essential in overseeing the implementation of such standards and ensuring compliance with data protection obligations. Particular care shall be taken to prevent unnecessary retention, unlawful further processing, or any processing that is incompatible with the initial purpose, in order to safeguard the rights and freedoms of data subjects, including their mental privacy and integrity.

3.2.4. Inferences and Mental Privacy

While the collection and processing of neural data for clinical and scientific research purposes should be encouraged—provided that all applicable legal and ethical requirements are met—strict limitations and prohibitions apply to the inference of mental states such as emotions, memories, intentions, preferences, and other cognitive characteristics, in line with the principles of human dignity, mental integrity, and mental privacy.

Inferences about mental states shall be explicitly restricted in the following circumstances:

(a) Where such inferences are made without the explicit awareness and free, informed, and specific consent of the data subject, unless expressly authorized by domestic legislation for a legitimate and proportionate aim in a democratic society;

(b) Where such inferences are unrelated to the lawful and stated purpose for which the neural data were collected;

(c) Where such processing may result in profiling, coercive influence, psychological manipulation, discrimination, or unjustified surveillance of mental activity.

In particular, the use of neural data to infer highly sensitive mental attributes—such as political opinions, personal memories, religious or philosophical beliefs, unconscious biases, or other deeply intimate characteristics—shall be strictly limited to scientific or medical research contexts and only where subject to robust legal, ethical, and technical safeguards, including independent oversight and meaningful rights for data subjects.

Furthermore, particular attention shall be paid to the risks of inaccuracy, bias, and misinterpretation associated with neural inference technologies, especially where artificial intelligence or automated decision-making tools are employed. Developers and data controllers must implement rigorous validation protocols, independent oversight mechanisms, and transparent reporting practices to ensure that inferences are scientifically robust and that the cognitive privacy and dignity of individuals are effectively protected.

[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 neurodevelopmental characteristics, should benefit from appropriate protection, in line with paragraph 6 of Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data. 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 neural data concerning unborn children, provided that such decisions are made in accordance with the best interests of the future child, consistent with relevant human rights instruments and ethical standards. The recognition of the unborn child as a data subject and any associated data protection entitlements shall be determined in accordance with applicable legal frameworks. In all cases, particular attention shall be paid to ensuring that neural data concerning unborn children are not used for purposes that may result in discrimination, stigmatization, or unjustified predictive profiling, in line with the principles of purpose limitation, data minimization, and non-discrimination.]

3.2.6. Safeguards and Limitations of Specific Neural Data Processing

The processing of neural data shall be authorised where it poses no significant risk of harm to the data subjects and is accompanied by appropriate legal guarantees and safeguards, as required by Article 11.2 of Convention 108+. Such safeguards shall include independent oversight, privacy and/or human rights impact assessments, transparency and explainability measures, data minimisation, and access controls, in accordance with the guidance provided in the Explanatory Report to Convention 108+.

Neural data collected for purposes such as preventive care, diagnosis, therapeutic treatment, neurorehabilitation, or scientific research shall be used for those specified purposes or to enable the data subject to make free and informed decisions. Any further processing must be justified under a compatible purpose and supported by a separate legal basis and additional safeguards.

The processing of neural data for commercial, advertising, or marketing purposes shall be subject to strict limitations and may only be permitted where it is expressly authorized by law and consistent with the principles of lawfulness, fairness, transparency, and respect for human dignity and mental integrity. While some commercial applications—such as consumer brain-computer interfaces for entertainment, self-quantification, or cognitive training—may serve legitimate and non-exploitative purposes, such uses must be fully voluntary, transparent, and based on the informed and freely given consent of the data subject. In all such cases, the processing must be accompanied by appropriate safeguards, including purpose limitation, data minimization, and clear user control over data use and sharing. By contrast, the use of neural data to infer, manipulate, or exploit cognitive or emotional states for the purpose of influencing individuals through a rational or subliminal means—especially where such influence bypasses critical reasoning or targets psychological vulnerabilities—is incompatible with the rights to autonomy, mental privacy, and human dignity, and is prohibited under these Guidelines.

When processing neural data for commercial, advertising, or marketing purposes, even with the apparent consent of the data subject, appropriate safeguards -including privacy and/or human rights impact assessments- must be implemented. This requirement reflects the principle that consent cannot be considered valid where it is obtained under asymmetrical power dynamics, lacks informed understanding of neurodata implications, or is used to legitimize activities that are inherently incompatible with human dignity and mental integrity. Processing for such purposes poses unacceptable risks of commodification of cognitive functions, exploitation of psychological vulnerabilities, and the erosion of autonomy.

With regard to the processing of neural data for judicial or criminal investigations, these Guidelines recognize that the use of neural data in such domains raises serious ethical, legal, scientific, and human rights concerns, particularly due to the deeply intrusive nature of such data and its potential to undermine fair trial guarantees, the presumption of innocence, and the right to mental privacy. Furthermore, they include the risk of infringing the right against self-incrimination, as protected under Article 6 of the European Convention on Human Rights and relevant constitutional traditions across Council of Europe member states. Accordingly, the processing of neural data for law enforcement or criminal justice purposes shall be permitted only in strictly exceptional circumstances, where the following cumulative conditions are met:

- the processing is expressly provided for by law,
- it pursues a legitimate aim, such as the prevention of an imminent and serious threat to public security or the protection of life or bodily integrity,
- it is demonstrably necessary and proportionate in a democratic society,
- it is scientifically valid and based on substantive evidence,
- and it is subject to robust procedural safeguards, including judicial oversight, independent scientific validation, and strict purpose limitation.

Use cases could include the processing of neural data in proceedings where an individual’s neurological condition affects their legal capacity, or where informed, voluntary, and medically supervised consent is given for clinical assessments relevant to the administration of justice. However, the use of neural data for purposes such as deception detection, emotional analysis, or the profiling of cognitive traits in suspects or defendants—particularly where undertaken without the subject’s free and informed consent—is strictly prohibited. Such practices conflict with the principles of legality, human dignity, and mental integrity and present unacceptable risks of misuse.

One illustrative case is the use of Brain Electrical Oscillation Signature (BEOS) profiling in criminal investigations. This technique has been applied in police investigations, including cases involving serious crimes such as murder, rape, and terrorism. However, BEOS has not been subject to peer-reviewed validation consistent with international scientific standards, and the technology has not been independently replicated or verified. Use of such scientifically unproven methods in criminal investigations may violate fair trial guarantees and constitutes an unjustifiable intrusion into mental privacy. These Guidelines therefore emphasize that the use of neural data in criminal justice or policing is not supported, particularly in jurisdictions governed by the EU Charter of Fundamental Rights, where additional restrictions and safeguards under EU data protection law (including the EDPB Guidelines on facial recognition and biometric data) apply. In all cases, a precautionary approach must be taken to prevent the misuse of speculative neurotechnological tools in sensitive legal domains.

The following applications of neural data in judicial or criminal justice contexts are strictly prohibited under these Guidelines due to their incompatibility with fundamental rights, scientific standards, and the principles of legality and proportionality:

1. Profiling of cognitive, emotional, or psychological traits unrelated to the legal case – including generalized inferences about personality, temperament, or affective predispositions that are not directly relevant to the legal proceeding at hand.
2. Techniques that compel or infer mental content — such as thoughts, memories, intentions, or beliefs — in a manner that may coerce individuals into revealing information against their will, thereby infringing the right against self-incrimination and the right to freedom of thought.
3. Use of techniques that lack independent, peer-reviewed, and corroborated scientific evidence – including methods that have not undergone rigorous validation, reproducibility testing, or evaluation under established evidentiary standards, such as the Daubert or Frye criteria.
4. Techniques aimed at predicting an individual's proclivity or probability to commit or recommit a criminal offence in the future (commonly referred to as predictive policing) — such applications are incompatible with human dignity, mental autonomy, and the presumption of innocence, and may lead to discriminatory or disproportionate outcomes.

3.2.7. Predictive and High-Risk Profiling

The processing of neural data for predictive purposes shall be subject to strict legal, ethical, and scientific limitations. A clear distinction must be drawn between the legitimate use of predictive analysis in clinical or research settings, such as identifying early indicators neurological conditions to support diagnosis or treatment, and the processing of predictive profiling to assess behavioral tendencies or psychological traits in non-medical contexts.

In line with Article 11.2 of Convention 108+, predictive processing involving neural data may be permitted only under conditions set out by law for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when there is no recognizable risk of infringement of the rights and fundamental freedoms of data subjects and also under the following conditions:

a) it is expressly provided for by law;
b) it respects fundamental rights and freedoms;
c) it is necessary and proportionate in a democratic society;
d) and appropriate safeguards and guarantees are implemented, such as independent oversight, purpose limitation, data minimization, and strict access control.

Predictive uses of neural data must never be employed for generalized surveillance, coercion, or speculative profiling of individuals for law enforcement purposes. In particular, the processing of neural data for high-risk predictive profiling is strictly prohibited in the following cases:

- when used for generalized surveillance or speculative assessment of personality, behavior, or emotional states;
- when designed to predict an individual's future criminality or likelihood of reoffending (i.e. predictive policing);
- when based on scientifically unvalidated techniques, or when lacking peer-reviewed evidence and independent verification;
- when intended to infer or expose thoughts, beliefs, or preferences in ways that risk violating the right to freedom of thought or mental privacy;
- or when such profiling results in discrimination, particularly if used to deny access to employment, education, insurance, social services, or due process protections.

Particular care must be taken to ensure full compliance with the principle of non-discrimination, which prohibits any unjustified differential treatment based on neural or mental characteristics. The use of predictive systems that associate specific neural patterns with behavioral tendencies, levels of intelligence, political orientation, or emotional disposition risks reinforcing harmful stereotypes, deepening social inequalities, and excluding individuals from opportunities on the basis of opaque or scientifically unproven inferences. Discrimination based on inferred cognitive or psychological traits—especially in employment, education, social services, or criminal justice—constitutes a serious violation of human rights and is incompatible with democratic values and the rule of law. In all cases, regulators and data controllers must ensure that predictive applications involving neural data do not lead to unjustified restrictions on individual freedoms.

3.2.8. Safeguards during Neural Data Transfer

The global nature of neuroscience research and collaboration necessitates robust mechanisms to protect neural data during cross-border transfers.

Neural data transfers must comply with Art. 14 of Convention 108+ 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.

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.

A Party shall not, for the sole purpose of the protection of neural data, prohibit or subject to special authorization the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention 108+. Data transfers to jurisdictions without equivalent protections should be subject to reinforced safeguards and risk assessments to mitigate potential vulnerabilities.

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

- (a) The data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; or *b*. the specific interests of the data subject require it in the particular case; or *c*. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; or *d*. it constitutes a necessary and proportionate measure in a democratic society for freedom of expression. (Art. 14.4 Conv. 108+).

- (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.

Experts' proposal

3.2.9. Data Protection Impact Assessments (DPIA) in the context of Neural Data Processing

Neural data processing poses risks that require proactive data protection impact 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 privacy and human rights 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. Transparency of the Processing

3.3.1. 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. 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. 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.

3.3.2. 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., commercial, advertising, or marketing purposes, 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 according to Convention 108+, Art.8.

3.3.3. The data subject should be informed at the latest at the moment of collection. Where the neural data are not collected from the data subjects, the controller shall not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts. However, it is a good practice to notified the data subject 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.

3.3.4. 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.

3.3.5. 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 information such as affective or cognitive traits.

3.3.6. 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.

3.4. Consent and Individual Autonomy in Neural Data Processing

3.4.1. Core Principles of Consent

Consent is a fundamental safeguard in the context of neural data processing. It enables individuals to retain meaningful control over the collection, processing, and sharing of their neural data.

In the field of neurotechnologies, it is essential to distinguish between two forms of consent:

(A) Data protection consent refers to consent as a legal basis for processing personal data, as defined under Article 5(2) of Convention 108+. This form of consent must be freely given, specific, informed, and unambiguous, and must be revocable at any time without detriment to the data subject. It serves as one of several legitimate legal bases under data protection law, and applies in all contexts where personal data, including neural data, are processed.

(B)Medical consent, by contrast, relates to the individual's authorization to undergo a medical intervention, including neurodiagnostic or neurotherapeutic procedures. This form of consent is governed by international standards such as the Oviedo Convention on Human Rights and Biomedicine (Article 5), which requires that consent be given freely and informed, based on adequate information about the purpose, nature, consequences, and risks of the intervention.

While these two forms of consent may overlap in practice, they are conceptually and legally distinct. For example, a person may consent to a medical treatment involving a brain-computer interface (medical consent) while also needing to give explicit consent for the processing and secondary use of the neural data collected through that interface (data protection consent).

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;
- Unambiguous, 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.

In cases where consent cannot be relied upon—such as when processing is required by law, for public interest purposes, or to protect vital interests—the legal basis must be clearly established, and appropriate safeguards must be put in place, in line with the principles of necessity, proportionality, and data minimisation. Special attention must also be given to vulnerable individuals, such as persons with cognitive impairments or minors, to ensure that consent—whether for data protection or medical purposes—is given by legally authorised representatives and reflects the best interests of the individual.

3.4.2. Ensuring [Freely Given] 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. 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. Legitimate Basis for Neural Data Processing Beyond Consent

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.

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

1. The data subject's explicit, free, specific, informed, and unambiguous 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.

Neural Data is a special category of data under Convention 108+, Art. 6, because its processing could reveal sensitive information, that may include, directly or by inference, a person's health status, mental states, emotional responses, cognitive abilities, or even political opinions, religious beliefs, sexual orientation, or ethnic origin.

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 complies with Article 5.1, including the principles of lawfulness, fairness, transparency, necessity, proportionality, and balancing of interests.

In all such cases, data controllers must apply additional guarantees appropriate to the sensitivity and risk of harm. These may include: separate secure storage, strong encryption, strict access controls, logging and audit mechanisms, and purpose limitation. Such measures help ensure that the processing of neural data does not undermine fundamental rights or enable discriminatory or disproportionate outcomes.

3.6. Subsequent Processing

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.

3.7. Impact Assessments and Privacy by Design

3.7.1. Impact assessments must be conducted before implementation to evaluate the risks and ensure neural data collection remains proportionate to its stated purpose. Impact assessments should be conducted transparently and shared with relevant supervisory authorities to promote **accountability** and trust.

Particularly, and according to art. 10, Convention 108+ each Party shall provide that controllers and, where applicable, processors, examine the likely impact of intended neural data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

Moreover, each Party shall provide that controllers, and, where applicable, processors, implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

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.

3.7.2. 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. Fairness

3.9.1 Neural data must be processed fairly as outlined in Article 5, paragraph 4(a).

3.9.2. 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.

3.10. Accuracy

3.10.1. 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.

3.10.2. 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.

3.10.3. 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.

3.11 Security

3.11.1. Given the highly sensitive nature of neural data—which can reveal insights into an individual's thoughts, emotions, and cognitive processes—especially enhanced security measures and safeguards are necessary. As provided for by Article 7 of Convention 108+ appropriate security measures must be developed to protect neural data from risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal dat , recognizing the unique vulnerabilities associated with this type of information

3.11.2. 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.

3.11.3. To mitigate these risks, controllers and processors must implement appropriate technical and organisational measures in accordance with Convention 108 and 108+, ensuring protection throughout the data lifecycle. Unlawful access, theft, or disclosure of neural data can lead to significant harms, including harassment, persecution, fraud, or identity theft. The need for enhanced safeguards is particularly critical when decoding techniques could intrude into the mental domain.

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

i. Data minimization by design, ensuring systems collect only the neural data strictly necessary for the specified purpose;

ii. Comprehensive risk assessment and mitigation, addressing both technical vulnerabilities and impacts on rights and freedoms;

iii. Access control and encryption, applying stringent policies and technical protections to restrict data access and secure data in transit and at rest;

iv. Incident response planning, including breach notification procedures and remedial measures;
Regular testing and review of security measures, including effectiveness checks, vulnerability reporting mechanisms, and corrective actions

Third-party protection, including safeguards against external tracking and disclosures of applicable liability frameworks.

3.11.5. Regulatory frameworks and internal governance policies should be adaptable and evidence-based, supporting innovation while maintaining high standards of data protection. Legal and policy responses must be tailored to the specific risk profile of each application and reviewed regularly to remain effective in the face of evolving technologies.

3.11.16. Controllers must carry out detailed risk assessments before initiating processing activities involving neural data. These assessments must identify any potential impacts on individuals and groups, and demonstrate that processing is necessary, proportionate, and justified in light of the intended purpose.

3.12. Accountability

3.12.1. Core Principles of Accountability

Accountability is a foundational principle of Convention 108+ , requiring data controllers and, where applicable, processors, to demonstrate compliance with data protection obligations. In the context of neural data, is especially critical due to the data's sensitivity, potential for inference of mental states, and heightened risks to privacy, dignity, and equality. Organizations nvolved in the development and deployment of neurotechnologies must embed accountability throughout the data lifecycle. This includes adopting structured governance, conducting regular risk and rights assessments, and ensuring that protective measures are not only implemented but documented, reviewed, and verifiable.

3.12.2. Key Actions to Ensure Accountability

To meet these obligations, the following measures should be adopted:

1. Human Rights Commitment and Risk Assessment: Organizations should publicly commit to a human rights-based approach to neural data governance. This includes conducting and publishing Human Rights Impact Assessments (HRIAs) at key stages—from research to deployment—clearly demonstrating how potential harms are identified and mitigated.
2. Stakeholder Engagement and Inclusion: Meaningful engagement with affected individuals, communities, experts, and civil society must inform development.

Feedback mechanisms should be documented and integrated into design and governance processes.

3. Policies, Procedures, and Ethical Governance: Organizations must adopt clear internal policies on human rights, data protection, and non-discrimination. Oversight bodies—such as ethics committees—should ensure these policies are implemented and updated.
4. Transparency and Explainability: Clear, accessible information must be provided on data subjects' rights and how their neural data are used. Where AI is involved, systems must be designed with explainability (XAI) in mind, offering understandable justifications for decisions and enabling detection of bias or error.
5. Training and Capacity Building: All personnel involved in neural data processing should receive regular training on data protection, ethical risks, and relevant legal standards.
6. Auditing, Monitoring, and Independent Oversight: Organizations should conduct regular audits and enable independent reviews of neurotechnological systems. Findings must lead to concrete corrective actions. Where appropriate, public reporting should be encouraged to promote trust and transparency.
7. Redress and Complaint Mechanisms: Effective procedures must be in place for individuals to seek redress for rights violations. These mechanisms should be easily accessible, responsive, and transparent in their operation.
8. Procurement and Vendor Due Diligence: Human rights criteria must be embedded in procurement processes. Vendors should be required to demonstrate compliance, including through HRIA reporting, with ongoing monitoring throughout the contract lifecycle.

3.12.3. 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.

3.13. Special Protections for Minors and Vulnerable Groups

3.13.1. Minors and vulnerable groups face unique risks when interacting with neurotechnologies due to their evolving cognitive capacities, increased susceptibility to influence, and, in many cases, limited ability to assess complex risks. These groups therefore require heightened legal and ethical protections.

3.13.2. In children and adolescents, the plasticity of the developing brain can magnify the impact of neurotechnologies. These tools may influence identity formation, autonomy, and decision-making, and could foster dependency or mental health vulnerabilities. The widespread adoption of brain-computer interfaces in consumer contexts—such as gaming or education—raises additional concerns about long-term psychological and cognitive effects.

3.13.3. Neurotechnologies that infer or manipulate mental states present risks to mental and physical integrity. Particularly concerning are commercial applications, including neuromarketing or profiling, which may exploit children's attention, emotions, or developmental traits. Such practices prioritize commercial objectives over the welfare of the child and must be strictly prohibited.

3.13.4. In educational settings, neurotechnologies must meet high standards of scientific validity, ethical justification, and privacy protection. Special care must be taken to ensure informed consent is meaningful and age-appropriate. Both children and their guardians may lack full understanding of the implications, and therefore safeguards must extend beyond formal consent to include continuous oversight and support.

3.13.5. Parental expectations around cognitive enhancement technologies can lead to the premature or coercive use of neurotechnologies on children. Clear regulatory guidance is needed to prevent undue pressure on children and to ensure that the best interests of the child remain the primary consideration.

3.13.6. To uphold children's rights and protect their cognitive and emotional development, the following safeguards should be implemented:

i. Informed Consent and Assent: Legal guardians must provide explicit, informed consent for neural data collection or processing involving minors. Additionally, minors should be given the opportunity to provide age-appropriate assent, ensuring their voluntary participation.

ii. Age-Appropriate Design and Communication: Neurotechnologies must be tailored to the child's age and developmental level, with information provided in formats understandable to both minors and their caregivers. Non-invasive technologies should be favoured where possible.

iii. Prohibition of Harmful Practices: The use of neurotechnologies for purposes such as neuromarketing, behavioural manipulation, or identity interference must be legally prohibited. Processing that may undermine children's autonomy, mental privacy, or well-being is incompatible with their rights.

3.13.7. Vulnerable adults—including those with cognitive impairments, mental health issues, or limited decision-making capacity—require reinforced safeguards when interacting with neurotechnologies. These individuals may be more susceptible to coercion, undue influence, or exploitation, particularly when technologies are presented as therapeutic or assistive. Informed consent must be a cornerstone of such protections. Data controllers must ensure that consent is genuinely informed, freely given, and adapted to the individual's cognitive and communicative abilities. Where decision-making capacity is diminished, safeguards must be in place to verify understanding and voluntariness. Supported decision-making frameworks should be prioritised, and substitute decision-making should be used only when strictly necessary and in accordance with applicable human rights standards.

3.13.8. When processing neural data from individuals with conditions such as dementia, Alzheimer’s disease, or other forms of cognitive disability, heightened vigilance is required to ensure that mental privacy is respected and that data are not used in ways that could be harmful, exploitative, or discriminatory. Tailored consent processes should be developed, which may include the involvement of caretakers or legally authorised representatives, while always seeking to respect the individual's will and preferences as far as possible. In all cases, the processing of neural data involving vulnerable adults must meet the standards of necessity, proportionality, and risk minimisation. These protections are not only ethical imperatives but legal obligations under data protection and human rights frameworks.

3.14. Supervisory Authorities

Under Article 15 of Convention 108+ each Party shall ensure the establishment of one or more independent authorities responsible for monitoring and ensuring compliance with the provisions of this Convention. Given the complexity and sensitivity of neural data processing, Parties must ensure that these Supervisory Authorities are equipped with the material, technical, and human resources necessary to carry out their oversight functions effectively, particularly in relation to neurotechnologies.

In exercising their mandate, Supervisory Authorities should pay specific attention to the following areas:

1. Protection of Mental Privacy
   Authorities must ensure that the collection and processing of neural data does not infringe on individuals' right to mental privacy. This includes heightened oversight over applications involving biometric identification, emotional inference, and cognitive profiling, which present elevated risks of misuse, manipulation, or psychological harm.
2. Enforcement of Consent and Purpose Limitation
   Supervisory bodies must verify that informed, freely given, and specific consent is obtained prior to the processing of neural data and that processing activities remain strictly limited to the legitimate purposes stated at the time of collection. Any deviation must trigger compliance review and potential remedial action.
3. Oversight of Special Categories of Neural Data
   Where neural data qualifies as a special category of personal data under Article 6 of Convention 108+—for example, when it relates to health, biometric identity, or other sensitive dimensions—authorities must ensure that processing is subject to appropriate legal bases and enhanced safeguards, including access controls, risk assessment, and minimisation obligations.

3.15. Exceptions

In limited and clearly defined circumstances, exceptions to data protection principles may apply under Article 11 of Convention 108+. Such exceptions must be interpreted narrowly, applied only when strictly necessary, and subject to proportionality and robust safeguards, to ensure that the essential protections afforded to individuals are not undermined.

3.16. Derogations

Derogations from Principles included in this Guidelines may be made according to exceptions established in Convention 108+ (Art.11) particularly in the following cases and taking into account that the derogation respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic:

a. Information to the data subject may be restricted if the derogation is provided for by law:

  - **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 when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects, 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.]

3.17. Oversight and Accountability

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, in 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, data 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

Under Article 9 of Convention 108+ all individuals, regardless of citizenship, nationality, or residency status, are entitled to a core set of rights regarding the processing of their personal data. These rights are fully applicable in the context of processing neural data, which often involves sensitive inferences about a person's mental states, identity, and autonomy. Any restriction of these rights must comply with Article 11 and meet the requirements of necessity, proportionality, and legitimate aim in a democratic society, while respecting the essence of fundamental rights and freedoms.

To ensure meaningful and enforceable rights in the context of neurotechnologies, the following rights must be legally guaranteed and operationalized through appropriate procedures and technical design:

1. **Right to Information**: Individuals must be clearly and accessibly informed about:

- The purpose and legal basis for collecting and processing their neural data;
- The categories of neural data processed and the entities accessing or receiving them;
- The expected retention period or criteria for storage;

- The use of automated processing or decision-making;
- Their rights under applicable law, and how to exercise them.

Information must be provided in clear, age- and culturally appropriate formats, ensuring full transparency and fairness.

2. **Right of Access**: Individuals have the right to:

- Confirm whether their neural data is being processed;
- Access a copy of their neural data, where technologically feasible, free of charge.

3. **Right to Rectification**: Inaccurate, outdated, or misleading neural data must be corrected without undue delay, upon request by the individual.

4. **Right to Erasure**: Individuals can request deletion of their neural data if:

- The processing is unlawful or no longer necessary;
- Consent is withdrawn and there is no other legal basis;
- The data were collected in violation of data protection principles.

If a controller refuses erasure, remedies must be made available, including complaint and appeal mechanisms.

5. **Right to Restrict Processing**:

Individuals may request the temporary suspension or restriction of their neural data processing in specific contexts, such as:

- Pending verification of accuracy;
- During an objection process;
- When processing is unlawful but erasure is not requested.

6. **Right to Object**: Data subjects may object to processing where:

- Processing is based on legitimate interest or public interest;
- The objection is grounded in their personal circumstances;
- Their rights and freedoms outweigh the controller's interest.

This includes the right to object to neuromarketing, behavioural profiling, or manipulation.

7. **Right to Not Be Subject to Automated Decisions**: Individuals must not be subject to decisions with legal or similarly significant effects based solely on automated processing of neural data, including profiling, unless:

- Explicit consent is given;
- Necessary for a contract or legal obligation;
- Safeguards are in place (e.g. human intervention, appeal mechanisms)

8. **Right to Explanation**:

Where automated decision-making is used, individuals have the right to a meaningful explanation of:

- The logic, significance, and intended effects of the processing;
- The data inputs, model assumptions, and interpretability standards applied.

9. **Right to Judicial and Non-Judicial Remedies**: In line with Article 12 of Convention 108+ individuals must have access to effective judicial and non-judicial remedies where their rights have been infringed. These should include redress, compensation, and the right to challenge unlawful processing.

10. **Right to Complaint:** Every individual has the right to lodge a complaint with a supervisory authority if they believe that the processing of their neural data violates applicable law or these Guidelines.

11 Right to Neural Data Portability: Individuals should be able to obtain and transfer their neural data in a structured, machine-readable format. Neurotechnologies must be designed to enable this right without compromising data security or mental privacy.

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.

To that end, policy makers should:

1. Establish Clear, Rights-Based Objectives
    - Define evidence-based, legitimate, and proportionate objectives for neurotechnologies aligned with public interest.
    - Adopt a human-rights-centred national strategy that prioritises dignity, autonomy, mental privacy, and non-discrimination.
2. Regulate Neural Data Processing
    - Clearly specify in law that the processing of neural data is only permitted for legitimate, specific, and lawful purposes.
    - Establish robust safeguards for neural data, recognising it as a special category of personal data subject to Article 6 of Convention 108+.
3. Strengthen Consent and Impact Assessment Requirements
    - Require that consent for neural data processing is informed, explicit, and freely given, with specific protections for minors and vulnerable individuals.
    - Extend Data Protection Impact Assessments (DPIAs) to include Human Rights Impact Assessments (HRIAs), with particular attention to cognitive and mental risks (e.g. via a Mental Data Protection Impact Assessment – MDPIA).
4. Embed Privacy and Human Rights by Design
    - Mandate the integration of privacy and human rights considerations into the design, deployment, and life cycle of neurotechnologies, following Article 10 of Convention 108+.
5. Promote Transparency, Oversight, and Accountability
    - Establish independent oversight bodies with powers to audit, investigate, and enforce compliance.
    - Create regulatory forums for cooperation between data protection authorities, bioethics bodies, and other relevant institutions.
    - Require stakeholder engagement at all stages of policy development, and publish consultation outcomes to ensure transparency and trust.
6. Guarantee Redress and Enforcement Mechanisms
    - Ensure civil and judicial remedies are accessible to individuals whose neural data rights have been violated.
    - Provide channels for individuals to lodge complaints and receive timely, meaningful redress.
7. Mitigate Harm and Enhance Security
    - Develop proactive risk mitigation strategies, including breach notification requirements and incident response plans.
    - Set clear rules for neural data retention, ensuring time limits, purpose restrictions, and secure disposal practices.

8. Protect Minors and Vulnerable Adults

- Prohibit neuromarketing, behavioural profiling, or manipulative uses targeting children or persons with cognitive impairments.
- Require ethical reviews and age-appropriate consent/assent procedures for research or commercial use involving minors.
- Introduce special safeguards for vulnerable adults, ensuring that consent is genuinely informed and freely given, with support for decision-making where needed.

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+.
Core responsibilities:

□ Consultative Role in Law and Policy
Under Article 15(3) of Convention 108+, Parties are obliged to consult SDPAs on legislative or administrative measures relating to personal data. SDPAs must be engaged from the earliest stages of neurotechnology-related policymaking to ensure fundamental rights are embedded by design.

□ Opinion-Giving and Regulatory Guidance
SDPAs should issue expert opinions on neural data processing operations that pose high risks, particularly regarding mental privacy, automated profiling, and biometrics. These opinions may inform national legislation or sectoral codes of practice.

□ Awareness Raising and Public Engagement
SDPAs must proactively inform the public of their role, responsibilities, and activities in the neurotechnology domain. This includes publishing reports, guidance documents, and engaging in media outreach to promote understanding and trust.

□ Stakeholder Collaboration
SDPAs should cooperate with researchers, developers, civil society, and vulnerable communities to ensure evolving practices in neurotechnology remain rights-respecting and socially legitimate.

□ Participation in Human Rights Impact Assessments
SDPAs should support or co-lead Human Rights Impact Assessments (HRIAs), including expanded Mental Data Protection Impact Assessments (MDPIAs), to ensure comprehensive risk evaluation and mitigation in neurotechnology design and deployment.

□ Regulatory Forums and Best Practices
Participation in national and international forums—alongside other regulators and

expert bodies—should be prioritised to coordinate enforcement strategies and share evolving best practices.

 Independent Oversight of Neural Data Processing
SDPAs must retain the ability to conduct independent audits and investigations into neurotechnologies. Their independence must be institutionally and financially protected to maintain objectivity and public trust.

Institutional Strengthening Priorities

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 Operational 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. **Facilitate inclusive dialogue**: Establish structured mechanisms to engage with relevant stakeholders, particularly vulnerable populations and underrepresented groups, to ensure responsive and inclusive regulation.

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+. The following recommendations support responsible innovation and legal compliance throughout the lifecycle of neurotechnological systems:

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.
- **Apply data minimisation**: 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.
- **Define 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.
- **Ensure compliant cross-border data transfers**: Apply Convention 108+ principles to international data flows, using encryption or pseudonymisation where required..

7.4. Oversight and Internal Accountability

- **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.
- **Develop accessible complaints procedures** for individuals to lodge complaints regarding data processing and seek redress for violations of their rights.

7.5. Special Protections for Vulnerable Populations

- Implement tailored safeguards for minors, persons with cognitive impairments, and other vulnerable groups, including simplified information, consent support, and strict profiling limits.

- Prohibit harmful applications, such as neuromarketing, behavioural manipulation, or covert profiling of vulnerable individuals without rigorous safeguards and legal basis.

7.6. Collaboration and Standard Setting

- **Engage with stakeholders**: Involve civil society, researchers, affected communities, and policymakers throughout development and deployment phases.
- **Support ethical and technical standardisation**: romote interoperability and alignment with international frameworks governing neural data and AI ethics.

7.7. Regulatory Cooperation and Reporting

Submit regular compliance reports to supervisory data protection authorities (SDPAs), detailing processing operations, safeguards, and human rights assessments.

Facilitate regulatory oversight by cooperating with national and international regulators and integrating findings into system improvements.

8. [ADDITIONAL RECOMMENDATIONS FOR FACILITATING NEUROSCIENCE RESEARCH AND INNOVATION

Neuroscience research offers substantial societal and medical benefits. To ensure that data protection regulations enable innovation without compromising individual rights, policy frameworks should actively support responsible research practices, especially in projects involving neural data.

The following recommendations aim to create a balanced, enabling environment for neuroscience research:

• **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-implantable 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.]