Elements of valid informed consent

Abstract

This document provides a structured framework for gaining informed consent from individuals before using their copyright works (including posts, articles, or comments), Name, Image, Likeness (NIL), or other Personal Data, in a engineered system.

1. Scope

This document provides a structured framework, aligned with best current practice, for gaining informed consent from individuals before using their copyright works (including posts, articles, or comments), Name, Image, Likeness (NIL), or other Personal Data, in a engineered system.

'Engineered system' includes (but is not limited to) the training of AI/ML technologies or systems.

Depending on your jurisdiction, the citizenship of the person who's data you is processing, and the type of organisation you are, there are potentially a number of alternative routes available for processing copyright works, NIL data, and personal data, other than by obtaining informed consent. Examples include US first amendment, US fair use, UK/EU fair dealing, and legitimate use. This document only concerns itself with the informed consent route.

The eleven elements of Informed Consent provided below are sourced from ISO/IEC 29100 and the EU General Data Protection Regulation (GDPR). For GDPR the main requirements are to be found in Article 4(11). The Article 29 Working Party provides further detail in chapters 2 and 3[1,2,3].

This document is also of use to those using the NIST RMF framework and wishing to pursue an informed consent route. It acts as a companion to that framework by providing detailed guidance on the essential elements of informed consent.

This document is applicable in any context where informed consent is sought from individuals for the use of their intellectual property, personal data, or identity in engineered systems. The process of seeking informed consent might be written, electronic, online, or recorded.

[1] https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf
[2] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf
[3] See Appendix

2. References

Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382, *Information technology — Vocabulary*
ISO/IEC 5207, *Information technology — Data usage — Terminology and use cases*
ISO/IEC TR 5469, *Artificial intelligence — Functional safety and AI systems*
ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*
ISO/IEC 29184, *Information technology — Security techniques — Online privacy notices*
ISO/IEC 27701, *Information technology — Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*
ISO/IEC 42001, *Information technology — Artificial intelligence — Management system*

Other references

Other ISO documents that touch on consent and should or could reference this document:

ISO 8000-8, *Data Quality*
ISO 9001, *Quality Management Systems*
ISO 9241-210 and **9241-220**, *Ergonomics of Human-System Interaction*
ISO 14001, *Environmental management systems*
ISO/IEC 19795-1, *Biometric performance testing and reporting*
ISO 20252, *Market, opinion, and social research*
ISO 20400, *Sustainable procurement*
ISO/IEC 22989, *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*
ISO/IEC 23894, *Guidance for AI ethical considerations*
ISO/IEC TR 24028, *Trustworthiness in AI*
ISO/IEC 25064, *Usability: User Needs and Requirements*
ISO 26000, *Social Responsibility*
ISO 26262, *Functional safety for road vehicles*
ISO/IEC 27001, *Information Security Management*
ISO/IEC 27002, *Code of Practice for Information Security*
ISO/IEC 27018, *Protection of Personal Data in the Cloud*
ISO/IEC 27550, *Privacy Engineering*
ISO/IEC 29134, *Privacy Impact Assessment (PIA) Guidelines*
ISO/IEC 29151, *Code of Practice for PII Protection*
ISO/IEC TS 29188-1, *Digital Advertising*
ISO 31000, *Risk Management*
ISO 37001, *Anti-Bribery Management Systems*
ISO/IEC 38507, *Governance of IT: Artificial Intelligence*
ISO 45001, *Occupational health and safety management systems*
ISO/IEC 27555, *Guidelines for privacy-enhancing data de-identification*

Healthcare, medical devices, clinical trials and health research

This document does not include best practice from the healthcare, medical devices, clinical trials, and health research fields. The standards listed below, rather than this document, are currently considered the best source for guidance and recommendations on Informed Consent in those contexts.

ISO 11673, *Clinical Laboratory Testing and In Vitro Diagnostic Test Systems* – Provides requirements for Informed Consent in these scenarios.

ISO 14155, *Clinical Investigation of Medical Devices for Human Subjects* – Provides detailed requirements for Informed Consent in clinical investigations.

ISO 14971, *Application of Risk Management to Medical Devices* – References Informed Consent in relation to the disclosure of risks to patients and users

ISO 20417, *Information to Be Supplied by the Manufacturer of Medical Devices* – Stresses obtaining Informed Consent where clinical testing is involved.

ISO 22367, *Medical Laboratories: Reduction of Errors* – Covers ethical practices in medical labs, including obtaining Informed Consent for diagnostic or research purposes.

3. Terms and definitions

3.1 Name, Image, and Likeness (NIL)

A natural person's personal attributes and forms of representation that capture an individual's identity such as their name, photograph, signature, voice, linguistic information, emotional tone, cultural background and nuances, regional variations, gait, gestures, mannerisms, personal expressions, behaviours, the sign language they use, the way they sign, or other personal characteristics and attributes associated with their identity.

3.2 Agency

The capacity of individuals to act independently and make their own free choices. It emphasizes the ability to control and manage one's own actions and decisions, particularly regarding how one's Name, Image, and Likeness (NIL) are represented and used.

3.3 Personal Data

Personal Data as defined in Regulation (EU) 2016/679 General Data Protection Regulation ("GDPR") Article4(1): "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (see alternatively ISO 24620-5, 3.2 and 3.6)

3.4 Engineered system

One or more of:

- *An **IT system** (ISO/IEC 2382, 3.8.8),*
- *the **training** (ISO/IEC 22989, 3.3.15) of an **AI system** (3.5),*
- *the **training** (ISO/IEC 22989, 3.3.15) of technology used to implement an **AI model** (ISO/IEC TR 5469. 3.16).*

3.5 AI system

*An **IT system** (ISO/IEC 2382, 3.8.8) "that generates outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives.*

*Note 1 to entry: The IT system can use various techniques and approaches related to **artificial intelligence** (ISO/IEC 2382, 3.1.3) to develop a **model** (ISO/IEC 2382, 3.1.23) to represent **data** (ISO/IEC 5207, 3.2), **knowledge** (ISO/IEC 2382, 3.1.21), processes, etc. which can be used to conduct **tasks** (ISO/IEC 2382, 3.1.35).*

*Note 2 to entry: AI systems are designed to operate with varying levels of **automation** (ISO/IEC 2382, 3.1.7)."*

(Source: ISO/IEC 22989, 3.1.4, modified)

4. The elements of valid informed consent

Informed consent must include these eleven elements to be valid:

- **Language:** Ensure that all communications with the individual (including, but not limited to, transparency of processes, consent, withdrawal of consent, questions and answers, and redress) are conducted in the individuals' preferred language[4].
- **Clear Communication**: Provide clear, specific, accessible, and comprehensive information about the nature of the action, use of data, or representation, including its purpose, scope, how it will be stored and protected.
- **Potential Risks:** Provide clear, specific, accessible, and comprehensive information about risks, benefits, and potential consequences.
- **Transparency**: Explain the processes involved, how the information will be used, who will have access to it, who controls and is responsible and accountable for the information, how long it will be retained. Be transparent about any reuses and possible future uses.
- **Competence**: Ensure that the individual giving consent is capable of understanding the information provided, including their rights and the implications of their consent. This may require age-appropriate or culturally sensitive explanations. For minors, dual-layer consent is essential[5].
- **Agency & Control**: Recognize and respect an individual's right to control and monetize how their data and likeness (NIL) are represented and used. This element supports individual agency by allowing people to retain control over their emotional, financial, and reputational wellbeing.
- **Voluntariness**: Make sure that consent is given unambiguously and voluntarily, without coercion, pressure, or manipulation, allowing individuals to make a free and informed choice.
- **Opportunity for Questions**: Give individuals the chance to ask questions and seek clarification to ensure they fully understand the terms and implications before consenting.
- **Right to Withdraw**: Inform individuals that they have the right to withdraw their consent at any time and explain the process for doing so without any negative consequences.
- **Documented & Traceable**: Inform individuals that written, electronic, or recorded consent, depending on the context, is formally secured and documented to ensure that there is a verifiable record that informed consent has been provided[6]. This documentation serves as both a safeguard for individuals' rights and an accountability measure for the organization, ensuring that consent is transparent and traceable.
- **Periodic Review**: Inform individuals that for long-term projects or ongoing data usage, renewed consent will be sought periodically to confirm the individuals' continued agreement under the same or updated terms[7].

[4] Discrimination based on language is prohibited under various international, regional, and national legal frameworks (e.g. national laws enactments of treaties and charters such as Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, EU Charter of Fundamental Rights, and American Convention on Human Rights). Ensuring that individuals receive consent information in their preferred language could be considered a reasonable accommodation to prevent discrimination, especially if language barriers are a factor of ethnicity, nationality, or other protected characteristics.

[5] Where consent is sought from a minor, including in education and child welfare scenarios, this document should be read in conjunction with the dual-layer consent (guardian and child) requirements and guidelines of ISO/IEC 29134, *Privacy Impact Assessment (PIA) Guidelines*.

[6] ISO/IEC 27701 provides one way for organisations to achieve the documentation and auditability requirement.

[7] ISO/IEC 27701 provides one way for organisations to achieve this.

Ethical considerations

This document recommends aligning with broader ethical guidelines (such as ISO 14155 for clinical research) when involving humans in testing.

Human rights considerations

This standard aligns with international human rights frameworks, such as the UN Guiding Principles on Business and Human Rights, which emphasize informed consent as a key component of respecting human rights in business practices.

Appendix

The principles from ISO/IEC 29100 (clause 5.1) are basically explained in 11 bullets as:

1. Consent and choice
2. Purpose, legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance

For GDPR, the Article 29 Working Party provides further detail in chapters 2 and 3[8,9] that the consent of the data subject must include the following elements:

- voluntary (consent is freely given),
- specific,
- informed,
- unambiguous (a clear affirmative action or unambiguous statement by the data subject agreeing to data processing), and
- documented and auditable

Informed means:

- information is clearly communicated,
- understandable (data subject is competent),
- transparent, and
- opportunities for questions are provided

For consent to be informed, the following additional information about must also be provided:

- controller's identity,
- purposes for, and uses of, the data,
- what (type of) data will be collected and used,
- the right to withdraw consent,
- potential risks, and
- how data will be stored and protected.

Article 5(1)(a): Fairness is an overarching principle, which requires that personal data may not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject.

[8] https://iapp.org/media/pdf/resource_center/20180416_Article29WPGuidelinesonConsent_publishpdf.pdf
[9] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

	ISO/IEC 29100											GDPR														
Elements of valid Informed Consent	Consent and Choice	Purpose, Legitimacy and Specification	Collection Limitation	Data Minimization	Use, Retention and Disclosure Limitation	Accuracy and Quality	Openness, Transparency and Notice	Individual Participation and Access	Accountability	Information Security	Privacy Compliance	Freely Given	Specific	Informed	Clear Affirmative Action	Clear Communication	Understandable	Transparent	Controller's Identity	Purpose and Use	Type of Data	Right to Withdraw	Potential Risks	Storage and Protection	Opportunity for Questions	Documentation
Language	✓						✓							✓		✓	✓	✓								
Clear Communication	✓	✓	✓	✓	✓	✓	✓	✓		✓			✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Potential Risks							✓							✓				✓				✓	✓			
Transparency		✓			✓		✓	✓	✓					✓				✓	✓	✓	✓	✓	✓	✓		
Competence	✓					✓		✓	✓					✓		✓	✓	✓				✓	✓		✓	
Voluntariness	✓							✓				✓		✓								✓				
Opportunity for Questions	✓							✓						✓				✓				✓			✓	
Right to Withdraw	✓							✓						✓				✓				✓				
Documentation									✓	✓	✓				✓									✓		✓
Periodic Review		✓			✓				✓		✓															✓

Mapping between the 10/11 elements of this document and the elements enumerated in ISO/IEC 29100 and GDPR