**RESPONSIBLE INNOVATION. CONFIDENTIALITY, PRIVACY AND DATA PROTECTION**

**Daniela Duță**

PhD. candidate, Institute of Legal Research „Acad. Andrei Rădulescu” of the Romanian Academy

*Abstract: In the era of technology, artificial intelligence and digitalization, responsible development and innovation are more important than ever. Confidentiality, privacy and data protection are important aspects of responsible innovation. These refer to individuals' right to protect their personal information and have control over how it is collected, stored and used, starting with the moment of conception and, implicitly, throughout the lifetime of the resulted technological product.*

*To promote responsible innovation, it is important for technology developers to implement appropriate security and data protection measures and to comply with applicable legislation. This can help develop technologies that are beneficial to society and individuals while protecting the fundamental rights and freedoms of users.*

*In addition to complying with data protection regulations, transparency and user’s information, security, data minimization/anonymization and privacy impact assessment, what other aspects should be considered for responsible innovation?*

***Key words: artificial intelligence, confidentiality, privacy, data protection, fundamental rights, security***

1. **Introduction**

In the current age of rapid technological advancement, responsible development and innovation are more important than ever. As technology continues to transform every aspect of our lives, it is essential to ensure that this transformation is done ethically and with responsibility. The present research represents an overview of the concept of responsible innovation and its importance in the current era of technology, artificial intelligence and digitalization and the importance of confidentiality, privacy and data protection in responsible innovation.

Increasingly, a large proportion of innovation is taking place in the digital economy. Innovation in business models based on Big Data, deep-learning algorithms and Internet of Things (IoT) is expected to dramatically alter many paradigms such as employment, communication, health and productivity that are fundamental to our lives. Acting responsibly in this area is therefore of primary importance in shaping society and the values of tomorrow.[[1]](#footnote-1)

Confidentiality refers to the safeguarding of personal, sensitive, or private information, by protecting data from unauthorized access, use, or disclosure, and in compliance with contractual or legislative provisions. It is essential to ensure that users have control over how their personal information is collected, stored and used, from the inception of the product through its entire lifecycle.

Privacy is also a vital aspect of responsible innovation, users have the right to control their personal information, and developers must ensure that they are transparent about how user data is collected and used, and users must be able to make informed decisions about whether to share their information.

Data protection is also a critical consideration for responsible innovation, developers must implement appropriate technical and security measures to protect the data subject from unauthorized access, theft, or misuse. This includes data encryption, data minimization/anonymization, secure data storage and access controls, to ensure that only authorized personnel can access the data.

Digital innovation should not be based on algorithms or databases that lead to manipulation of information, infringement of freedom of expression, shortcomings in data protection and privacy or freedom of association. Neither should it negatively affect the right to education and multilingualism, consumer rights and capacity building in the context of the right to economic development.[[2]](#footnote-2)

There are other aspects that should be taken into consideration for responsible innovation such as social responsibility and the potential impact of the products and services on society; the developers must minimize any adverse effects and maximize the social benefits of their innovation, product safety. This can help ensure that technologies are beneficial to society and individuals while simultaneously protecting the fundamental rights and freedoms of users, but these aspects are not the subject of the present research.

Several research methods have been used in documenting the issues under scientific research, analyzed from a legal point of view. Among these, the *comparative method* is used to identify the similarities and differences regarding responsible innovation and the responsibility principle, and the data protection accountability principle. Through the *legal method*, the national and European legislative framework was identified and that could be applicable.

**2. Applicable recommendations, guidelines, and law provisions**

There are several recommendations, guidelines and legal provisions related to the responsible innovation, including:

**The Artificial Intelligence Act**[[3]](#footnote-3) **-** This proposal imposes some restrictions on the freedom to conduct business (article 16) and the freedom of art and science (article 13) to ensure compliance with overriding reasons of public interest such as health, safety, consumer protection and the protection of other fundamental rights (‘responsible innovation’) when high-risk AI technology is developed and used. Those restrictions are proportionate and limited to the minimum necessary to prevent and mitigate serious safety risks and likely infringements of fundamental rights[[4]](#footnote-4).

Artificial intelligence is a rapidly developing family of technologies that require novel forms of regulatory oversight and a safe space for experimentation, while ensuring responsible innovation and integration of appropriate safeguards and risk mitigation measures. To ensure a legal framework that is innovation-friendly, future-proof and resilient to disruption, national competent authorities from one or more Member States should be encouraged to establish artificial intelligence regulatory sandboxes to facilitate the development and testing of innovative AI systems under strict regulatory oversight before these systems are placed on the market or otherwise put into service.[[5]](#footnote-5)

**The European Declaration on Digital Rights and Principles for the Digital Decade[[6]](#footnote-6)** presents the EU’s commitment to a secure, safe and sustainable digital transformation that puts people at the center, in line with EU core values and fundamental rights. [[7]](#footnote-7)

Because the digital transformation affects every aspect of people’s lives and presents challenges for our democratic societies, our economies and for individuals, the Declaration should serve as a reference point for businesses and other relevant actors when developing and deploying new technologies. Promoting research and innovation is important in this respect.[[8]](#footnote-8) The Declaration aims to promote that:

* People are at the center of the digital transformation in the European Union. Technology should serve and benefit all people living in the EU and empower them to pursue their aspirations, in full security and respect for their fundamental rights ensuring responsible and diligent action by all actors, public and private, in the digital environment.[[9]](#footnote-9)
* Technology should be used to unite, and not divide, people. The digital transformation should contribute to a fair and inclusive society and economy in the EU, making sure that the design, development, deployment and use of technological solutions respect fundamental rights, enable their exercise, and promote solidarity and inclusion.[[10]](#footnote-10)
* Everyone should be empowered to benefit from the advantages of algorithmic and artificial intelligence systems including by making their own, informed choices in the digital environment, while being protected against risks and harm to one’s health, safety, and fundamental rights, promoting human-centric, trustworthy and ethical artificial intelligence systems throughout their development, deployment and use, in line with EU values.[[11]](#footnote-11)
* Everyone should have access to digital technologies, products and services that are by design safe, secure, and privacy-protective, resulting in a high level of confidentiality, integrity, availability, and authenticity of the information processed, protecting the interests of people, businesses and public institutions against cybersecurity risks and cybercrime, including data breaches and identity theft or manipulation. This includes cybersecurity requirements for connected products placed on the single market.[[12]](#footnote-12)

The Organization for Economic Co-operation and Development (**OECD) Recommendation of the Council on Artificial Intelligence[[13]](#footnote-13)** identifies five complementary values-based principles for the responsible stewardship of trustworthy AI and calls on AI actors to promote and implement them: a) inclusive growth, sustainable development and well-being; b) human-centered values and fairness; c) transparency and explainability; d) robustness, security and safety; d) and accountability.

Based on the accountability principle, the AI actors should be responsible for the proper functioning of AI systems and for the respect of the above principles, based on their roles, the context and consistent with the state of art.

**The UNESCO Recommendation on the Ethics of Artificial Intelligence**[[14]](#footnote-14) represents a historic and unique agreement of 193 Member States on the fundamental values, principles and policies that should govern the development of this game-changing technology. It provides concrete pathways, including innovative tools, methodologies, and initiatives to ensure maximizing the positive impact of AI, while addressing the associated risks. The Recommendation is addressed to Member States, but it provides ethical guidance to all AI actors, including the private sector.[[15]](#footnote-15)

According to theUNESCO Recommendation,AI actors and Member States should respect, protect, and promote human rights and fundamental freedoms, (…), assuming their respective ethical and legal responsibility, in accordance with national and international law, in particular Member States’ human rights obligations and ethical guidance throughout the life cycle of AI systems, including with respect to AI actors within their effective territory and control. The ethical responsibility and liability for the decisions and actions based in any way on an AI system should always ultimately be attributable to AI actors corresponding to their role in the life cycle of the AI system.[[16]](#footnote-16)

Appropriate oversight, impact assessment, audit, and due diligence mechanisms, including whistle-blowers’ protection, should be developed to ensure accountability for AI systems and their impact throughout their life cycle. Both technical and institutional designs should ensure auditability and traceability of (the working of) AI systems to address any conflicts with human rights norms and standards and threats to environmental and ecosystem well-being**.[[17]](#footnote-17)**

**White Paper on Artificial Intelligence - A European approach to excellence and trust**[[18]](#footnote-18) provides that AI systems – and certainly high-risk AI applications – must be technically robust and accurate to be trustworthy. That means that such systems need to be developed in a responsible manner and with an ex-ante due and proper consideration of the risks that they may generate. Their development and functioning must ensure that AI systems behave reliably and as intended. All reasonable measures should be taken to minimize the risk of harm being caused.

**The Ethics Guidelines for Trustworthy Artificial Intelligence**[[19]](#footnote-19) prepared by the High-Level European Commission Expert Group on Artificial Intelligence which includes principles such as transparency, accountability, and fairness. It is necessary that mechanisms be put in place to ensure responsibility and accountability for AI systems and their outcomes, both before and after their development, deployment, and use.

Auditability entails the enablement of the assessment of algorithms, data, and design processes. Evaluation by internal and external auditors and the availability of such evaluation reports can contribute to the trustworthiness of the technology. In applications affecting fundamental rights, including safety-critical applications, AI systems should be able to be independently audited.[[20]](#footnote-20)

Minimization and reporting of negative impacts, both the ability to report on actions or decisions that contribute to a certain system outcome, and to respond to the consequences of such an outcome, must be ensured. Identifying, assessing, documenting, and minimizing the potential negative impacts of AI systems is especially crucial for those (in)directly affected. The use of impact assessments (e.g., red teaming or forms of Algorithmic Impact Assessment) both prior to and during the development, deployment and use of AI systems can be helpful to minimize negative impact. These assessments must be proportionate to the risk that the AI systems pose.

**The General Data Protection Regulation[[21]](#footnote-21)** places obligations on organizations to protect personal data and ensures that individuals have the right to know what information is held about them and to have it corrected or deleted if necessary.

Accountability principles require controllers to actively and continuously implement measures to promote and safeguard data protection in their processing activities and are responsible for compliance of their processing operations with data protection law and their respective obligations.

Also, controllers must be able to demonstrate compliance with data protection provisions to data subjects, the public and supervisory authorities at any time. Processors must also comply with some obligations strictly linked to accountability, such as keeping a record of processing operations and appointing a Data Protection Officer.[[22]](#footnote-22)

OECD also adopted the **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data** that highlighted that controllers have an important role in making data protection work in practice. The guidelines comprise an accountability principle to the effect that a data controller should be accountable for complying with measures which give effect to the principles stated above.[[23]](#footnote-23)

New developments in Artificial Intelligence are transforming the world, from science and industry to government administration and finance. The rise of AI decision-making also implicates fundamental rights of fairness, accountability, and transparency as per the **Universal Guidelines for Artificial Intelligence[[24]](#footnote-24).** The assessment and accountability obligation relate that an AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks and the institutions must be responsible for decisions made by an AI system.

As research evaluates algorithms that could rule our lives, code should be open and auditable. With the general complexity and issue of transparency of design and functionality of deep-learning and big data, this is becoming even more sensitive, and a call that we should establish a framework for algorithm design. One such framework is the Asilomar principles for the design of AI, with the goal of creating beneficial rather than undirected intelligence, using principles, such as transparency in failure, clarity in responsibility, alignment to human values, robustness with respect to security, or respect of privacy[[25]](#footnote-25).

The **Digital Services Act** (DSA)[[26]](#footnote-26) defines clear responsibilities for providers of intermediary services and in particular online platforms, such as social media and marketplaces and mandatory risk assessments and more transparency over algorithms. The DSA includes provisions related to the responsibility of online platforms in ensuring the safety, security, and rights of their users. This includes measures to prevent the spread of illegal content such as hate speech, terrorist content and counterfeit products, as well as requirements for transparency in online advertising and data protection.

The promotion of AI-driven innovation is also closely linked to the Data Governance Act[[27]](#footnote-27), the Open Data Directive[[28]](#footnote-28) and other initiatives under the EU strategy for data[[29]](#footnote-29) , which will establish trusted mechanisms and services for the re-use, sharing and pooling of data that are essential for the development of data-driven AI models of high quality.

**3. The Accountability principle**

General Data Protection Regulation and Modernized Convention 108[[30]](#footnote-30) determine that the controller is responsible for, and should be able to ensure, compliance with the data protection principles.[[31]](#footnote-31) Controllers can facilitate compliance with this requirement in various ways, which include:• recording processing activities and making them available to the supervisory authority upon request; • in certain situations, designating a data protection officer who is involved in all issues relating to personal data protection; • undertaking data protection impact assessments for types of processing likely to result in a high risk to the rights and freedoms of natural persons; • ensuring data protection by design and by default; • implementing modalities and procedures for the exercise of the rights of the data subjects; • adhering to approved codes of conduct or certification mechanisms.[[32]](#footnote-32)

Responsibility is a specific principle for personal data processing, as well as setting out an obligation for controllers to demonstrate their compliance with the provisions of the data protection law. This accountability is a continuous obligation. It does not manifest itself only at the end of a data processing operation when something goes wrong; rather, it is a proactive obligation to develop adequate data management in practice. Moreover, in keeping with the idea that individual control over personal data should operate as a default setting, it shift the burden of proof to the organization conducting data processing in many instances and focuses on accountability for responsible data stewardship, rather than mere compliance while ensuring that expectations and protection of privacy is preserved.[[33]](#footnote-33)

Accountability is not an easy task. For the controller to be accountable in today's data driven society, it requires an organization that is able to show a regulator, customer or business partner evidence of having met, and continuing to meet, all of the obligations under the GDPR. This is not just a few documents and a database with records of processing activities. Accountability requires the organization to have a data protection policy, a statement that sets out how an organization protects personal data. It requires transparency about data protection responsibilities across the organization and indeed awareness that everyone in the organization who comes into contact with personal data is partly responsible for compliance with the GDPR.[[34]](#footnote-34)

**4. Data protection by design and by default**

Another proponent of accountability is the implementation of data protection by design and by default. To achieve this, a cultural shift may be required to ensure that data protection is considered at the outset of every new project and for the duration of its life.[[35]](#footnote-35)

Data protection by design requires that controllers put in place measures to effectively implement data protection principles and to integrate the necessary safeguards to meet the requirements of the regulation and protect the rights of data subjects.[[36]](#footnote-36) These measures should be implemented both at the time of processing and when determining the means for processing. In implementing these measures, the controller needs to consider the state of the art, the costs of implementation, the nature, scope and purposes of personal data processing and the risks and severity for the rights and freedoms of the data subject.[[37]](#footnote-37)

Data protection by default requires that the controller implements appropriate measures to ensure that only personal data which are necessary for the purposes will be processed by default. This obligation applies to the amount of personal data collected, the extent of the processing, the storage period and accessibility.[[38]](#footnote-38)

**5. Penalties**

For violating the principle of accountability, I will mention some sanctions applied by the supervisory authorities:

5.1 The Irish DPA (DPC) has imposed a fine of EUR 17 million on Meta Platforms Ireland Limited[[39]](#footnote-39) (former Facebook Ireland Limited) on 15.03.2022. The decision is based on twelve notifications of data breaches that occurred between June 7, 2018, and December 4, 2018. The outcome of the DPC's investigation revealed that Meta had violated Article 5 (2) and Article 24 (1) GDPR. During its investigation, the DPC found that Meta failed to demonstrate that it had taken appropriate technical and organizational measures to protect the data of EU users. The fine proceedings involved cross-border data processing, which is why the decision was subject to the co-decision procedure under Art. 60 GDPR involving all other European supervisory authorities as co-decision-makers.

5.2 Vodafone Italia S.p.A.[[40]](#footnote-40) was fined EUR 12,251,601 on 12.11.2020 for unlawfully processing personal data of millions of customers for telemarketing purposes. The proceedings were preceded by hundreds of complaints from data subjects about unsolicited telephone calls, which led to an investigation by the data protection authority. This investigation revealed several violations of the data protection law, including the violation of consent requirements and the violation of general data protection obligations such as accountability. Moreover, further violations could be found in the handling of contact lists purchased from external providers. Finally, security measures for the management of customer data were also considered inadequate.

5.3 The Danish DPA has imposed a fine of EUR 1.3 million on Danske Bank[[41]](#footnote-41) on 05.04.2022. The DPA opened an investigation against the bank after it informed the DPA that it had a problem with the deletion of personal data. During the investigation, the DPA found that the bank had failed to document the rules for deletion and storage of personal data in more than 400 systems. Consequently, the bank was unable to prove that such rules, which are required under the GDPR, existed. The DPA considered this to be a breach of the bank's accountability obligation under Art. 5 (2) GDPR.

**6. Conclusion:**

Confidentiality, privacy, and data protection are crucial aspects of responsible innovation, these concepts pertain to individuals' right to safeguard their personal information and have control over how it is collected, stored, and used, starting from the point of the conception and throughout the life of the resulting technological product.

For responsible innovation, in addition to complying with data protection regulations, transparency and user’s information, security, data minimization/anonymization and privacy impact assessment, other aspects that should be considered in technical and institutional designs are auditability and traceability of (the working of) AI systems to address any conflicts with human rights norms and standards.

**7. Bibliography**

Studies published in journals:

* 1. Leo Besemer, Privacy and data protection based on the GDPR. Undersanding The General Data Protection Regulation, Van Haren Publishing, 2020, p.35
* 2. Orla Lynskey, The foundations of EU Data protection Law, Oxford University Press, 2015;
* 3. [Marc Dreyer](https://sciprofiles.com/profile/283440), [Luc Chefneux](https://sciprofiles.com/profile/author/bmRTRHR1Tzg5RWgzWHlEVlVtV2VhUElpWEo4ZVV0TDdIWk5wazhuTy9DOD0%3D), Anne Goldberg, Joachim Von Heimburg, Norberto Patrignani, Chris Shilling, [Monica Schofield](https://sciprofiles.com/profile/author/TGM4NFk1b0o4TlhzVTU0bkZITzB6SXBYKzFWeXgwVUtpQmQxWnZCa3hobz0%3D), Responsible Innovation: A Complementary View from Industry with Proposals for Bridging Different Perspectives, Sustainability, 2017;
* 4. Handbook on European data protection law, European Union Agency for Fundamental Rights and Council of Europe, 2018;

Recommendations, guidelines, proposals, and laws

* 1. Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (ARTIFICIAL INTELLIGENCE ACT) and amending certain union legislatives acts, Brussels, 21.4.2021, COM(2021) 206 final, 2021/0106(COD)
* 2. European Declaration on Digital Rights and Principles for the Digital Decade 2023/C 23/01, PUB/2023/89
* 3. OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449
* 4. United Nations Educational, Scientific and Cultural Organization (UNESCO), France, adopted on 23 November 2021
* 5. White Paper on Artificial Intelligence - A European approach to excellence and trust, Brussels, 19.2.2020 COM (2020) 65 final
* 6. The Ethics Guidelines for Trustworthy Artificial Intelligence prepared by the High-Level European Commission Expert Group on Artificial Intelligence, 2019
* 7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88
* 8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88
* 9. OECD (2013), Guidelines on governing the Protection of Privacy and transborder flows of personal data, Art. 14
* 10. Universal Guidelines for Artificial Intelligence, 23 October 2018, Brussels, Belgium, AI Universal Guidelines – thepublicvoice.org
* 11. Future of life Institute. Asilomar AI Principles. Available online: <https://futureoflife.org/ai-principles/> (accessed on 05.05.2023)
* 12. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) PE/30/2022/REV/1, *OJ L 277, 27.10.2022, p. 1–102*
* 13. Proposal for a Regulation on European data governance (Data Governance Act) COM/2020/767
* 14. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83
* 15. Commission Communication, A European strategy for data COM/2020/66 final
* 16. Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data, CM/Inf(2018)15-final, 18 May 2018, Art. 7 (2)

**Daniela Duță** is a PhD student at the Institute of Legal Research „Acad. Andrei Rădulescu” of the Romanian Academy. She can be contacted at ghituleasad@yahoo.com

1. [Marc Dreyer](https://sciprofiles.com/profile/283440), [Luc Chefneux](https://sciprofiles.com/profile/author/bmRTRHR1Tzg5RWgzWHlEVlVtV2VhUElpWEo4ZVV0TDdIWk5wazhuTy9DOD0%3D), Anne Goldberg, Joachim Von Heimburg, Norberto Patrignani, Chris Shilling, [Monica Schofield](https://sciprofiles.com/profile/author/TGM4NFk1b0o4TlhzVTU0bkZITzB6SXBYKzFWeXgwVUtpQmQxWnZCa3hobz0%3D), Responsible Innovation: A Complementary View from Industry with Proposals for Bridging Different Perspectives, Sustainability, 2017; <https://doi.org/10.3390/su9101719>, Available online: [Sustainability | Free Full-Text | Responsible Innovation: A Complementary View from Industry with Proposals for Bridging Different Perspectives (mdpi.com)](https://www.mdpi.com/2071-1050/9/10/1719#B128-sustainability-09-01719) (accessed on 05.05.2023)

 [↑](#footnote-ref-1)
2. [Marc Dreyer](https://sciprofiles.com/profile/283440), [Luc Chefneux](https://sciprofiles.com/profile/author/bmRTRHR1Tzg5RWgzWHlEVlVtV2VhUElpWEo4ZVV0TDdIWk5wazhuTy9DOD0%3D), Anne Goldberg, Joachim Von Heimburg, Norberto Patrignani, Chris Shilling, [Monica Schofield](https://sciprofiles.com/profile/author/TGM4NFk1b0o4TlhzVTU0bkZITzB6SXBYKzFWeXgwVUtpQmQxWnZCa3hobz0%3D), Responsible Innovation: A Complementary View from Industry with Proposals for Bridging Different Perspectives, *Sustainability* 2017; <https://doi.org/10.3390/su9101719>, Available online: [Sustainability | Free Full-Text | Responsible Innovation: A Complementary View from Industry with Proposals for Bridging Different Perspectives (mdpi.com)](https://www.mdpi.com/2071-1050/9/10/1719#B128-sustainability-09-01719) (accessed on 05.05.2023) [↑](#footnote-ref-2)
3. Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (ARTIFICIAL INTELLIGENCE ACT) and amending certain union legislatives acts, Brussels, 21.4.2021, COM(2021) 206 final, 2021/0106(COD) [↑](#footnote-ref-3)
4. Ibid., Context of the proposal, 3.5 [↑](#footnote-ref-4)
5. Ibid., para. 71 [↑](#footnote-ref-5)
6. European Declaration on Digital Rights and Principles for the Digital Decade 2023/C 23/01, PUB/2023/89

JO C 23, 23.1.2023, p. 1-7 [↑](#footnote-ref-6)
7. Available online: [European Declaration on Digital Rights and Principles | Shaping Europe’s digital future (europa.eu)](https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles), (accessed on 05.05.2023) [↑](#footnote-ref-7)
8. Ibid., para. 8. [↑](#footnote-ref-8)
9. European Declaration on Digital Rights and Principles for the Digital Decade 2023/C 23/01, PUB/2023/89, JO C 23, 23.1.2023, p. 1-7, Chapter I [↑](#footnote-ref-9)
10. Ibid.,Chapter II [↑](#footnote-ref-10)
11. Ibid.,Chapter III [↑](#footnote-ref-11)
12. Ibid.,Chapter V [↑](#footnote-ref-12)
13. OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 [↑](#footnote-ref-13)
14. Published in 2022 by the United Nations Educational, Scientific and Cultural Organization (UNESCO), France, adopted on 23 November 2021 [↑](#footnote-ref-14)
15. Ohchr.org/UNESCO Recommendation on the Ethics of Artificial Intelligence [↑](#footnote-ref-15)
16. Ibid., para. 42. [↑](#footnote-ref-16)
17. Ibid., para. 43. [↑](#footnote-ref-17)
18. White Paper on Artificial Intelligence - A European approach to excellence and trust, Brussels, 19.2.2020 COM(2020) 65 final [↑](#footnote-ref-18)
19. The Ethics Guidelines for Trustworthy Artificial Intelligence prepared by the High-Level European Commission Expert Group on Artificial Intelligence, 2019 [↑](#footnote-ref-19)
20. Ibid. p.19 [↑](#footnote-ref-20)
21. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88 [↑](#footnote-ref-21)
22. Handbook on European data protection law, European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 134 [↑](#footnote-ref-22)
23. OECD (2013), Guidelines on governing the Protection of Privacy and transborder flows of personal data, Art. 14 [↑](#footnote-ref-23)
24. Universal Guidelines for Artificial Intelligence, 23 October 2018, Brussels, Belgium, [AI Universal Guidelines – thepublicvoice.org](https://thepublicvoice.org/ai-universal-guidelines/) [↑](#footnote-ref-24)
25. Future of life Institute. Asilomar AI Principles. Available online: <https://futureoflife.org/ai-principles/> (accessed on 05.05.2023) [↑](#footnote-ref-25)
26. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) PE/30/2022/REV/1, *OJ L 277, 27.10.2022, p. 1–102* [↑](#footnote-ref-26)
27. Proposal for a Regulation on European data governance (Data Governance Act) [COM/2020/767](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767) [↑](#footnote-ref-27)
28. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83 [↑](#footnote-ref-28)
29. [Commission Communication, A European strategy for data COM/2020/66 final](https://eur-lex.europa.eu/legal-content/EN/TXT/Commission%20Communication%2C%20A%20European%20strategy%20for%20data%20COM/2020/66%20final.), [https://eur-lex.europa.eu/legal-content/EN/TXT/Commission%20Communication,%20A%20European%20strategy%20for%20data%20COM/2020/66%20final](https://eur-lex.europa.eu/legal-content/EN/TXT/Commission%20Communication%2C%20A%20European%20strategy%20for%20data%20COM/2020/66%20final). [↑](#footnote-ref-29)
30. Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data, CM/Inf(2018)15-final, 18 May 2018, Art. 7 (2) [↑](#footnote-ref-30)
31. Handbook on European data protection law, European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 134 [↑](#footnote-ref-31)
32. Handbook on European data protection law, European Union Agency for Fundamental Rights and Council of Europe, 2018, p.135 [↑](#footnote-ref-32)
33. Orla Lynskey, The foundations of EU Data protection Law, Oxford University Press, 2015, p.260 [↑](#footnote-ref-33)
34. Leo Besemer, Privacy and data protection based on the GDPR. Undersanding The General Data Protection Regulation, Van Haren Publishing, 2020, p.35 [↑](#footnote-ref-34)
35. Leo Besemer, Privacy and data protection based on the GDPR. Undersanding The General Data Protection Regulation, Van Haren Publishing, 2020, p.36 [↑](#footnote-ref-35)
36. General Data Protection Regulation, art. 25 (1). [↑](#footnote-ref-36)
37. Handbook on European data protection law, European Union Agency for Fundamental Rights and Council of Europe, 2018, p.183 [↑](#footnote-ref-37)
38. General Data Protection Regulation, Art. 25 (2). [↑](#footnote-ref-38)
39. <https://www.enforcementtracker.com/ETid-1094> [↑](#footnote-ref-39)
40. <https://www.enforcementtracker.com/ETid-438> [↑](#footnote-ref-40)
41. <https://www.enforcementtracker.com/ETid-1114> [↑](#footnote-ref-41)