

**PLAN:**

**PART I : Global socio-technological landscape**

**I- Data access and the exponential growth of genomic data**

**II- Artificial intelligence as an extension of human cognition**

**III- “Universal” Conceptual Basis of Informed Consent**

**IV- Challenging Informed Consent: Artificial Intelligence and Sensitive Data**

- 1. Hacking and Corruption of Human Autonomy*
- 2. How do the potential risks of AI deployment and DV challenge informed consent ?*

**PART II : GUIDANCE ON INFORMED CONSENT**

**I- Reconceptualizing Informed Consent in the age of AI and Data Visitation**

- 1. Informed Consent: a concept that evolves as techniques evolve*
- 2. Towards a reconsideration of classical forms of informed consent?*

**II- Reconsiderations of the overall conditions of informed consent**

- 1. The confrontation of informed consent with explicability and transparency issues*
- 2. Affirmation of ethical principles of use of AI and governance issues*

**III- Specific Cases**

- 1. Informed Consent in Human-Computer Interaction*
- 2. Informed Consent in Genomic Data Research*

**PART III - RECOMMENDATIONS AND GUIDELINES**

**Annex I**

## Part I - GLOBAL SOCIOTECHNOLOGICAL AND ETHICAL LANDSCAPE

### I- Data Visitation and Exponential Growth of Big Data: reconsidering access to data

The deployment of the use of digital technology in all areas of society is illustrated in particular by the accelerated use of Artificial Intelligence (AI). This method, which takes several forms, including self-learning AI systems, requires the use or reuse of a very large amount of data: big data<sup>1</sup>.

Therefore, access to and sharing of data is a major current issue, raising tensions for the deployment of innovation. Access to and sharing of data is the starting point for its use and re-use and is subject to strict and varying rules depending on whether the data is anonymous, personal or sensitive. Indeed, personal data can cover different types of information and are therefore classified by the European Data Protection Regulation (GDPR) according to categories: data relating to identity, data relating to personal life, data relating to professional life<sup>2</sup>. Then, security measures can change the nature of personal data by making them anonymous, i.e. completely and definitively detached from the natural person concerned, or pseudonymous by limiting the possibilities of direct identification. Finally, the GDPR identifies data that are sensitive by their nature, such as health data<sup>3</sup>. The category and nature of the data concerned has a direct influence on the issues of data collection, sharing and re-use.

A global incentive to share data<sup>4</sup>, which requires, among other things, broadening access to data for research purposes. This is illustrated in the European Union by the European Commission's intention to establish a regulation to set up the European Health Data Space with the aim of regulating and supporting the use, re-use and sharing of data<sup>5</sup>.

---

<sup>1</sup> <https://bmcmethics.biomedcentral.com/articles/10.1186/s12910-022-00871-z>

<sup>2</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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).

<sup>3</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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), Article 9.

<sup>4</sup> <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/102/52/PDF/N2010252.pdf?OpenElement> p.08.

<sup>5</sup> European Commission, Proposal for a regulation - The European Health Data Space, COM(2022) 197/2, 3 May 2022.

However, there are significant limitations to data sharing that hinder the approaches implemented. In this sense, the TEHDAS (Toward European Health Data Space) consortium published in September 2021 the results of several case studies identifying the barriers to sharing health data for secondary use<sup>6</sup>. The barriers identified as limits to sharing health data are legal, in particular due to differences between different legal frameworks. These national or regional differences are also felt in terms of existing infrastructures and human, financial and technical resources. Data security issues (data management, data quality and interoperability) also pose problems. Finally, the ethical issues of trust and transparency, but also of privacy protection, including questions about the informed consent of patients, are essential<sup>7</sup>.

Thus, these legal, organizational and ethical barriers lead to a mistrust of data sharing<sup>8</sup>. It is also possible to envisage that the aggregation of a large amount of data in one place raises increasing concerns about risks to data integrity and security, particularly in the event of theft or loss of data, which would pose a considerable risk to the privacy of individuals. Similarly, uncontrolled access to large amounts of data concerning, even indirectly, an individual or specific populations carries risks of data misuse.

It is in this context that reflections are developing around the technique of Data Visitation (DV). This method, which does not seem to be the primary consideration of official texts at national and international level<sup>9</sup> and which is not yet the subject of a clear and precise definition, brings a new way of considering access to data .

The DV seems to break with this approach since it allows access to health data without having to move them. In this sense, DV appears to be an innovative and interesting solution to the growing challenges of accessing data for research, including sensitive categories of data such as health or genomic data, by maintaining appropriate governance over the use of the data while allowing the processing of the data for research purposes<sup>10</sup>.

---

<sup>6</sup><https://tehdas.eu/app/uploads/2021/09/tehdas-summary-of-results-case-studies-on-barriers-to-sharing-health-data-2021-09-28.pdf?fbclid=IwAR2q1RJj27un7RfptuBDmQanig2vrBpkNOGr0P3Yan06LPbUXp-bJz5lgl8>

<sup>7</sup><https://tehdas.eu/app/uploads/2021/09/tehdas-summary-of-results-case-studies-on-barriers-to-sharing-health-data-2021-09-28.pdf?fbclid=IwAR2q1RJj27un7RfptuBDmQanig2vrBpkNOGr0P3Yan06LPbUXp-bJz5lgl8>, p.05.

<sup>8</sup> <https://jme.bmj.com/content/48/1/3>

<sup>9</sup> Results of the literature review carried out by group 3 of the AIDV working group between December 2022 and March 2023.

<sup>10</sup> We also point out that DV is intrinsically linked to AI. DV is intrinsically linked to AI, as its implementation requires the use of AI algorithms capable of identifying the relevant data for a given question and fetching this data directly from where it is found. In turn, the AI system (AIS) deployed for DV is progressively fed by the data it has gone to consult and thus becomes increasingly sophisticated.

Access to large amounts of data and the deployment of AI are accompanied by legal and ethical considerations and questions<sup>11</sup>. The move towards the use of big data and AI- and DV-based methods requires an articulation of legal and ethical considerations. In particular, the issues raised by the deployment of AI and data access require a re-examination of the effectiveness, applicability and form of consent.

## **II- Artificial Intelligence as Extensions of Human Cognition : Deployment in a Digital World**

Breakthroughs in computational power and efficiency are enabling humanity to create powerful artificial intelligence (AI) systems that not only allow greater capacity for information processing and analysis, but also deeper insights of the cognitive processes of a human person. In essence, AI systems are increasingly providing humanity the means to satisfy its desires – from the mundane to the most profound – as they become adept in knowing the human individual at a personal level.<sup>12</sup> Yet this capability is not only made possible by sophisticated algorithms but also the data-intensive environment that makes AI technology an important part of daily life. The creation and consumption of data has become the primary determinant of value and meaning. In other words, the measure of an individual's worth now depends on how much he or she contributes to the overall global data flow.<sup>13</sup> A fulfilling life has become intertwined with being 'seen' and valued in and through the digital world. As a result, the relationship between humanity and technology has never before become more intimate and inseparable. The capability of AI to discern the wants of the individual, and the unconditional desire of the individual for meaning are the two factors fueling the unprecedented development of AI. Through these two factors, AI is effectively rendered as an "extension of human cognition" because it no longer functions as merely a tool but rather as part of how a person thinks.<sup>14</sup> But what makes AI unique in this regard – as compared to the "pen and paper" example of extended mind theorists – is that it learns how to make itself an irreplaceable part of human cognition.<sup>15</sup> AI is defining the current global

---

<sup>11</sup> Council of Europe, Study, "Toward regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law", December 2020.

<sup>12</sup> Report of the High Commissioner for Human Rights A/HRC/48/31, 9-10; See Jeff Orlowski (dir), *The Social Dilemma* (Netflix: Center for Humane Technology, 2021).

<sup>13</sup> Yuval Noah Harari, 'The Data Religion,' in *Homo Deus: A Brief History of Tomorrow* (New York: Harper Collins, 2015), 623-26.

<sup>14</sup> See Peter Reiner and Saskia Nagel, 'Technologies of the Extended Mind: Defining the Issues,' in Judy Illes (ed), *Neuroethics: Anticipating the Future* (Oxford: Oxford University Press, 2017), 109-11.

<sup>15</sup> See Andy Clark and David Chalmers, "The Extended Mind," in *The Extended Mind*, ed. Richard Menary (London: MIT Press, 2010), 27-29.

sociotechnological landscape, but this will further accelerate with its growing importance, particularly in the field of genomic research, which consequently would enable it to holistically understand human beings by synergizing their online activities to their respective genomic data.

### **III- “Universal” Conceptual Basis of Informed Consent**

Enlightenment ideals of modernity and humanism have created a paradigm shift away from a transcendental conception of meaning towards a human-centered notion of it. Instead of being ‘given’ by some kind of divine being, one’s life meaning is created and sustained by the individual him/herself. This anthropocentric view of the world is the underlying idea of reality that constitutes philosophies centered on human autonomy and dignity – the most known of which is Immanuel Kant’s Deontological Ethics, which essentially believes in the capacity of humans to reason, and to choose and act independently based on such innate (or even ‘sacred’) capacity.<sup>16</sup> Morality is not supranatural but rather it emanates from human rationality – particularly from the logical consistency and *necessity* that this capacity entails – through the exercise of autonomy.<sup>17</sup> This means that individuals are both enforcers and subjects of their own moral laws, which by necessity would have to be applicable universally and that which respects the independence and rationality of individuals.

Privacy and informed consent are two intertwined practices necessary for upholding such respect, and preserving the dignity of a human person as a free agent. These two practices basically facilitate how information flows in and out of the individual in a manner that does not hinder or violate how he or she makes sense of them by him/herself. Privacy protects the person from intrusions that would compromise his/her capacity to think and act independently, while informed consent enables the individual to have the appropriate information that will capacitate him/her to think and act independently.<sup>18</sup>

Kantian deontology is and continues to be a powerful force in the Western philosophical tradition to such extent that it has become the conceptual basis for the Universal Declaration of Human Rights, which was adopted by the UN General Assembly in 1948, and since then

---

<sup>16</sup> Luigi Caranti, ‘Kant’s Theory of Human Rights,’ in *Handbook of Human Rights*, ed. Thomas Cushman (London: Routledge, 2011), 35-37.

<sup>17</sup> Harari, *Homo Deus*, 359-85.

<sup>18</sup> *Nuremberg Code*, Article 1 (August 1947); *International Covenant on Civil and Political Rights*, Provision 7 (March 1976).

become the basis of all international human rights treaties and frameworks.<sup>19</sup> But as the world increasingly become data-driven – shaped by the generation and consumption of information – intrusions to privacy and informed consent are fast becoming a necessary evil due to the fact that, as pointed out earlier, surviving and thriving in such a world, one would need to be part of the global data flow – in other words, to make everything about his life intimately intertwined with the digital world, which will then inevitably include his own personal information. This makes it easy for large companies to extract and (re)use data without informed consent and (often than not) in violation of privacy of the individual by either denying him the services that are necessary in enabling him to participate in the global data flow (e.g., online transactions, research collaboration, social media communication, etc.) that would force him to agree to whatever terms and conditions that these companies offer, or using data-intensive technologies such as AI and big data that makes it almost impossible to render data collection, processing and (re)use transparent and understandable. Efforts to address this problem have now started to gain traction at the global level as exemplified by the creation of the following UN guidance documents<sup>20</sup>.

But given the necessity today of being part of the global data flow in order to survive and thrive, the current global sociotechnological milieu is driving humanity to a point of no return wherein it is being made to violate its own sense of autonomy by gearing it towards pursuing a meaningful existence that nonetheless reduces it into a mere data to be collected, sold and used. In a sense, the **human-centered paradigm** grounded on modernism and humanism is imploding upon itself as autonomy has become a mere means rather than an end of what humanity wants to be.<sup>21</sup>

#### **IV- Challenging Informed Consent: Artificial Intelligence and Sensitive Data**

##### *1. Hacking and Corruption of Human Autonomy*

Considering the fact that personal data has effectively become a valuable currency in the present data-intensive world. It enables individuals to engage and be a part of the global flow of data, but at the same time, it is also through which exploitative forces are able to

---

<sup>19</sup> United Nations Human Rights Office of the High Commissioner, 'Universal Declaration of Human Rights,' (1948).

<sup>20</sup> See Annex I of the Deliverable.

<sup>21</sup> See **The Great Decoupling** in Harari, Homo Deus, 497-567.

intrude on the privacy and autonomy of individuals. This rationalizes the sensitivity of personal information – particularly speaking, those that feature the following information:

- (a) Psychographic data – personal information highlighting the subjective expressions of the individual that features his/her belief systems, aspirations, and desires and aversions;<sup>22</sup>
- (b) Genomic data – personal information highlighting the objective yet unique genetic constitution of the individual that determines his/her biological structure and processes (i.e., neural processes).<sup>23</sup>

Together, psychographic and genomic information reveal fundamentally *who* the individual is, which would provide better reading of his personality and predispositions. This “mind reading” – regardless of the possible benefits it could bring – is in-itself already a violation of privacy.<sup>24</sup> But what is more insidious is that it is a step closer towards cognitive manipulation and corruption of human autonomy. Having the knowledge of a person’s desires and aversions provides the capability to use such feelings against him – making him psychotically obsessed with whatever object those feelings have to such an extent that it shapes how he thinks and decides while deluding him with a sense of freedom.

Protection of psychographic and genomic data is subsumed in the definition of sensitive data forwarded by the UN through the 2017 Data Privacy, Ethics and Protection Guidance Note:

Sensitive data should be considered as any data related to (i) racial or ethnic origin, (ii) political opinions, (iii) trade union association, (iv) religious beliefs or other beliefs of a similar nature, (v) physical or mental health or condition (or any genetic data), (vi) sexual orientation and other related activities, (vii) the commission or alleged commission of any offence, (viii) any information regarding judicial proceedings, (ix) any financial data, (x) children and (xi) an individual(s) or group(s) of individuals that face any risks of harm (e.g. physical, emotional, economic).

However, developments in AI highlight not only the immense need and potential of massive amounts of sensitive data in crafting profitable business models and customized healthcare but also risks of increasingly efficient techniques in conducting political and biological surveillance by hacking (and corrupting) human autonomy.

---

<sup>22</sup> ‘What is Psychographics? Understanding The Tech that Threatens Elections,’ *CB Insights* (May 2020), Retrieved from <https://www.cbinsights.com/research/what-is-psychographics/>.

<sup>23</sup> ‘What is Genomic Data?,’ *Amazon* (2023), Retrieved from <https://aws.amazon.com/what-is/genomic-data>.

<sup>24</sup> See Rachel Wurzman and James Giordano, “‘NEURINT’ and Neuroweapons: Neurotechnologies in National Intelligence and Defense,” in *Neurotechnology in National Security and Defense*, ed. James Giordano (Florida: Taylor & Francis Group, 2015), 93.

Psychographic data enables companies to develop a product or service that would better appeal to clienteles and prospective customers. However, the capability of AI to analyze huge sets of data all at once enabled companies to extract high quality psychographic data that provide intimate psychological information of individuals across the globe. This not only help them constantly improve the marketability of their products and services, but more importantly make the attention of the individuals themselves as a marketable commodity. Through the so-called “attention-extraction” economic model driven by AI, companies are able to profit more as this model ensures constant engagement of clientele and prospective customers by extracting and using their psychographic information, which is made readily available by social media and tech companies that keep track of their online activities.<sup>25</sup> Such constant engagement rests on being able to make it addicting by knowing and amplifying their innermost desires and fears to such extent that their own autonomy becomes a psychopathic tool of his wants – of course, in this case, his wants are no longer his own to begin with.

Thus, one of the risks posed by AI on the protection of sensitive data is not only that its use could lead to violation of autonomy at a global scale but also it could be deployed as a manipulative tool that deceptively transforms such violation into a meaningful expression of it. Informed consent is thereby no longer a shield of privacy and human autonomy as it once was.

Genomic data is nonetheless overtaking psychographic data coming from the Internet in terms of size. This kind of personal information is already at the zetta scale level of data size.<sup>26</sup> The exponential growth of genomic data in recent years is significantly driven by breakthroughs in biotechnology coupled with advances in AI application in that field. With greater computational power and efficiency, it has become easier to sequence and process genomic data as the so-called “curse of dimensionality” is mitigated by the optimizing nature of AI algorithms.<sup>27</sup> Moreover, emergence of health trackers such as Google Fit and Apple Health are pursuing real-time analysis of individual-level genomic data and constitute large

---

<sup>25</sup> ‘Paying Attention: The Attention Economy,’ *Berkeley Economic Review* (March 2020), Retrieved from <https://econreview.berkeley.edu/paying-attention-the-attention-economy/>.

<sup>26</sup> ‘Sensitive Data Contexts and Disciplines: A Look at Different Approaches,’ *Conference Seminar* (Gothenburg: Research Data Alliance, 2023).

<sup>27</sup> Nikolay Oskolkov, ‘Machine Learning View of Multi-Omics Data Integration,’ *Symposium* (Virtual: Pine Biotech, 2022).

datasets notably used to understand and mitigate genetic diseases.<sup>28</sup> As a result, it has become possible to acquire information of predictive value about diseases or health traits, to accurately diagnose pathologies and develop personalized prevention or treatment strategies at individual and population level. Moreover, it provided a significant boost in the areas of precision medicine and genetic engineering.

Nonetheless, as much as genetic engineering maximizes the benefit of genomic data, it is also wherein the protection of such sensitive information becomes problematic, particularly in the context of AI in biotechnology. It is actually more problematic compared to AI using psychographic data as means for mind manipulation since gene alteration, carried with precision through AI, may lead to *irreversible* changes in the genetic, biological and ultimately neural constitution of the individual, or on the constitutional human genetic heritage.<sup>29</sup> Thus, it does not only threaten to violate and corrupt human autonomy – it threatens to destroy it altogether. What is more worrying is that if the irreversibility of AI-driven genetic engineering is synergized with the sustainability of psychographic manipulation. This is increasingly becoming a reality as there is growing research in mental health looking on how to correlate genomic data with online psychographic data of individuals.<sup>30</sup> Furthermore, this synergy might even perhaps be inevitable considering that psychographic manipulation leads individuals obsessed by their own desires – and this could ultimately end up with the individual willingly discarding his own autonomy in pursuit of something that he or she deems to be better than being human itself.

## *2. How do the potential risks of AI deployment and DV challenge informed consent ?*

Big data and AI are interdependent and their deployment requires consideration of risks associated with them, to ensure respect of human autonomy<sup>31</sup>. Similarly, the use of AI can lead to the risk of errors, scientific bias or discriminatory bias which can have consequences for individuals, especially in sensitive areas such as health research<sup>32</sup>. Decisions made using

---

<sup>28</sup> Oleg Afonin, 'Securing and Extracting Health Data: Apple Health vs. Google Fit,' Elcomsoft (January 2019), Retrieved from <https://blog.elcomsoft.com/2019/01/securing-and-extracting-health-data-apple-health-vs-google-fit/>.

<sup>29</sup> Jonathan Pugh, 'Reversibility, Consent, and the Regulation of Emerging Neurosurgical Therapies in Psychiatry,' *Conference Presentation* (Montreal: International Neuroethics Society, 2022).

<sup>30</sup> Jit Sarkar, 'Clinical Informatics: Use Cases and Challenges,' *Symposium* (Virtual: Pine Biotech, 2022).

<sup>31</sup> United Nations Educational, Scientific and Cultural Organization. Recommendation on the Ethics of AI, (New York: United Nations General Assembly).

<sup>32</sup> Council of Europe, Study, "Toward regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law", December 2020.

automatic data processing including algorithms can lead to disastrous results due to low data quality or bias in the process<sup>33</sup>. Innovative AI methods for DV thus force us to recall the importance of protecting human dignity, through the respect of the autonomy of the person and his fundamental rights<sup>34</sup>.

In this respect, a large number of documents, including reports from the UN, warn of the risks of AI and Big Data technologies for the preservation of privacy and autonomy of individuals<sup>35</sup>. The UN, as well as the European Union recall the affirmation of the respect of fundamental rights in order to provide sufficient protection<sup>36</sup>. In this sense, informed consent is presented as a guarantee of the effectiveness of fundamental rights. However, the UN reports highlight practical and conceptual obstacles to the implementation of informed consent, which require reconsideration of the use of informed consent depending on whether it is consent for access or use of data, consent for the use of AI, or even depending on the purpose of use (e.g. research or health)<sup>37</sup>.

In this sense, we identify that informed consent is a form of protection that already evolves according to the context and the purpose, it can be prospective, specific or even dynamic<sup>38</sup>. Informed consent provides guarantees of protection and may be required by law under certain conditions<sup>39</sup>.

Considering the developments in technology and the risks they may present for the individual and his or her rights, it appears that the design and implementation of informed consent must be reconsidered for optimal and appropriate protection. Should consent for data processing be the same as consent for AI use? Should consent be tailored to the method of data processing or to the context of use (e.g. research)?

This reconsideration is not easy in that consent can quickly be perceived as an obstacle if it is not practical to obtain (technical impossibility)<sup>40</sup>. But is this a good justification for going beyond the practical limits of respecting consent? In addition, some authors consider that there is an ethical obligation to share such data if it is in the public interest, notably for the

---

<sup>33</sup> Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda.

<sup>34</sup> UNESCO, "Report of the International Bioethics Committee of UNESCO (IBC) on consent", 2008.

<sup>35</sup> UN, Report of the High Commissioner for Human Rights A/HRC/39/29: The right to privacy in the digital age, 3 August 2018.

<sup>36</sup> UN, Report of the Secretary-General A/HRC/43/29: Report on the role of new technologies in the realization of economic, social and cultural rights, 5 March 2020.

Council of Europe, Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, 8<sup>th</sup> April 2020.

<sup>37</sup> Report of the High Commissioner for Human Rights A/HRC/48/31: The right to privacy in the digital age, 15th September 2021.

<sup>38</sup> <https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Framework-2023.pdf>

<sup>39</sup> 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).

<sup>40</sup> <https://jme.bmj.com/content/44/6/392>

improvement of research<sup>41</sup>. Is this consideration applicable to data visitation? Whatever the answer, the consideration is about commitment, respect for essential ethical principles, privacy and the principle of transparency.

## **Part II - GUIDANCE ON INFORMED CONSENT**

### **I- Reconceptualizing Informed Consent in the age of AI and Data Visitation**

#### *1- Informed Consent: a concept that evolves as techniques evolve*

At both international and European level, informed consent has been developed as a tool to protect fundamental rights<sup>42</sup>. First of all, the importance of informed consent is affirmed, particularly in the field of research, in the form of a legal obligation, which must respect a strict formalization, attesting to the autonomy, or even self-determination of the individual (essential coherence of the application of fundamental rights)<sup>43</sup>. However, with the deployment of the use of personal data, the conceptualisation and implementation of consent in the field of health research has had to evolve. An articulation was then implemented between two distinct consents: consent in the context of interventional research, which protects bodily integrity<sup>44</sup>; and consent in the context of data protection, which protects informational integrity<sup>45</sup>, both are fundamental to the respect of the individual's right to privacy and require a balance to be struck with digital methods<sup>46</sup>.

The adaptation of the implementation of consent for data protection also follows precise formalization rules<sup>47</sup>. Consent used as a legal basis for data processing<sup>48</sup> must meet specific formal and implementation requirements. It must be free, specific, informed and

---

<sup>41</sup> <https://jme.bmj.com/content/44/6/392>

<sup>42</sup> P. du Bois, Pierre, The European Union and Human Rights, International Relations, vol. 132, no. 4, 2007, pp. 33-39, available at: <https://www.cairn.info/revue-relations-internationales-2007-4-page-33.htm>.

UN, Report of the High Commissioner for Human Rights A/HRC/39/29: The right to privacy in the digital age, 3 August 2018.

<sup>43</sup> Declaration of Helsinki, World Medical Association, June 1964.

<sup>44</sup> Shuster E. The Nuremberg Code: hippocratic ethics and human rights. Lancet 1998;351(9107):974–7.

<sup>45</sup> EDPB, Guidelines 05/2020 on consent under regulation 2016/679, Version 1.1.

<sup>46</sup> O CATHAOIR Katharina, "The evolution of human rights in the European Union and its impact on consent for genetics/genomics research", oral intervention in session GA4GH 2023 "Consent for the sharing of biological materials and data in genetics/genomics research. The impact of evolving European standards within open science frameworks". 20 April 2023.

<sup>47</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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), Article 6.

<sup>48</sup> However, consent is not the only standard for allowing access to data in the context of research activities. In the GDPR, consent is presented as one of the possible legal bases for access and use of data implemented when there is an increased risk to the protection of individuals and their privacy.

unambiguous<sup>49</sup>. This strict implementation leads to the consideration of consent as a limit to data access and this limit is also underlined in relation to AI deployment. There is a balance between protection and innovation and the analysis of the literature sometimes points to a criticism of strict consent as a barrier to data access and use.

Informed consent cannot therefore be presented as a strict and immutable concept. The risk would be to empty this principle of all its essence with the emergence of consent fatigue due to a very large number of uses of data through the Internet, which a single person cannot control, for example . The risk is that consent is diminished in this digital world where one has to consent to each data processing, identified according to the purpose, by ticking boxes without really grasping all the information.

Therefore, a third dimension of the implementation of informed consent is to be considered in the context of AI. Indeed, the deployment of AI transforms certain risks for privacy and the preservation of human dignity and thus calls into question the effectiveness of certain fundamental rights. AI thus calls into question not only the purposes of the expression of consent but also its content and the form it should take in order to avoid automatically applying an inappropriate consent as a meaningless shield<sup>50</sup>.

It must be a broad and evolving concept that can be adapted to today's challenges<sup>51</sup>. The classical conception of consent must be transformed by promoting information to go beyond consent to trust in professional organizations, giving individuals the possibility to control the use of their personal data. The consent is then no longer formalized as it was traditionally and adapted to the specific challenges of AI<sup>52</sup> and DV.

Furthermore, considering an adapted form of consent to AI would allow the deployment of AI via a win-win use. Indeed, the deployment of AI can have an impact on informed consent that is not perceived under the classic prism of the risk involved. Indeed, AI can be seen as a tool to improve the autonomy of individuals by facilitating, for example, access to data and the monitoring of protective measures taken upstream. The person concerned could, depending on the use made of the AI model, benefit from better data monitoring. The deployment of AI could then favour and make relevant the implementation of a dynamic

---

<sup>49</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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), Article 4 and 7.

<sup>50</sup> Council of Europe, "Toward regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law", Study, December 2020.

<sup>51</sup> HEIKKILÄ Melissa, The Algorithm, MIT Technology Review, new letter of 5.01.2023.

<sup>52</sup> EU, Independent High Level Expert Group on Artificial Intelligence set up by the European Commission, "Ethics Guidelines for Trustworthy AI", guidelines, 2019.

consent<sup>53</sup> which would allow the data subject to become an actor in the deployment of AI models and to regain control of the data. Such consideration can only be effective if AI respects a certain level of transparency and if the individual is sufficiently included in the DV process.

## *2- Towards a reconsideration of classical forms of informed consent?*

The literature review carried out prior to this deliverable identified a point of convergence towards the need to develop consent by promoting information towards trust and proactive consideration of individuals<sup>54</sup>. Indeed, it emerged from this literature review that the most favored form of informed consent used is specific consent, most often written. However, this form of informed consent does not appear to be adapted to the challenges of AI and DV and forces us to reconsider the other forms of consent that could be applied<sup>55 56</sup>. Informed consent for the collection, storage and use of data can take several forms, listed below:

- **Opt-in Consent:** This form of consent requires individuals to actively and explicitly give their consent, for example by checking a box or clicking a button<sup>57</sup>.
- **Opt-out Consent:** With this form of consent, individuals must express their opposition explicitly<sup>58</sup>.
- **Specific Consent:** This is for example the form of consent required by the European Data Protection Regulation (GDPR) and requires clear and precise information to be provided to individuals so that they can freely consent to the processing of their data for a specific purpose, via a specific form<sup>59</sup>.
- **Layered or Multi-layered Consent:** This form of consent is composed of different layers of information, recipients or purposes<sup>60</sup>. Essential information can be

---

<sup>53</sup> **Towards dynamic informed consent** Henri-Corto Stoeklé, Jean-François Deleuze, Guillaume Vogt and Christian Hervé Med Sci (Paris), 33 2 (2017) 188-192 DOI: <https://doi.org/10.1051/medsci/20173302015>.

<sup>54</sup> Poster published at the 20th anniversary RDA Alliance.

<sup>55</sup> European Economic and Social Committee, Opinion European Economic and Social Committee on European Health Data Space, Communication from the Commission to the European Parliament and the Council. A European Health Data Space: harnessing the power of health data for people, patients and innovation. [COM(2022) 196 final], 3 May 2022.

<sup>56</sup> UNESCO, Recommendation on the Ethics of Artificial Intelligence, 24 November 2021.

<sup>57</sup> <https://bigid.com/blog/opt-in-vs-opt-out-consent/>

<sup>58</sup> <https://bigid.com/blog/opt-in-vs-opt-out-consent/>

<sup>59</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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), Article 4 and 7.

<sup>60</sup> Bunnik EM, Janssens AC, Schermer MH. A tiered-layered-staged model for informed consent in personal genome testing. Eur J Hum Genet. 2013 Jun;21(6):596-601. doi: 10.1038/ejhg.2012.237. Epub 2012 Nov 21. PMID: 23169494; PMCID: PMC3658183.

highlighted (layer 1) and then other optional information (layer 2) can be made accessible, for example<sup>61</sup>.

- **Dynamic Consent:** This form of consent is characterized by a willingness to make consent mutable and to adapt it as techniques and knowledge evolve for the same purpose<sup>62</sup>. It can take the form of personalized consent and communication platforms, allowing continuous communication and information. Different forms of consent can thus converge in the broader form of dynamic consent and thus allow the individual to evolve his or her decision-making<sup>63</sup>.
- **Broad Consent:** This is a form of consent that allows an individual to give broad consent to the use and re-use of their data for further research, for example, without further explicit consent from them<sup>64</sup>.

In addition, other, less traditional, conceptions of the form of consent can be mentioned here, such as that of "**Community consent**"<sup>65</sup>. This concept, developed in particular in genomic research, highlights the possibility of grouped consent, i.e. a whole community consenting together to the same purpose.

In addition to the form of the consent used, it can also be formalized in different ways, such as in paper or electronic format.

Finally, the implementation of informed consent may be required by law, for example in the field of medical research or where consent is the legal basis for data processing under the European Data Protection Regulation (GDPR).

Existing forms of consent can be applied in the context of data visitation. However, a truly relevant and protective use of informed consent requires adapting the modalities of implementation of consent to the purposes of data visitation. This reflection is in line with the modalities established by the GDPR which creates a consent purpose compatibility<sup>66</sup>

---

<sup>61</sup> Symons, TJ, Straiton, N., Gagnon, R. et al. Consumer perspectives on simplified multilevel consent for a pragmatic low-risk but complex trial. *Trials* 23 , 1055 (2022). <https://doi.org/10.1186/s13063-022-07023-z>.

<sup>62</sup> Budin-Ljøsne, I., Teare, HJA, Kaye, J. et al. Dynamic consent: a potential solution to some of the challenges of modern biomedical research. *BMC Med Ethics* 18, 4 (2017). <https://doi.org/10.1186/s12910-016-0162-9>.

<sup>63</sup> Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. Dynamic consent: a patient interface for 21st century research networks. *Eur J Hum Genet*. 2015;23(2):141-6.

<sup>64</sup> Antonio Sandu, [Ana Frunza](#) , Ethics in Research Practice and Innovation, Chapter 9 "Informed Consent in Research Involving Human Subjects, 2019, 21p.

<sup>65</sup> Developed countries should not impose ethics on other countries, *BMJ* 2002; 325:796 : <https://doi.org/10.1136/bmj.325.7368.796/a>.

<sup>66</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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), Recital 50.

AI and DV thus open a reflection on the most suitable form of consent. In this sense, some authors agree that the forms of Broad and Dynamic Consent could be more appropriate in the face of the challenges of AI and Big Data<sup>67</sup>.

Therefore, the choice of the extent and form of consent must be made in accordance with the legal and/or ethical framework applicable to the research, or even the methods used to achieve specific purposes.

## **II- Reconsiderations of the overall conditions of informed consent**

### *1. The confrontation of informed consent with explicability and transparency issues*

Informed consent should therefore be considered via a gold standard focused on the values of governance, explicability and transparency<sup>68</sup>. Such a reflection requires highlighting the "informed" dimension of consent. This consideration is essential and raises questions in itself with regard to the distinction between informed and enlightened consent. Information is therefore of considerable importance, both in its form and in its level of accessibility. Indeed, in order to retain the full conceptual value of informed consent, it is important to provide clear, fair and appropriate information to individuals<sup>69</sup>. However, the opaque dimension and the lack of explicability of AI systems, of their functioning, of the way data are analyzed, of the explanation of the results obtained, considerably limits the information transmitted. Indeed, it appears complicated to provide an individual with sufficient and clear information to enable him to consent in complete freedom. This is particularly true in the doctor-patient relationship<sup>70</sup>. This observation requires reconsidering the role and importance of information.

Furthermore, in addition to the data concerned, the recipients, the method implemented and the purposes pursued, information should also be provided on the risks inherent in the use of AI for the VIS. Individuals must be sufficiently aware and informed of the functioning, risks and purpose of AI to be able to give truly free and informed consent.

---

<sup>67</sup> Henri-Corto Stoeklé et al , Data Medicine: 'Broad' or 'Dynamic' Consent?, *Public Health Ethics* , Volume 15, Issue 2, July 2022, Pages 181-185, <https://doi.org/10.1093/phe/ phac014>.

<sup>68</sup> Human Rights Council, "Report of the High Commissioner for Human Rights A/HRC/48/31: The right to privacy in the digital age" (2021).

<sup>69</sup> UN, Report of the High Commissioner for Human Rights A/HRC/39/29 / *The right to privacy in the digital age*, 3 August 2018.

<sup>70</sup> Council of Europe, "The impact of artificial intelligence on the doctor-patient relationship", CDBIO Report by Brent Mittelstadt, June 2022.

In this sense the notion of transparency is essential. Only by knowing and understanding what the individual is submitting to can he or she be sure that he or she is acting and can act freely of his or her own accord. If there is a lack of transparency, privacy could be seriously undermined, as the individual would not be fully informed of interventions that could impede his or her ability to exercise his or her own autonomy<sup>71</sup>.

The principles of explicability and transparency then appear to be foundations of a human rights-based approach to global AI governance, as the development of "explainable AI" aims to ensure transparency on how AI algorithms process data and arrive at the solutions they provide<sup>72</sup>. This consideration requires a privacy by design conception of AI models to assert key ethical principles that must also be central to the content of information and consent.

## *2. Affirmation of ethical principles of use of AI and governance issues*

In this context, the creation of a new consent layer for AI requires an assessment of the principled application of ethics to the use of AI.

In order to ensure that the use of AI meets essential ethical principles and common values such as fairness, justice and autonomy. To this end, it is also important that the individual can regain control over the use of AI and its own data in order to ensure that it is used in a way that is consistent with the requirements of a society and a common good while protecting the individual<sup>73</sup>. Thus, as we have said, transparency, information and explicability are essential conditions for valid consent. In this sense, we note that the notion of self-determination stands out in the European texts studied. This consideration also contributes to the strengthening of the confidence that can be placed in the DV methods<sup>74</sup>. Moreover, a governance framework integrating these values must be specifically defined in order to ensure the effective application of such principles<sup>75</sup>.

We note that the ethical principles often mentioned concern the individual and respect for his or her autonomy, which is the very essence of the expression of consent. However, AI does not only impact the individual, but also society<sup>76</sup>: it is important to protect individual

---

<sup>71</sup> Andreotta, Kirkham and Rizzi, *AI, big data, and the future of consent*, p. 1721.

<sup>72</sup> Report A/HRC/43/29 of the Secretary-General: Report on the role of new technologies in the realization of economic, social and cultural rights, 5 March 2020.

<sup>73</sup> UE, Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, "Ethics Guidelines for Trustworthy AI", guidelines, 2019.

<sup>74</sup> <https://jme.bmj.com/content/48/1/3>

<sup>75</sup> <https://jme.bmj.com/content/48/1/3>

<sup>76</sup> <https://www.sciencedirect.com/science/article/pii/S0267364920300340>

decisions, perhaps through group actions, while protecting against the risks of discrimination or inequity.

On this point, it seems essential that the FAIR principles applicable to data, especially in the field of research, are also put forward in any DV process. These principles aim to ensure that research data is findable, accessible, interoperable and reusable, and therefore concern the characteristics of data to facilitate the sharing of quality data<sup>77</sup>.

The deployment of AI and DV is part of the development of digital techniques that reinforce certain vulnerabilities and give rise to new ones, such as lack of access and digital literacy or the reinforcement of existing social or biological inequalities for example<sup>78</sup>. Therefore, the application of the FAIR principles alone seems insufficient. Indeed, a generalised and common access to data can be done to the detriment of existing and new minorities reinforcing a lack or absence of representativeness<sup>79</sup>. Therefore, in addition to the FAIR principles, reflections are emerging on the deployment of CARE principles for data governance<sup>80</sup>. The CARE Principles for Indigenous Data Governance were developed by the Global Alliance for Indigenous Data in North America (GIDA) in 2019. This principle requires greater consideration for Indigenous peoples and communities who do not enjoy the full benefits of data access. However, we emphasise the importance of developing these principles as a tool to protect all vulnerable groups from the deployment of AI.

These principles help to highlight the role of data in innovation, but also in enhancing self-determination. The CARE principles build on the FAIR principles for data governance but combine consideration of the purposes of data with consideration of individuals and groups of individuals<sup>81</sup>. The deployment of the CARE principles responds to the issues of justice and equity but also raises new questions about the consideration of vulnerabilities in the context of AI. Is this conception the same? The affirmation of ethical principles plays a role in the content of informed consent. Similarly, the form of consent chosen should depend on the purposes and potential levels of risk assessed. However, considering these various elements does not appear to be sufficient without thinking about appropriate governance. The governance modalities are essential in order to guarantee the respect of the effectiveness of the consent without having to recontact the individuals each time and for each data visitation situation.

---

<sup>77</sup> <https://www.nature.com/articles/sdata201618>

<sup>78</sup> <https://journals.openedition.org/crdf/6462>

<sup>79</sup> <https://new.ogsl.ca/fr/principes-care/>

<sup>80</sup> <https://www.gida-global.org/care>

<sup>81</sup> <https://static1.squarespace.com/static/5d3799de845604000199cd24/t/637acdc59cc1b65057118e99/1668992455706/fgene-13-1052620.pdf>

### III- Specific Cases

#### 1. *Informed Consent in Human-Computer Interaction*

Advancements in AI paved the way for an intimate interaction between human individuals and technology. AI in both of its embedded (i.e., smart devices) and embodied (i.e., robotics) versions is increasingly integrated in human environments as cognitive extensions, becoming an inseparable part of how people survive and thrive in today's data-intensive world. But as pointed out in earlier discussions, the manner in which AI clandestinely collects and analyzes data in order to be effective extensions of human cognition, and the way in which they shape (or manipulate) decision-making processes of individuals as such extensions, challenges how informed consent could be possibly conceived and practiced in human-computer interaction (HCI).<sup>82</sup> However, what compounds the difficulty of exercising informed consent is the fact that AI continues to be an emerging technology, thereby the sociotechnological environment it brings about continues to evolve. Furthermore, HCI is also shaped by sociocultural factors that affect the way individuals put boundaries in their privacy.<sup>83</sup> Indeed, the study of informed consent in the context of HCI – particularly that of AI as cognitive extensions – is still nascent and in exploratory stage. So far there are two intertwined models for informed consent being explored in the area of HCI – FRIES and TEASE:

<b>FRIES Model of Informed Consent</b>	<b>TEASE Model of Informed Consent</b>
<b>Freely given</b> – “consenting is a choice you make without pressure or manipulation”	<b>Traffic Lights</b> – a “traffic lights system” denoting “stop”, “slow down”, and “continue”
<b>Reversible</b> – “anyone can change their mind about what they feel like doing, anytime”	<b>Establish ongoing dialogue</b> – “dialogue between participants around consent, boundaries and desire”

---

<sup>82</sup> Adam Andreotta, Nin Kirkham and Marco Rizzi, ‘AI, big data, and the future of consent,’ *AI and Society*, Vol. 37 (2022), 1721.

<sup>83</sup> See Pietro Romeo, ‘Cyber-Anthropology and Human-Computer Interaction: The Reshaping of Nature and Culture in a Technology-Mediated World,’ *Medium* (December 2018), Retrieved from <https://pietroromeo.medium.com/cyber-anthropology-and-human-computer-interaction-the-reshaping-of-nature-and-culture-in-a-3a4d8a7486>.

<b>Informed</b> – “You can only consent to something if you have the full story”	<b>Aftercare</b> – “participants check in after play, discussing how the ‘scene’ [interaction] met their expectation of consent and desire, or where limits may have been reached or breached”
<b>Enthusiastic</b> – “You should only do stuff you want to do, not things that you’re expected to do”	<b>Safewords</b> – “safewords are used to immediately withdraw consent; they can also be utilized to signal that one party is becoming uncomfortable”
<b>Specific</b> – “saying yes to one thing doesn’t mean you’ve said yes to others”	<b>Explicate soft and hard limits</b> – “hard limits are absolute prohibitions against certain activities, while soft limits denote something that is currently not allowed in the interaction but may be revisited and permitted under specific circumstances”

Source: Yolande Strengers et.al, ‘What Can HCI Learn from Sexual Consent?: A Feminist Process of Embodied Consent for Interactions with Emerging Technologies,’ *Association for Computing Machinery* (2021).

Scholars of HCI and privacy are of the view that the TEASE model is especially crucial in ensuring interaction of individuals and smart technologies – both embodied and embedded versions of AI – would bring about a relationship wherein the practice of informed consent based on FRIES model could be exercised, enhancing their sense of privacy and autonomy. However, in order to apply the TEASE model effectively, it would nonetheless require some innovations in the design of the smart technologies themselves. The primary design innovation that must be considered is that these technologies must be able to allow seamless exercise of “on going affirmation”, which means that consent is not just a requirement but rather an integral part of the entire interaction itself that ultimately helps enhance user experience.<sup>84</sup> Such design prevents coercing the user into consenting just to avail the services of the technology it likes to interact with.

---

<sup>84</sup> Strengers et.al, *What Can HCI Learn from Sexual Consent?*

Given so, the design must be able to integrate the “traffic lights system” in its interface that would allow the users to be part of directing how their respective interactions with smart AI technologies will go. This system in order to be effective foundation of the TEASE model would have to have a receptive design that provides a feedback mechanism, which not only intends to improve user experience but to do so in such a way that considers the soft and hard limits that the user is able to explicate during the interaction. Furthermore, besides being receptive to the limitations to which the user is comfortable with, the interaction would be more participative when it helps build user confidence towards the technology is when the user can review and understand the algorithmic models (i.e., addressing AI black box problem).<sup>85</sup> In this respect, incorporating TRUST (Transparency, Responsibility, User Focus, Sustainability, Technology) and CARE (Collective Benefit, Authority to Control, Responsibility and Ethics) principles throughout the AI life cycle to ensure the intelligibility and human-centeredness of algorithmic models.<sup>86</sup>

Besides the discussed receptivity and sensitivity, and algorithmic transparency, it is also helpful if the design – specifically that of embodied AI technologies – is able to provide these technologies capacity for social navigation in order to facilitate HCI that respects not only the limitations set by the individual but also the sociocultural realities that shapes how he or she perceives technology, and the boundaries he or she put in place in interacting with it.

However, as AI becomes increasingly sophisticated extensions of human cognition, there is also a growing concern that the TEASE model – even together with TRUST and CARE principles – would not be able to bring about the practice of informed consent in HCI in line with FRIES. As discussed earlier, the nature of AI technologies as cognitive extensions is a double-edge sword – their capability to act as part of human thinking comes from their effectiveness as tools for mind manipulation. This is demonstrated by the already prevalent use of AI as persuasive technologies for sustaining customer engagement and maximizing profit. Thus, there will always be an element of persuasion and deception in the interaction that compromises FRIES in three ways:

- (a) Considering that there is deception to begin with – shaping the mind of the user to think in a certain way – then it is questionable whether consent could be freely given;<sup>87</sup>
- (b) Given that the AI in this case – in order to perform what it is programmed to do – must obscure certain facts or functions, which prevents the user from being informed

---

<sup>85</sup> Alex Zhou, ‘Developing Trust in Black Box AI: Explainability and Beyond,’ *Wilson Center* (August 2022), Retrieved from <https://www.wilsoncenter.org/blog-post/developing-trust-black-box-ai-explainability-and-beyond>.

<sup>86</sup> See *UNESCO Recommendation on the Ethics of Artificial Intelligence*, November 24, 2021, 17-23.

<sup>87</sup> Strengers et.al, *What Can HCI Learn from Sexual Consent?*

of the whole picture as well as the opportunity to reverse any decision he or she might take, and to choose what specific interaction he or she would want to have;<sup>88</sup>

- (c) The fact that AI as smart persuasive technology manipulates users to primarily sustain engagement via appealing and amplifying their desires, it is therefore questionable whether users are genuinely enthusiastic in the course of their interaction with this technology.<sup>89</sup>

Accounting these three points, there is then a continuing need to explore technological innovations, which would be able to provide a kind of HCI with embedded and embodied AI technologies that can facilitate ongoing affirmation – integrating consent for the entire duration of the interaction – while ensuring that manipulation will not result to a sustainable and irreversible mind control. In other words, innermost emotions will not be used to hack the user's autonomy nor will brain structures be reconstituted to totally destroy his or her autonomy. In this case, redesigning AI to fit TEASE will no longer be sufficient, there must be another technology that must be introduced in the interaction that would be able to provide users the means to mitigate (or even escape) AI manipulation throughout the interaction process.

## 2. Informed Consent in Genomic Data Research

Under consideration

### **Part III - RECOMMENDATIONS AND GUIDELINES**

In general, the possible solutions seem to be a reconsideration of the classic form of informed consent to move towards a more flexible notion of trustful governance of self-determination, perhaps through a dynamic consent approach, but with greater emphasis on the obligations concerning information and privacy-friendly governance of data access.

More specifically, recommendations have been identified according to the actors involved.

#### ***Recommendations for States:***

- Incentivise and implement mechanisms to ensure accessible and sufficient information about the functioning, challenges and risks of the use of AI in order to allow for an improvement of knowledge in this area.

---

<sup>88</sup> Ibid.

<sup>89</sup> Ibid.

- Provide an adapted and harmonised framework for the implementation of AI for the deployment of Data Visitation methods
- Public consultation on AI and DV? On informed consent in the digital and research areas?
- Public information campaigns and educational programs for empowering and awareness people?
- Develop harmonised strategies for data governance, AI and informed consent frameworks that are continuous and sufficient.
- Develop an ethical approach to the use of AI in line with internationally and European recognised fundamental rights and principles.
- Develop standards for data sharing, data reuse and even data visitation.

***For legislators:***

- Consider the existing issues regarding the articulation of the frameworks in order to avoid the accumulation of regulations which leads to legal uncertainty and increased risk of non-compliance.
- Clarify the requirements for the use, the form and required content of consent for the deployment of AI and DV.
- Establish clear data access governance rules and guidelines for research activities in consultation with professional stakeholders and representatives of the civil society.

***For researchers:***

- Adapt the modalities and form of access to information and consent according to the technique, the regulatory requirements and the purposes pursued.
- Identify the most relevant form of informed consent according to the purposes pursued and adapt the information accordingly by providing details on the method, the issues and the risks.
- Work in collaboration with AI specialists to allow sufficient explicability of AI systems.
- Take into account vulnerable groups of people with a potential evolution of this consideration: in relation to the respect of informational integrity/privacy, we are not all equally vulnerable.
- Strive to implement the EU-like personal data minimisation approach, based on an assessment of the necessity of processing such data.

***For companies:***

- Raising awareness and ensuring respect for the fundamental rights of individuals, including privacy.

***For citizens:***

- Seize the challenges of AI deployment and DV methods by taking into account the risks but also the benefits for society (especially in the field of research).
- Affirm the expression of a common and citizen will on the identification of the purposes of AI use that citizens wish to see developed and the limits to be respected.

## Annex I

UN Guidance	Date	Recommendation(s)
-------------	------	-------------------

<p>Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda</p>	<p>November 2017</p>	<p>Adequate consent should be obtained prior to data collection or when the purpose of data re-use falls outside of the purpose for which consent was originally obtained.</p> <p>To ensure that consent is informed, it is recommended that as many details about the purpose of data use (e.g., any risks, harms and potential positive and negative impacts) should be included in the notice when the consent is sought.</p>
--	----------------------	--

<p>UNESCO Recommendation on the Ethics of Artificial Intelligence</p>	<p>November 24, 2021</p>	<p>Policy Area 3: Data Policy</p> <p>71. Member States should work to develop data governance strategies that ensure the continual evaluation of the quality of training data for AI systems</p> <p>72. Member States should strongly encourage all AI actors, including business enterprises, to follow existing international standards...to carry out adequate privacy impact assessments</p> <p>73. Member States should ensure that individuals retain rights over their personal data</p> <p>74. Member States should establish their data policies or equivalent frameworks, or reinforce existing ones</p> <p>75. Member States should promote open data...access to information and open government to reflect AI-specific requirements and promoting mechanisms, such as open repositories for publicly funded or publicly held data</p> <p>76. Member States should promote and facilitate the use of quality and robust datasets for training, development and use of AI systems</p> <p>77. Member States...adopt a digital commons approach to data where appropriate, increase interoperability of tools and datasets</p>
---	------------------------------	---