16 March 2022
Maastricht, The Netherlands

Data Protection as a Corporate Social Responsibility

Going beyond mere legal compliance to stimulate responsible data processing activities, enhance the effective protection of data subjects and their rights, and trigger virtuous competition in this field among organisations

Maastricht University
ECPC
European Centre on Privacy & Cybersecurity

© Maastricht University European Centre on Privacy & Cybersecurity 2022

Data Protection as a Corporate Social Responsibility Project

Abstract

This document summarizes the Maastricht University Data Protection as a Corporate Social Responsibility Framework (UM-DPCSR Framework) which has been developed in the context of a two-year multistakeholder research project[1] carried out at Maastricht University's European Centre on Privacy and Cybersecurity (ECPC). The idea of data protection as a corporate social responsibility was conceived by Prof. Dr. Paolo Balboni. It was first introduced on his personal blog in 2017 and then officially presented during his inaugural lecture on 10 May 2019. The related research project officially started on 1 January 2020 and was completed on 31 December 2021. The present document illustrates the key findings of the research which will be published in a forthcoming book. Organisations that wish to adhere to the UM-DPCSR Framework will also be provided with an implementation Toolkit. The UM-DPCSR Framework and the related implementation Toolkit will be updated on a regular basis by the authors in collaboration with a permanent Working Group.

Authors

Paolo Balboni
Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre on Privacy and Cybersecurity, Maastricht University Faculty of Law – Private Law

Kate Francis
PhD Candidate at the European Centre on Privacy and Cybersecurity, Maastricht University Faculty of Law

[1] The project is entitled "Data Protection as a Corporate Social Responsibility is the New Competitive Edge: Developing a New Dimension of Data Protection as a Corporate Social Responsibility".

Table of contents

1. About the Research Project

The digital revolution has transformed the global economy which is currently regulated through legislation such as the European Union's General Data Protection Regulation[2] (GDPR) and the ePrivacy Directive.[3] Hailed as one of the most stringent and protective data protection laws in the world, the GDPR takes a fundamental rights approach to the protection of personal data, provides clear rules for organisations, and reduces regulatory fragmentation.[4] Nearly four years from 25 May 2018 when the GDPR became applicable, however, the time has come to acknowledge that the Regulation itself and, more generally, mere legal compliance[5] cannot sufficiently protect the fundamental rights and freedoms that we uphold,

[2] The General Data Protection 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)

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

[4] European Commission. (n.d.). Data protection in the EU. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

[5] The authors have taken into consideration also the actual and forthcoming complementary legislations and policies on data, e.g., and non-extensively:

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010
- European Commission. (2022, February 23). A European Strategy for data. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/strategy-data
- European Commission. (2020, February 20). Data sharing in the EU – common European data spaces (new rules). Retrieved from https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Data-sharing-in-the-EU-common-European-data-spaces-new-rules-_en
- Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767
- Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN
- Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN
- Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final. Retrieved from https://ec.europa.eu/info/sites/default/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf
- 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 Legislative Acts, COM/2021/206 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
- European Commission. (2000, December 16). Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final). Retrieved from https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

especially in the European Union (EU), and adequately mitigate the risks presented by new technologies and the economic models that tend to degrade democratic systems in the exploitation of data.[6]

The need for an approach to data protection that can be considered 'ethical', espousing value-based models in the development of a newly virtuous form of social responsibility that goes beyond what is prescribed by the GDPR, has been confirmed by the European Data Protection Supervisor,[7] the European Commission,[8] and the Council of Europe,[9] among others.[10] The regulatory gap left by data protection legislation can be filled and the black boxes that drive the internet economy brought to light by fostering a socially responsible business culture around the use of data that embraces and goes beyond what is strictly required by the law, incentivising effective respect for the fundamental rights and freedoms of individuals. To this end, the UM-DPCSR Framework advances incentives for lawful, ethical, transparent, fair, and secure data processing to the advantage of both users and organisations.

The UM-DPCSR Framework is a feasible, practical, assessable, and importantly, implementable structure for the application of the concept of 'Data Protection as a Corporate Social Responsibility' within organisations. Our objective at ECPC is to trigger virtuous data protection competition between companies by creating an environment that identifies and promotes data protection as an asset which can be used to help companies to responsibly further their economic targets. The proposed UM-DPCSR Framework does not aim to avoid current or delay future legislation in any way. Instead, it aims to fill a gap which is presently left by the GDPR and still be there after the completion of the legislative process related to forthcoming data-related legislations and policies (e.g., the ePrivacy Regulation, the Artificial Intelligence Act, the Data Act, etc.).[11]

- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Retrieved from https://eur-lex.europa.eu/eli/dir/2016/1148/oj
- Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN
- Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, COM/2020/829 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN
- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881

[6] Anderson, J., & Rainie, L. (2020). Concerns about democracy in the digital age. *Pew Research Center Internet & Technology*. Retrieved from https://www.pewresearch.org/internet/2020/02/21/concerns-about-democracy-in-the-digital-age/.

[7] European Data Protection Supervisor. (2018, January 25). Report Towards a digital ethics – EDPS Ethics Advisory Group. Brussels, Belgium: EDPS. Retrieved fromS: https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

[8] European Commission. (2018). European Group on Ethics in Science and New Technologies Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems. Brussels, Belgium: European Commission. Retrieved from https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

[9] Council of Europe. (2017). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data adopted January 2017. Strasbourg, France: Council of Europe. Retrieved from. https://rm.coe.int/16806ebe7a.

[10] Balboni, P., Botsi, A., Francis, K., Taborda Barata, M. (2020). Designing Connected and Automated Vehicles around Legal and Ethical Concerns – Data Protection as a Corporate Social Responsibility. *In Proceedings of SETN 2020 Workshop on AI, Law and Ethics hosted by the 11th Hellenic Conference on AI special events section*.

[11] See footnote 5.

In essence, **the UM-DPCSR Project translates theoretical ethical principles into tangible and practical guidelines to build a solid framework for organisations to apply in order to foster transparency, accountability, fair, and secure data processing activities that positively contribute to the greater good of a sustainable data-driven economy and a democratic digital society.**

2. What is Corporate Social Responsibility?

Corporate Social Responsibility (CSR) is defined by the European Commission as the responsibility that companies take with respect to their societal impact.[12] As confirmed by the Proposal for a Directive on corporate sustainability due diligence, there is presently a material need for responsible and sustainable corporate conduct in global value chains.[13] This can be accomplished by following the law and fusing such legal compliance with human rights, ethical, environmental, and social considerations.[14] The aim of CSR is to do good, both in economic and social terms. This means acting in a way that is compatible with the greater goals of the organisation and also those of the society in which the organisation operates, creating "systemic linkages and interdependencies with stakeholders along the value chain"[15] in the context of data processing activities.

Engaging in CSR therefore means taking the legal framework as a given compliance baseline and moving beyond it by way of concrete strategies aiming to 'do good'. Like CSR, Environmental, Social and corporate Governance (ESG) aims to promote positive social actions by companies. ESG, however, also aims to quantify relevant efforts on the part of the organisation.[16] Following this logic, the UM-DPCSR Framework does not repeat what is already established in the European law, such as the GDPR and the ePrivacy Directive, but instead builds upon it to further what can be considered 'ethical' behaviours that benefit the involved stakeholders, in line with the concepts of CSR and ESG. Fundamentally, the Framework attempts to mitigate the negative privacy and data protection consequences of aggressive data-driven practices with the aim of creating a better digital society.

[12] European Commission. (n.d.). Corporate social responsibility & Responsible business conduct. Retrieved from https://ec.europa.eu/growth/industry/sustainability/corporate-social-responsibility-responsible-business-conduct_en

[13] European Commission (2022, February 23). Just and sustainable economy: Commission lays down rules for companies to respect human rights and environment in global value chains. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1145

14 European Commission. (n.d.). Corporate social responsibility & Responsible business conduct. Retrieved from https://ec.europa.eu/growth/industry/sustainability/corporate-social-responsibility-responsible-business-conduct_en

[15] Schönherr, N., Findler, F., & Martinuzzi, A. (2017). Exploring the interface of CSR and the Sustainable Development Goals. *Transnational Corporations,* 24(3): 33-49.

[16] Hung, C. (2021, September 23). Three Reasons Why CSR and ESG Matter to Businesses. *Forbes.* Retrieved from https://www.forbes.com/sites/forbesbusinesscouncil/2021/09/23/three-reasons-why-csr-and-esg-matter-to-businesses/#:~:text=Both%20terms%20relate%20to%20the,or%20quantify%20such%20social%20efforts.

3. Data Protection as a new form of Corporate Social Responsibility

It is common knowledge that many organisations view data protection laws and obligations as burdensome compliance requirements. At the same time, consumers (and individuals in general) are increasingly aware of privacy and data protection concerns, and more frequently are demanding sustainability and transparency from organisations they engage with and support.[17] According to research from the Morgan Stanley Institute for Sustainable Investing, the vast majority of millennials, 95 percent, have shown interest in sustainable investing (up from 86 percent in 2017).[18] With specific reference to information risk, consumer data protection can also be conceptualized as an aspect of sustainable and responsible behaviour, having the power to provide significant returns on investment (ROI).[19]

Recent studies demonstrate that investing in data protection pays off. The 2020 Cisco Privacy Benchmark Study ascertained that for each pound spent on privacy and data protection, "companies are getting £2.70 worth of improvements to their data loss mitigation, agility, innovation, customer loyalty and other key areas."[20] Indeed, by investing in data protection and embedding it into organisational practices, strategies, and stakeholder communication, both company finances and the greater public can benefit from increased protections and sustainability.

4. The Rules of the UM-DPCSR Framework and their application

The five Principles of socially responsible data protection[21] and the respective twenty-five rules of the UM-DPCSR Framework are illustrated in Table 1 below. An implementation Toolkit will be provided to

[17] *New Global Research from Accenture Interactive Urges CMOs to Put People Before Data Collection to Deliver a Better Digital Advertising Experience*. Accenture. (2019, October 16). Retrieved from https://newsroom.accenture.com/news/new-global-research-from-accenture-interactive-urges-cmos-to-put-people-before-data-collection-to-deliver-a-better-digital-advertising-experience.htm

[18] Morgan Stanley Institute for Sustainable Investing. (2019). *Sustainable Signals: Individual Investor Interest Driven by Impact, Conviction and Choice*. Retrieved from https://www.morganstanley.com/pub/content/dam/msdotcom/infographics/sustainable-investing/Sustainable_Signals_Individual_Investor_White_Paper_Final.pdf

[19] See Cisco. (2020). *Cisco Data Privacy Benchmark Study 2020 CISCO, From Privacy to Profit: Achieving Positive Returns on Privacy Investments*. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf?CCID=cc000160&DTID=esootr000515&OID=rptsc020143; also see Smith, A. (2022). Making the Case for the Competitive Advantage of Corporate Social Responsibility. *Business Strategy Series*, *8*, 186-195. doi: http://dx.doi.org/10.1108/17515630710684187.

[20] Cisco. (2020). *2020 Data Privacy Benchmark Study: Discover how organisations are benefiting from data privacy investments*. Retrieved from https://www.cisco.com/c/en_uk/products/security/security-reports/data-privacy-report-2020.html#~data-privacy-report

[21] Prof. Dr. Balboni first presented the five 'principles' which form the basis of the UM-DPCSR Framework during his inaugural lecture on Friday, 10 May 2019. See Maastricht University. (2019). *Inaugural lecture Paolo Balboni*. Retrieved from https://www.maastrichtuniversity.nl/news/inaugural-lecture-paolo-balboni

organisations[22] that wish to adhere to the UM-DPCSR Framework. By following the tangible and practical guidelines of the UM-DPCSR Framework, Organisations will be facilitated in their efforts to foster transparency, accountability, fair and secure data processing activities that positively contribute to the greater good of a sustainable data-driven economy and a democratic digital society. Every Organisation that wishes to adhere to the Framework will be required to appoint a **UM-DPCSR Framework Coordinator**, who is responsible for the correct implementation of the UM-DPCSR Framework within the Organisation.

The UM-DPCSR Framework has been primarily developed for businesses, but it can also be applied *mutatis mutandis* by other types of organisations.

UM-DPCSR Framework

Principle 1. Embed data protection, fairness, and security in the design of processes

Rule 1: Implement Data Security by Design. The Organisation shall implement Data Security by Design into its data processing activities throughout the whole life cycle. **"Keep it secure"**

Rule 2: Implement User Empowerment by Design. The Organisation shall actively empower individuals with respect to their data. **"Keep it user-centric"**

Rule 3: Implement Fairness by Design. The Organisation shall ensure that the fundamental rights to privacy and data protection are upheld by designing and developing systems that process personal data in a proportional, fair, and secure manner. **"Keep it fair"**

Rule 4: Implement 'Loyalty' by Design/Fiduciary commitment. The Organisation shall coherently apply the tenets of fiduciary commitment to data processing activities. **"Keep it loyal"**

Rule 5: Implement 'Digital Solidarity' to uphold human rights. The Organisation shall only apply business models that permit the fair, transparent, and secure use of data in a way that benefits society. **"Keep it solidary"**

Principle 2. Be transparent with individuals about the collection and further processing of their data

Rule 1: Before processing. The Organisation shall use icons (and sounds) for an easily visible, intelligible and clearly legible provision of information concerning the intended processing.

[22] The capitalized term 'Organisation' refers to Organisations which apply to be 'listed' in the UM-DPCSR Registry. See the Adherence to the UM-DPCSR Framework section below for more information.

Rule 2: During processing. Be transparent about how the processing (for example, fully automated decision making by algorithms) works. The Organisation shall implement new modalities that render the data processing transparent by way of, for example, the use of images, standardized icons, flashing lights, and sounds.

Rule 3: Be clear about how the Organisation benefits from the processing of data and the subsequent benefit for society derived from such processing. The Organisation shall be transparent about how it benefits from the data of individuals and how it provides benefits (fair in-kind value) to individuals or society at large.

Rule 4: Actively test the effectiveness of institutional transparency information (outward-facing privacy and data protection documentation) with individuals. The Organisation shall regularly assess the understandability of the information provided to individuals about the use of their data.

Rule 5: Regularly publish Transparency Reports. The Organisation shall publish reports which showcase how it informs individuals about the collection and further processing of their data and the effectiveness of the means used to convey such information.

Principle 3. Balance profits with the actual benefits for citizens

Rule 1: Carry out a Profitable and Beneficial Test (P&B Test). The Organisation shall carry out a P&B Test to evaluate how data processing activities benefit both the Organisation and society.

Rule 2: Engage with stakeholders to understand their values and beliefs when selecting suppliers. The Organisation shall survey stakeholders to find consensus in common goals and greater objectives.

Rule 3: Establish trusted data processing activities (for example, for use in AI and big data analytics) that actively oppose bias and discrimination. The Organisation shall actively seek not to cause harm.

Rule 4: Organise data processing activities in consideration of the environment and climate issues. The Organisations shall minimize data processing activities to actively contribute to the reduction of energy consumption and carbon emissions along the value chain.

Rule 5: Carry out a Materiality Assessment. The Organisation shall carry out materiality assessments at regular intervals to ensure alignment with ever-changing social, economic, and environmental needs.

Principle 4. Publish relevant findings based on statistical/anonymized data to improve society

Rule 1: Business to Consumer Data Sharing. The Organisation shall make findings derived from data known to consumers by way of understandable and useful Digital Society Insights Reports. **"B2C Data Sharing"**

Rule 2: Business to Business Data Sharing. The Organisation shall engage in or establish secure and transparent data collaboratives with relevant peer-stakeholders to improve the analytical potential of the data in its possession. **"B2B Data Sharing"**

Rule 3: Business to Government Data Sharing. The Organisation shall actively seek to provide the public sector with relevant data-based insights. **"B2G Data Sharing"**

Rule 4: Business to Research Data Sharing. The Organisation shall engage in business to scientific research data sharing to provide data to sustainable innovation initiatives, following the FAIR data principles. **"B2R Data Sharing"**

Rule 5: Business to Humanitarian Action Data Sharing. Engage in business to humanitarian aid data sharing to support humanitarian actions. **"B2H Data Sharing"**

Principle 5. Devote a portion of revenues to awareness campaigns for citizens with regards to the data-centric society

Rule 1: Invest in digital social capital to promote social enterprise within the Organisation. The Organisation shall make use of digital and data-driven tools to engage internal stakeholders with the aim of positively contributing to the Organisation.

Rule 2: Allocate a portion of revenue to be devoted to awareness campaigns, in and outside of the Organisation. The Organisation shall implement a metric/model that will identify an adequate portion of revenue to be devoted to awareness campaigns.

Rule 3: Develop a yearly data awareness program. The Organisation shall make a programme available to individuals with clear objectives regarding data protection and cyber-/data-security literacy.

Rule 4: Contribute to digital educational initiatives for youth. The Organisation shall carry out concrete actions to further education about data protection rights and cybersecurity hygiene for youngsters.

Rule 5: Actively promote the protection of individuals in relation to data practices. The Organisation shall devise specific outreach programs on disinformation, fake news, and data-driven threats.

Table 1: UM DPCSR Framework

5. Adherence to the UM-DPCSR Framework

The UM-DPCSR Framework consists of five principles and 25 rules which are conceptualized as assessable controls.

From 1 April 2022, ECPC will start accepting submissions from Organisations that would like to adhere to the Framework. In the meantime, enquiries and manifestations of interest can be sent to Prof. Dr. Paolo Balboni at paolo.balboni@maastrichtuniversity.nl.

ECPC has adopted a 'listing' approach for adherence to the Framework wherein Organisations are listed in a public database - the **UM-DPCSR Registry** - under three different statuses:

1. **Applicant** status;
2. **In-Progress** status; and
3. **Implemented** status).

In 2023, third-party verification by accredited auditors will also be provided.

Upon completion of the submission - which may be subject to a yearly contribution to be listed in the **UM-DPCSR Registry** - Organisations will also receive:

1. **access to the UM-DPCSR Toolkit** (practical guidelines to implement the UM-DPCSR Framework);
2. **training/coaching for the UM-DPCSR Coordinator** in charge of implementing the Framework within the Organisation; and
3. **use of the UM-DPCSR seal** (once the Organisation has implemented the Framework).

ECPC will sample a fixed percentage of the Organisations listed with respect to their UM-DPCSR compliance posture each year and adopt remedies with respect to potential issues in the listed Organisations by, e.g.:

- **notifying the Organisation of a need for remediation** within, e.g., 15 days for minor infractions (clerical mistakes, inconsistencies);
- **suspend the listing**, pending compliance with identified minor substantial gaps;
- **revoke the listing** in case of substantial non-compliance.

NOTE: The UM-DPCSR Framework is neither a certification under Article 42 GDPR nor a code of conduct under Article 40 GDPR. In fact, the scope of the Framework is not to certify and/or further specify compliance with the GDPR. This is because the UM-DPCSR Framework presumes GDPR compliance and goes one step further to require that Organisations process personal data in a fair, transparent, ethical, secure, and sustainable manner with a clear commitment to actively promote data protection rights and cybersecurity hygiene within the digital society.

6. The UM DPCSR Rules with short explanation

This section provides a short description of each UM-DPCSR Rule. It does not specifically refer to the

controls which constitute the Rules. Instead, the following descriptions are intended to provide the reader with a general conceptualization of the UM-DPCSR Rules themselves.

Principle 1. Embed data protection, fairness, and security in the design of processes

Principle 1. Embed data protection, fairness, and security in the design of processes

Rule 1: Implement Data Security by Design. The Organisation shall implement Data Security by Design into its data processing activities throughout the whole life cycle. **"Keep it secure"**

The first Rule of Principle 1 of the UM-DPCSR Framework calls for the Organisation to implement Data Security by Design into its data processing activities. This Rule recalls the fundamental importance of data security as an enabler of both technological advancements and consumer trust.[23] Individuals must be able to trust the technologies they use and the providers with whom they share their data. This stems from the necessity of individuals to be relatively certain that the confidentiality and integrity of their personal information will be adequately protected by the Organisation throughout the whole life cycle (e.g., from collection to the deletion of the data).

Data security is a fundamental prerequisite for ethical and fair data processing. To foster the propagation of new innovations, questions related to security concerns must first be successfully addressed. Adopting a 'by design' approach to security in this context means integrating security best practices into the modus operandi of the Organisation at the Organisational level (in terms of building a culture of security awareness inside the Organisation) and the technical level (in terms of the design of products and services which should take security into due account).[24]

The Organisation, both when acting as data controller and as data processor, will implement this Rule by way of meeting adequate requirements that contain the pre-requisites for Data Security by Design. Such requirements will be embedded into the Organisation's workflows for the provision of goods and services, building on the Confidentiality, Integrity, Availability (CIA) Triad[25] frequently applied in the field of information security. More precisely, through the application of 'Janusian' thinking[26] in the implementation

[23] See European Union Agency for Cybersecurity. (2020). *Artificial Intelligence: Cybersecurity Essential for Security & Trust*. Retrieved from https://www.enisa.europa.eu/news/enisa-news/artificial-intelligence-cybersecurity-essential-for-security-trust.
Also see Balboni, P. (2020). AI & Cybersecurity: Reflections on a multidimensional relationship [Blog]. Retrieved from https://www.paolobalboni.eu/index.php/2020/10/20/ai-cybersecurity-reflections-on-a-multidimensional-relationship/

[24] See, e.g., European Union Agency for Cybersecurity. (2022). *Data Protection Engineering: From Theory to Practice*. European Union Agency for Cybersecurity. Retrieved from https://www.enisa.europa.eu/publications/data-protection-engineering

[25] European Union Agency for Cybersecurity. (2016). *Guidelines for SMEs on the security of personal data processing*. European Union Agency for Cybersecurity. Retrieved from https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

[26] Janus, the Greek god of doors and gates, of beginnings and endings, has most often been depicted as a man with two heads, each head facing in an opposite direction. The intrinsic benefit of such a 'Janusian' dual perspective, and thus the underlying

of the UM-DPCSR Rules, data security will coexist with the rights to privacy and the protection of personal data, and fairness and ethics will co-exist in the data-related/driven activities of the Organisation, not only fulfilling accountability expectations, but going beyond them to make net positive decisions that consider the interest and the expectations of the data subjects, the users or stakeholders of the specific Organisation. The performance of concrete actions in this way by the implementing Organisation are intended to increase trust on the part of consumers and foster profitability and value in the long-term.[27]

Principle 1. Embed data protection, fairness, and security in the design of processes

Rule 2: Implement User Empowerment by Design. The Organisation shall actively empower individuals with respect to their data. **"Keep it user-centric"**

The second Rule of the first Principle of the UM-DPCSR Framework concerns the implementation of User Empowerment by Design, actively empowering individuals with respect to their data and related processing activities. More precisely, this calls for the implementation of processing activities that effectively empower individuals to manage their activity and space in the digital arena to foster self-determination. This means putting individuals in control and ensuring that accessibility and ability-based design are duly considered.[28]

This conceptualization fundamentally moves the attention of the Organisation and its designers and product developers from the mere concentration on the technology itself towards the end user of the technology – the individual.[29] The European Data Protection Supervisor in EDPS *Opinion 9/2016 on Personal Information Management Systems: Towards more user empowerment in managing and processing personal data* also provides useful context to this end in stressing the fundamental concept that individuals must be in control of their data, meaning, for example, that algorithms and AI need to be

power of Janusian thinking, is precisely that it allows multiple perspectives to be simultaneously considered. Janusian thinking is about brining opposites together but at the same time, keeping them there, taking into considerations pros, cons, how they interact, etc., in order to then develop something which is both novel and useful. Therefore, it allows for the exploration of new, surprising ways to unite opposing theories ('AND' instead of 'OR' thinking). It permits new non-linear and innovative approaches to traditional subjects, as opposed to applying what can be deemed as 'standard' or proven compromises and solutions. In this way, we can move away from traditional dichotomies such as 'Knowledge vs./OR Privacy' or 'Security vs./OR Privacy', to 'Knowledge, Security AND Privacy'. See, e.g., Paradoxical thinking skills. (2016). Retrieved 9 March 2022, from https://www.pallikkutam.com/edu-landscape/paradoxical-thinking-skills and Barrett, D. (1997). *The Paradox Process: Creative Business Solutions...Where You Least Expect to Find Them*. New York: AMACOM).

[27] OECD (2019). *OECD Business and Finance Outlook 2019: Strengthening Trust in Business*, OECD Publishing, Paris. https://doi.org/10.1787/af784794-en.

[28] Ladner, R. (2015). Design for User Empowerment. *Interactions*. Retrieved from https://dl.acm.org/doi/pdf/10.1145/2723869

[29] See p. 3, Gallula, D. and Frank, A.J. (2014). User Empowering Design. In Proceedings of the 2014 European Conference on Cognitive Ergonomics (ECCE '14). *Association for Computing Machinery*, New York, NY, USA, Article 38, 1–3. DOI:https://doi.org/10.1145/2637248.2742999

human and user-centric. [30] User Empowerment by Design therefore goes beyond user-centric design and aims to ensure that from the design stage that the empowerment of the individuals is taken into consideration by inventors and developers.

This Rule shall be applied by implementing Organisations acting as controller or processor. The Organisation is required to establish a bespoke **User Empowerment by Design Program** to ensure that questions related to user empowerment, including accessibility, are considered and addressed throughout the product/service lifecycle, starting from the R&D and design conceptualization phases. The Programme will be comprised of policies and procedures, prior assessments, and *ex post* verification protocols to ensure that the requirements of user empowerment are met, including ensuring that products and services are accessible.

Through the establishment of the **User Empowerment by Design Program**, users will have more control over their data and of the related processing activities, experiencing true self-determination. The Organisation that is able to successfully implement this Rule will, in the long-term, benefit from increased trust from individuals and, therefore, the likelihood of sustained support for the Organisation will be augmented.

Principle 1. Embed data protection, fairness, and security in the design of processes

Rule 3: Implement Fairness by Design. The Organisation shall ensure that the fundamental rights to privacy and data protection are upheld by designing and developing systems that process personal data in a proportional, fair, and secure manner. **"Keep it fair"**

The third Rule of the UM-DPCSR Framework requires the Organisation adhering to the Framework to implement Fairness by Design into its data processing activities. The concept of Fairness by Design[31] plays an important role in the conceptualization of a socially responsible data protection methodology.[32] The processing of personal data may hinder various fundamental rights, especially when new and pervasive technologies such as algorithmic processing, machine learning techniques and big data and smart analytics are used to carry out automated decision-making activities.[33] Examples of this are hate-speech detection

[30] European Data Protection Supervisor. (2016). *Opinion 9/2016 on Personal Information Management Systems: Towards more user empowerment in managing and processing personal data*. Brussels: EDPS. Retrieved from https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

[31] The concept of Fairness by Design has been developed and promoted by Prof. Dr. Paolo Balboni, who first launched the idea on his blog in 2018. See Balboni, P. (2018). Cambridge Analytica and the Concept of Fairness by Design [Blog]. Retrieved from https://www.paolobalboni.eu/index.php/2018/07/16/cambridge-analytica-and-the-concept-of-fairness-by-design/

[32] Mr. Davide Baldini, Researcher, at the department of law of the University of Florence who wrote his Master thesis on "EU Data Protection Legislation: Between Promoting the Internal Market and Protecting Fundamental Rights", significantly contributed to the UM-DPCSR Framework with reference to the *Fairness by Design* Rule included in the study.

[33] See Article 22 GDPR. Also see Article 29 Working Party. (2017). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017 as last Revised and Adopted on 6 February 2018* and Global Privacy Assembly. (2021). *Working Group on Ethics and Data Protection in Artificial Intelligence Report*. Retrieved from

software, which has been found to discriminate African Americans,[34] the automatic filtering of content within internet platforms, which may hinder freedom of expression, or anti-fraud algorithms which are often biased against the less affluent, and so on.[35] Fairness by Design ultimately pursues to interpret the GDPR in a way that enables the law to effectively regulate algorithmic processing by implementing procedural safeguards aimed at providing individuals and society with a high level of protection against harm to fundamental rights and societal welfare.

Data processing, and specifically automated decision-making, which is becoming increasingly common with the proliferation of new technologies, presents novel challenges to the rights of individuals, making it more important for technologies to not only serve a practical function, but to be fair and 'good' in doing so. Fairness by Design leverages the often overlooked but very relevant principle of fairness[36] set forth in Article 5(1)(a) GDPR. In doing so, it introduces elements of ethics and user empowerment within the data protection legal framework. On the one hand, Fairness by Design aims to regulate and prevent undue individual and societal harm, which may arise, for example, as a consequence of algorithmic processing, machine learning techniques, and the use of big data and smart analytics resulting in automated decision-making.[37] On the other hand, the concept is based on the data protection by design principle, as set forth in Article 25 GDPR, which prescribes that processing activities should embody data protection principles in their very design, thereby including fairness.

In other words, Fairness by Design fundamentally calls for systems to be designed and developed in a responsible manner, implementing technical and Organisational measures to process personal data in a proportionate way and, more generally, to ensure that the fundamental rights to privacy and data protection are upheld.[38] Moreover, it is widely acknowledged that data security represents a fundamental prerequisite to trustworthy and ethical data processing, as without the adoption of a risk-based approach that aids in the management of data security, the social and economic benefits of digital technologies cannot be fully implemented.[39]

---

https://edps.europa.eu/system/files/2021-10/1.3f-version-4.0-ethics-and-data-protection-in-ai-working-group-adopted_en_0.pdf

[34] Coldewey, D. (2019). Racial bias observed in hate speech detection algorithm from Google. *TechCrunch*. Retrieved from https://techcrunch.com/2019/08/14/racial-bias-observed-in-hate-speech-detection-algorithm-from-google/

[35] For an analysis concerning fundamental rights which might be endangered by automated decision-making see p. 29 and the following of Council of Europe. (2019). *Council of Europe study DGI(2019)05,* Responsibility and AI (pp. 29-98). Council of Europe. Retrieved from https://rm.coe.int/responsability-and-ai-en/168097d9c5,

[36] Art. 8(2) of the Charter of Fundamental Rights of the European Union provides that (emphasis added) "*Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.*"

[37] See Article 22 GDPR. Also see Article 29 Working Party. (2017). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017 as last Revised and Adopted on 6 February 2018* and Global Privacy Assembly. (2021). *Working Group on Ethics and Data Protection in Artificial Intelligence Report*. Retrieved from https://edps.europa.eu/system/files/2021-10/1.3f-version-4.0-ethics-and-data-protection-in-ai-working-group-adopted_en_0.pdf

[38] International Conference of Data Protection and Privacy Commissioners. (2018). *Declaration on Ethics and Data Protection in Artificial Intelligence*. Brussels. Retrieved from https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_ai-declaration_adopted_en_0.pdf

[39] High-Level Expert Group on Artificial Intelligence. (2020). *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*. Retrieved from https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment. Also see p. 17 European Commission. (2018). *Ethics and data protection*. Retrieved from https://ec.europa.eu/info/sites/default/files/5._h2020_ethics_and_data_protection_0.pdf

Therefore, **the concept of Fairness by Design is to be considered as three-fold, in that it embodies legal, ethical and security elements into the processing of personal data.**

Figure 1: Fairness by Design triangle

Fairness by Design broadly entails that, when designing or implementing a new processing activity, its impact on individuals' rights and interests, and on societal welfare at large, are taken into account in order to avoid undue limitation of fundamental rights. In this respect, Fairness by Design transcends what is strictly prescribed by the law, while at the same time the concept is grounded within primary (Article 8 par. 2 of the Charter) and secondary European Union legislation (GDPR).

It is apparent that there is more at stake than only the right to privacy, as already recognized by Article 1(2) GDPR, which generally refers to the protection of the "fundamental rights and freedoms of natural persons" as one of the two aims of the GDPR (the other one being the free flow of personal information within the European Union). At the same time, however, the GDPR has been criticized as not being fully equipped to combat algorithmic discrimination, unfairness and bias.[40] The main reason for this lies in the fact that the law was conceived to address personal data processing of a static nature, where personal data are sourced from the data subject or a third party and subsequently processed for a predetermined purpose; however, in an algorithmic setting, personal data are continuously inferred from other information and used to make predictions and decisions about individuals.[41] In other words, the GDPR is mostly concerned with regulating input data, while in today's world, inferred data are gaining more and more importance each day that passes. Even Article 22 GDPR, which specifically addresses the regulation of automated decision-making, presents various shortcomings, mostly due to its narrow scope of application.[42]

As noted above, multiple rights and freedoms can be hindered by the processing of personal data. In this respect, the more automated the processing is (i.e., the more a decision is taken in an automated fashion without meaningful human intervention), the more it risks seriously encroaching upon fundamental rights.

[40] See, *inter alia*, Goodman, B. (2016). Discrimination, Data Sanitisation and Auditing in the European Union's General Data Protection Regulation. *European Data Protection Law Review, 2*(3). doi: https://doi.org/10.21552/EDPL/2016/4/8

[41] Wachter, S. (2019). Data Protection in the Age of Big Data. *Nature Electronics, 2*.; Mantelero, A. (2014). The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. *Computer Law & Security Review, 30*(6), 643-660. doi: 10.1016/j.clsr.2014.09.004

[42] Baldini, D. (2019). Article 22 GDPR and prohibition of discrimination. An outdated provision?. Retrieved 8 March 2022, from https://www.cyberlaws.it/2019/article-22-gdpr-and-prohibition-of-discrimination-an-outdated-provision/

In this context, the relevant human rights which reflect common European values, shared by all EU Member States and institutions, are those listed in the Charter, as specified in their explanations and in the relevant case-law of the Court of Justice of the European Union. However, the (intertwined) rights to liberty (Article 6), private life (Article 7), freedom of thought (Article 10) and of expression (Article 11), as well as the right to non-discrimination (Article 21) are deemed to be especially relevant when automated profiling is involved.

Examples of automated decision-making activities which may hinder those rights include fraud detection and creditworthiness algorithms, which may disproportionately impact the poor, algorithms on social risk which may impact minorities by reinforcing bias and prejudices, news filters on social platforms which may hinder freedom of expression, and so on.[43] Even seemingly more mundane processing activities, such as behavioural or targeted advertising, may relevantly impact individual rights,[44] such as freedom of thought where the targeting is too precise, continuous, or where it involves special category data (see for example the micro-targeting which has taken place in the Cambridge Analytica case[45]).

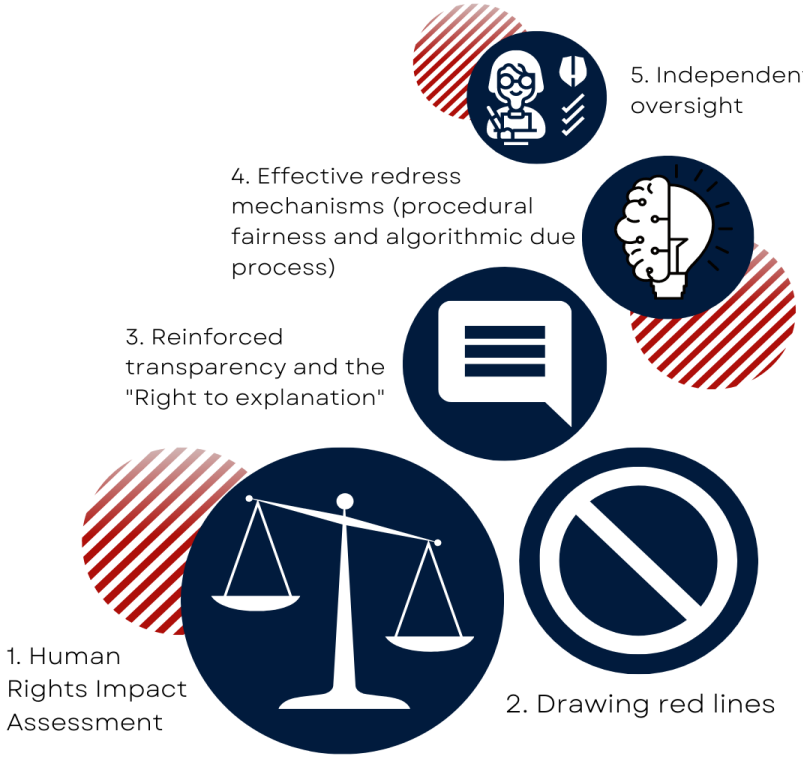


Figure 2: Five requirements of Fairness by design

[43] Lee, N., Resnick, P., & Barton, G. (2019). *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*. Brookings Institution. Retrieved from https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

[44] See Wiewiórowski, W. (2022). It is time to target online advertising. Retrieved 14 March 2022, from https://edps.europa.eu/press-publications/press-news/blog/it-time-target-online-advertising_en. To this end, also see the recent case of the Belgian Data Protection Authority against IAB Europe: Belgian Data Protection Authority. (2022). *The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR*. Retrieved from https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr

[45] Information Commissioner's Office. (2018). *Investigation into the use of data analytics in political campaigns Investigation update*. Retrieved from https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf

In accordance with this Rule, the Organisation shall embed Fairness by Design into its activities by integrating five steps into the life cycle of data processing activities which involve the use of automated processing, including profiling.[46] The Organisation will accomplish this by:

1. performing human rights impact assessments;
2. drawing red lines for certain types of processing that pose a significant threat to human rights and risk a severe and irreversible impact on fundamental rights and societal welfare in general;
3. providing reinforced transparency and the right to a meaningful explanation;
4. putting in place effective redress mechanisms (procedural fairness and algorithmic due process);
5. ensuring independent oversight over relevant data processing activities.

Principle 1. Embed data protection, fairness, and security in the design of processes

Rule 4: Implement 'Loyalty' by Design/Fiduciary commitment. The Organisation shall coherently apply the tenets of fiduciary commitment to data processing activities. **"Keep it loyal"**

The implementation of 'Loyalty' by Design is the 4th Rule of Principle 1. 'Loyalty' by Design entails the conceptualization and coherent application of a fiduciary commitment for privacy and data protection. The two concepts are closely related. Loyalty, which entails trust, such as that established between a beneficiary and a trustee,[47] is what Gold calls "a hallmark of the fiduciary relationship."[48]

This Rule is inspired by the duty of loyalty in fiduciary relationships and represents a way to go beyond mere legal compliance to the benefit of users. The fiduciary duty of loyalty is nothing new, in fact, it has been considered a linchpin of American corporate law for centuries.[49] In the context of the UM-DPCSR Framework, however, this Rule shall be applied in information relationships where, typically, there is a power imbalance, such as between the controller and the data subject.

As Richards and Hartzog have proposed as way to reform the American legal privacy and data protection landscape along these trustful lines:

[46] As defined under Article 4(4) GDPR.

[47] Fiduciary. (2022). *Oxford Reference*. Retrieved from https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095816799

[48] Gold, Andrew S., The Loyalties of Fiduciary Law (December 20, 2013). Philosophical Foundations of Fiduciary Law, Andrew S. Gold & Paul B. Miller, eds., Oxford University Press, 2014, Forthcoming, Available at SSRN: https://ssrn.com/abstract=2370598

[49] See p. 1076, Rauterberg, G., & Talley, E. (2017). Contracting Out of the Fiduciary Duty of Loyalty: An Empirical Analysis of Corporate Opportunity Waivers. *Columbia Law Review, 117*(5), 1075-1152. Retrieved from https://columbialawreview.org/content/contracting-out-of-the-fiduciary-duty-of-loyalty-an-empirical-analysis-of-corporate-opportunity-waivers/

> Trust - the willingness to accept vulnerability to the actions of others - is the essential ingredient for friendship, commerce, transportation, and virtually every other activity that involves other people. It allows us to build things, and it allows us to grow. Trust is everywhere, but particularly at the core of the information relationships that have come to characterize our modern, digital lives. Relationships between people and their ISPs, social networks, and hired professionals are typically understood in terms of privacy. But the way we have talked about privacy has a pessimism problem - privacy is conceptualized in negative terms, which leads us to mistakenly look for 'creepy' new practices, focus excessively on harms from invasions of privacy, and place too much weight on the ability of individuals to opt out of harmful or offensive data practices.[50]

Implementing Principle 1, Rule 4, 'Loyalty' by Design/Fiduciary commitment therefore means applying the rationale put forward by Richards and Hartzog. It entails using privacy as an opportunity to move away from a negative conceptualization of it to promote positive, sustainable information relationships by fostering trust.[51] In this way, trust becomes a guiding principle for privacy relationships.[52] It should be pointed out that this must be genuine trust, i.e., "Trust that is accountable".[53] As suggested by Balkin,

> The logic of fiduciary obligations holds that the greater the imbalance of power, the greater the asymmetries of information, the greater the degree of control over the client's environment, and the greater the client's vulnerability, the greater the need for fiduciary obligations becomes.[54]

Following this logic, society will benefit from the Organisation promoting accountable trust[55] and privacy rules will contribute to both building trust and moving away from a negative conceptualization of privacy to promote positive, sustainable information relationships.[56]

Cheffins has suggested that the duty of loyalty has the potential to cultivate what can be considered as a "protective environment for investors" where the "misappropriation of corporate assets, 'sweetheart' deals between a company and its insiders, and other types of managerial self-dealing will potentially constitute breaches of duty."[57] In the climate of accountable trust within the UM-DPCSR Framework, failing to adequately secure data, failing to be transparent about processing activities and the benefits gained by the Organisation, and failure to empower users and comply with Fairness by Design would corrode trust and

---

[50] See p. 431, Richards, N., & Hartzog, W. (2016). Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review*, *431*(9), 431-471

[51] See Ibid. p. 432. Richards and Hartzog also note that, "Thinking about privacy in terms of trust also reveals a principle that should become a new bedrock tenet of privacy law: Loyalty. Rejuvenating privacy law by getting past Privacy Pessimism is essential if we are to build the kind of digital society that is sustainable and ultimately beneficial to all— users, governments, and companies."

[52] See Ibid. pp. 435-436.

[53] See Ibid. p. 459.

[54] See p. 26, Balkin, J. (2020). The Fiduciary Model of Privacy. *Harvard Law Review Forum*, *134*(11). Retrieved from https://harvardlawreview.org/wp-content/uploads/2020/10/134-Harv.-L.-Rev.-F.-11.pdf

[55] See p. 469, Richards, N., & Hartzog, W. (2016). Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review*, *431*(9), 431-471

[56] Ibid. See also the theory of "Warranted Trust" developed by Balboni in his book Balboni, P. (2009). *Trustmarks in E-Commerce: The Value of Web Seals and the Liability of their Providers*. T.M.C. Asser Press.

[57] See p. 464 Cheffins, B. (2001). Does Law Matter? The Separation of Ownership and Control in the United Kingdom. *The Journal of Legal Studies*, *30*(2), 459-84, as seen on p. 1077 in Rauterberg, G., & Talley, E. (2017). Contracting Out of the Fiduciary Duty of Loyalty: An Empirical Analysis of Corporate Opportunity Waivers. *Columbia Law Review*, *117*(5), 1075-151

irreparably damage the fiduciary relationship between the data controller and the data subject in violation of this Rule.

In practical terms, to implement this Rule, the Organisation will need to structure its processing activities in a way that promotes positive, respectful and sustainable data exchanges with individuals aimed at building trustworthy relationships. This could be, e.g., that the Organisation will make efforts to increase what we might call 'genuine' transparency (see Principle 2); that it will draw red lines for certain types of processing that pose a significant threat to human rights and risk having severe and irreversible impacts on fundamental rights and societal welfare in general (see Principle 1, Rule 3); avoiding data processing activities that are not (also) in the interest of data subjects (see Principle 3, Rule 1);[58] moving away from putting the burden of making complex decisions with limited information on data subjects.[59] Furthermore, under this Rule, Organisations will need to actively seek to safeguard the privacy of individuals from both the government and other private entities, understanding that "The fiduciary model treats this approach as more than simply good public relations; it is required by the duties of care, confidentiality, and loyalty to end users".[60]

Principle 1. Embed data protection, fairness, and security in the design of processes

Rule 5: Implement 'Digital Solidarity' to uphold human rights. The Organisation shall only apply business models that permit the fair, transparent, and secure use of data in a way that benefits society. **"Keep it solidary"**

The fifth Rule of the UM-DPCSR Framework requires the Organisation adhering to the Framework to Implement 'Digital Solidarity' to uphold human rights. The implementing Organisation will adhere to this Rule by saying 'no' to harmful business models that do not promote fair, transparent, secure, and beneficial (for the society) use of data. This notion strongly builds on of Fairness by design (Principle 1 Rule 3) and 'Loyalty' by Design/Fiduciary commitment (Principle 1, Rule 4) as well as Principles 3, 4 and 5.

In the EDPS Strategy 2020-2024, "Shaping a Safer Digital Future: A New Strategy for a New Decade", European Data Protection Supervisor Wojciech Rafał Wiewiórowski declared that

> Europe must uphold its values in the digital world, but, as much as we need 'sovereignty', the EU also needs **digital solidarity - making data work for all people across Europe's borders, especially for the most vulnerable. Digital solidarity would refuse to replicate the now tarnished and discredited business models of constant surveillance and targeting, which have been damaging the trust in the digital society.**

[58] P. 436, Richards, N., & Hartzog, W. (2016). Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review, 431*(9), 431-471

[59] Ibid.

[60] See pp. 19-20 Balkin, J. (2020). The Fiduciary Model of Privacy. *Harvard Law Review Forum, 134*(11). Retrieved from https://harvardlawreview.org/wp-content/uploads/2020/10/134-Harv.-L.-Rev.-F.-11.pdf

> This means, engaging with the EU industrial policy to **boost privacy enhancing technologies, designed in Europe and exported around the world**. It is about using all the available tools, not just data protection enforcement, but also taxation and international trade, to foster a fairer and more sustainable digital Europe.[61]

It is imperative under the understanding promoted by the EDPS above, and in compliance with this Rule, to actively anticipate future trends, in an attempt to be ahead of the game, to foresee risks to the rights and freedoms of data subjects with respect to activities of the Organisation to foster digital solidarity. This Rule thus requires the Organisation to respond to any foreseen digital human rights issues and to take immediate action to mitigate unforeseen and unforeseeable harms when realized.

In particular, express attention must be paid to vulnerable groups (e.g., children, elderly people, employees, marginalized groups, women, new readers/beginning readers, etc.), inclusivity and free speech should be encouraged and at the same time, both cyberbullying and trolling should be contrasted.[62] Regard should also be given to the potential of control and manipulation as Michelle Bachelet, UN High Commissioner for Human Rights eloquently stated, "by-products of a legitimate drive for efficiency and progress."[63]

Figure 3: Digital Solidarity

Digital solidarity under the UM-DPCSR Framework focuses on vulnerable data subjects

[61] P. 5, European Data Protection Supervisor. (2022). *The EDPS Strategy 2020-2024: Shaping a Safer Digital Future*. Brussels: EDPS. Retrieved from https://edps.europa.eu/press-publications/publications/strategy/shaping-safer-digital-future_en

[62] As UN High Commissioner for Human Rights Michelle Bachelet noted in her Keynote speech at the Japan Society in New York on 17 October 2019, "A lot of our attention is rightly focused on challenges to freedom of expression online and incitement to hatred and violence. Online harassment, trolling campaigns and intimidation have polluted parts of the internet and pose very real off-line threats, with a disproportionate impact on women. In the most deadly case, social media posts targeted the Rohingya community in Myanmar in the run-up to the mass killings and rapes in 2017. Human rights investigators found that Facebook – and its algorithmically driven news feed – had helped spread hate speech and incitement to violence." Human rights in the digital age - Can they make a difference? Bachelet, M. (2019). *Human rights in the digital age - Can they make a difference?*. Speech, Japan Society, New York. Retrieved from https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25158&LangID=E

[63] Ibid.

At the start of the UM-DPCSR compliance program, i.e., the initial stage in which the Organisation implements the UM-DPCSR Framework, the client-impacting data processing activities of the Organisation included in the Article 30 GDPR Record of Processing Activities should be evaluated according to the controls of this Rule and such evaluation should be adequately documented by the DPCSR Coordinator in accordance with accountability requirements under the Framework. Following this first phase, the Organisation should evaluate all new projects which entail the processing of personal data according to the criteria of this Rule to ensure that human rights and digital solidarity are fostered.

Principle 2. Be transparent with individuals about the collection and further processing of their data

Principle 2. Be transparent with individuals about the collection and further processing of their data

Rule 1: Before processing. The Organisation shall use icons (and sounds) for an easily visible, intelligible and clearly legible provision of information concerning the intended processing.

The second principle of the UM-DPCSR Framework aims to stimulate transparency with citizens concerning the collection, and therefore processing, of their data. The first Rule of Principle 2 calls for the Organisation to be transparent about data processing activities *before* processing takes place, i.e., before collection. One of the primary aims of the forthcoming Maastricht DPCSR Framework is found in the cardinal principle of transparency, which can be improved with the help of visual aids such as data protection icons.

Under the GDPR, data subjects must be informed about the processing of their personal data. For example, when relied upon as a legal basis, consent must be freely given, *informed*, *specific*, and require a positive (opt-in) action.[64] Very often, however, the exercise of personal autonomy through the provision of consent is all but informed. This is largely due to inaccessibility (e.g., resulting from difference in reading levels, information asymmetry, legalese, dark patterns, etc.).[65]

[64] See Articles 4(11), 6(1)(a) 7, 8, 9(2)(a) and Recitals 32, 38, 40, 42, 43, 171 GDPR. Also see the European Data Protection Board. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020*. EDPB. Retrieved from https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
Consent. (2022). Retrieved 8 March 2022, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

[65] See, e.g., Bashir, M., Hayes, C., Lambert, A. D., & Kesan, J. P. (2015). Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology*, *52*(1), 1-10. https://doi.org/10.1002/pra2.2015.145052010043;
Krumay, B., & Klar, J. (2020). Readability of Privacy Policies. *Data And Applications Security and Privacy XXXIV*, 388-399. doi: 10.1007/978-3-030-49669-2_22.; and

In order to provide information on data processing activities in a clear and plain, intelligible and easily accessible way, the accessibility of the 'average' user must be considered. Language that may be important for one individual may be out of reach for another, but the right to privacy and data protection is a right that all individuals are endowed with. This means that it is necessary to provide for different ways to communicate privacy information, for example, through data protection icons.

The Article 29 Working Party (WP29) Guidelines on transparency[66] under Regulation 2016/679, endorsed by the European Data Protection Board,[67] confirm the utility of a multi-layered approach to information provision with the aim of improving transparency to data subjects, recalling Recital 60 GDPR which states that information to the data subject can be provided together with standardised icons.[68] The WP29 however, notes that, **"the use of icons should not simply replace information necessary for the exercise of a data subject's rights nor should they be used as a substitute to compliance with the data controller's obligations under Articles 13 and 14."**[69] This is clearly stated in Article 12(7) GDPR, which, in reference to icons reads,

> The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

Following this logic, and with the goals of furthering sustainable and transparent data processing and stimulating the provision of comprehensive, manageable, and meaningful information to individuals, two sets of icons have been developed under the UM-DPCSR Framework, seen in Figure 4 below.

Also see New York Times. (2020). What's Going on in This Graph? | Internet Privacy Policies. Retrieved from https://www.nytimes.com/2020/01/02/learning/whats-going-on-in-this-graph-internet-privacy-policies.html#:~:text=Privacy%20policies%20describe%20data%20that,1400%20(high%20college%20level.

[66] Concerning the fact that Article 12 GDPR specifies that information to data subjects shall be provided "in writing or by other means", the WP29 specifies that:
"Under Article 12.1, the default position for the provision of information to, or communications with, data subjects is that the information is in writing. (Article 12.7 also provides for information to be provided in combination with standardised icons and this issue is considered in the section on visualisation tools at paragraphs 49 to 53). However, the GDPR also allows for other, unspecified "means" including electronic means to be used. WP29's position with regard to written electronic means is that where a data controller maintains (or operates, in part or in full, through) a website, WP29 recommends the use of layered privacy statements/ notices, which allow website visitors to navigate to particular aspects of the relevant privacy statement/ notice that are of most interest to them (see more on layered privacy statements/ notices at paragraph 35 to 37). However, the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (whether in a digital or paper format) which can be easily accessed by a data subject should they wish to consult the entirety of the information addressed to them. Importantly, the use of a layered approach is not confined only to written electronic means for providing information to data subjects. As discussed at paragraphs 35 to 36 and 38 below, a layered approach to the provision of information to data subjects may also be utilised by employing a combination of methods to ensure transparency in relation to processing." See WP29 Guidelines on transparency under Regulation 2016/679, Page 27.

[67] The EDPB replaced the Article 29 Working Party and is comprised of representatives from the Data Protection Authorities of European Union Member States.

[68] See p. 25, Article 29 Working Party. (2017). *Guidelines on transparency under Regulation 2016/679 Adopted on 29 November 2017 as last Revised and Adopted on 11 April 2018*. Retrieved from https://ec.europa.eu/newsroom/article29/items/622227/en

[69] Ibid.

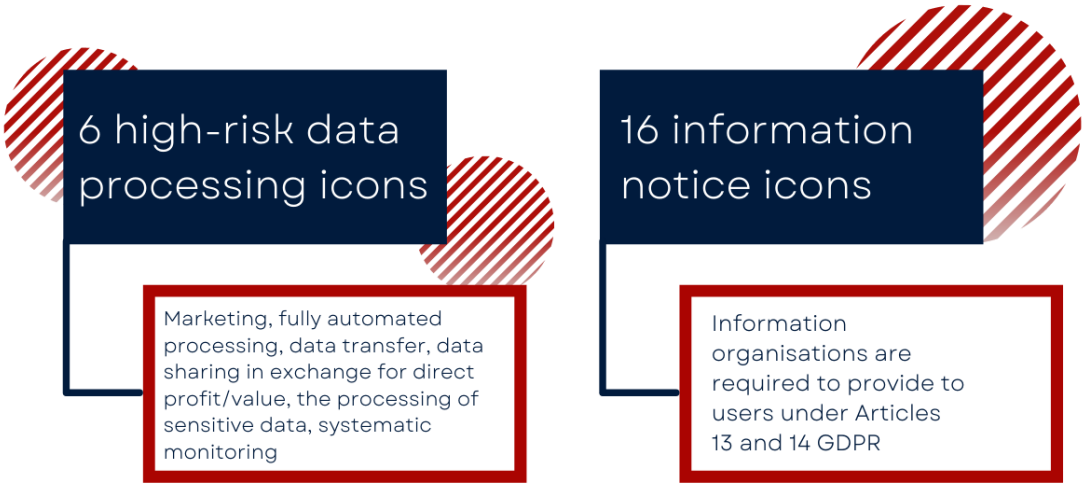


Figure 4: UM-DPCSR Icons

In 2020, the UM-DPCSR Icon Working Group[70] (Icon WG), comprised of the researchers from ECPC and Stakeholders from the UM-DPCSR project with UX design expertise, developed six UM-DPCSR data protection icons[71] for potentially high-risk processing activities. The six high-risk data processing icons include marketing, fully automated processing, data transfer, data sharing in exchange for direct profit/value, the processing of sensitive data, and systematic monitoring. Once more specific indications are provided from EU Authorities with respect to the preferred format of machine-readability, the icons shall be rendered machine-readable by the implementing Organisation, in accordance with the provisions of the GDPR.[72]

[70] The Icon WG was comprised of Paolo Balboni, Kate Francis and Sarah Bakir (Privacy Coordinator CIOO | CIOO First Line Risk – Center of Expertise Risk – Rabobank), Luuk Beursgens (UX Strategist at Rabobank), Valentina Fiorendi (Visual - UX/UI Designer - @ Diennea - MagNews), Joost Haar (UX Designer - Rabobank), Fabio Masini (Chief Technology Officer Manager @ Diennea - MagNews), and Michela Parziale (Digital Consultant Manager @ Diennea - MagNews.

[71] Balboni, P., & Francis, K. (2020). Maastricht University Data Protection as a Corporate Social Responsibility (UM DPCSR) Research Project: UM DPCSR Icons Version 1.0. Retrieved 8 March 2022, from https://www.maastrichtuniversity.nl/maastricht-university-data-protection-corporate-social-responsibility-um-dpcsr-research-project-um

[72] See Article 12(7) GDPR and Recital 60 GDPR which require icons which are presented electronically to "be machine-readable." As the WP29 points out in its Guidelines on Transparency, the GDPR does not provide a definition of "machine-readable". However, "Recital 21 of Directive 2013/37/EU17 defines 'machine- readable' as: 'a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats.'" For more details on the definition of machine readability, see, e.g., European Union Agency for Cybersecurity. (2022). Data Protection Engineering: From Theory to Practice. European Union Agency for Cybersecurity. Retrieved from https://www.enisa.europa.eu/publications/data-protection-engineering
Rossi, A., & Palmirani, M. (2019). DaPIS: a Data Protection Icon Set to Improve Information Transparency under the GDPR. Bologna: Università di Bologna, CIRSFID. Retrieved from http://gdprbydesign.cirsfid.unibo.it/wp-content/uploads/2019/01/report_DaPIS_jan19.pdf

Organisations adhering to the UM-DPCSR Framework should use the UM-DPCSR icons where appropriate, e.g., on websites and apps, both within registration and purchase forms and within layered privacy notices, and also during fully automated processing pursuant to Principle 2, Rule 2 (see below). These icons, developed according to a scientific methodology developed by the researchers and tested with users in an extensive survey,[73] are intended to be used together with privacy notices, to give users an immediate understanding that certain high-risk processing activities are taking place. The so-called 'high-risk' processing data protection icons shall be used by organisations adhering to the UM-DPCSR Framework to actively provide a signal to users, potentially making individuals more aware of what happens to their data. **Please refer to Annex A to see the UM-DPCSR high-risk processing icons**.

Complementary to the high-risk processing icons, in the context of participation to the Italian Data Protection Authority's "Easy privacy information via icons? Yes, you can!" data protection icons contest,[74] the Icon WG also developed a further 16 icons that correspond to the information Organisations are required to provide to users under Articles 13 and 14 GDPR. The authors submitted the 16 icons to the Italian Data Protection Authority in the spring of 2021 together with a presentation of the methodology and rationale behind their development. The UM-DPCSR Icons were selected among the winners of the Italian Authority's contest.[75] These icons should be implemented by the Organisation within privacy policies and information notices where appropriate.

The UM-DPCSR Icon WG's data protection icons comply with the requirements deduced from the WP29 Guidelines on transparency under Regulation 2016/679:

1. Icons shall not replace information to be provided to data subjects;[76]
2. Icons shall provide an "give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing";[77]
3. Icons shall be presented in various contexts,[78] and when "are presented electronically they shall be machine-readable";[79]

[73] Balboni, P., & Francis, K. (2021). Help us improve transparency online and build a better digital society - Help us improve transparency online and build a better digital society - Maastricht University. Retrieved 8 March 2022, from https://www.maastrichtuniversity.nl/help-us-improve-transparency-online-and-build-better-digital-society

[74] Informative chiare. (2021). Retrieved 8 March 2022, from https://www.garanteprivacy.it/temi/informativechiare

[75] Ibid. Also see Balboni, P., & Francis, K. (2021). Easy privacy information via icons? Yes, you can! - Easy privacy information via icons? Yes, you can! - Maastricht University. Retrieved 8 March 2022, from https://www.maastrichtuniversity.nl/easy-privacy-information-icons-yes-you-can

[76] As part of a layered privacy notice, the WP29 states that, "Other possible ways to convey the information to the data subject arising from the following different personal data environments may include the following modes applicable to the relevant environment... Screenless smart technology/ IoT environment such as Wi-Fi tracking analytics: icons, QR codes, voice alerts, written details incorporated into paper set-up instructions, videos incorporated into digital set-up instructions, written information on the smart device, messages sent by SMS or email, visible boards containing the information, public signage or public information campaigns". See WP29 Guidelines on transparency under Regulation 2016/679, page 21.

[77] See Recital 60 GDPR and WP29 Guidelines on Transparency under Regulation 2016/679, para. 50

[78] In its Transparency Guidelines, the WP29 clarifies that there may be situations where icons are not presented electronically, for example "icons on physical paperwork, IoT devices or IoT device packaging, notices in public places about Wi-Fi tracking, QR codes and CCTV notices." See para. 51

[79] See Recital 60 GDPR and WP29 Guidelines on Transparency under Regulation 2016/679, para. 50

4. The symbols and images used in the development of icons shall be universally used and recognized in the EU;[80]
5. The icons shall be evidence-based.[81]

Please see Annex B at the end of this document for more information on the UM-DPCSR Data Protection Icons, which should be implemented in the privacy policies and information notices of the Organisation adhering to the Framework.

Principle 2. Be transparent with individuals about the collection and further processing of their data

Rule 2: During processing. Be transparent about how the processing (for example, fully automated decision making by algorithms) works. The Organisation shall implement new modalities that render the data processing transparent by way of, for example, the use of images, standardized icons, flashing lights, and sounds.

The second rule of Principle 2 requires Organisations to be transparent with users *during* processing. It calls for the Organisation adhering to the UM-DPCSR Framework to be transparent about how the processing (for example, algorithm) works. The closely related principles of openness, trust, and transparency are not only pillars of democracy,[82] but also of data protection law. In fact, one of the most relevant *fil rouge* in the GDPR is found in transparency. Applied in the context of EU data protection law, individuals are endowed with the right to know how their personal data is collected and used.

Transparency, however, is challenged in the context of online privacy policies and terms and conditions of use which are complex and are often not read.[83] Particular difficulties in applying the principle of transparency are also found in new and emerging technologies which present hurdles both in terms of logical compliance and in terms of adhering to ethical and transparency-related principles. Applications often process data in the background without users being aware of such processing taking place. For example, a mobile app may track the geolocation of a user even when the app is not open, or a smart TV

[80] As previously mentioned, this requirement represents a challenging obstacle as symbols change with time and those which are identifiable for individuals of certain age groups may not be for others. Furthermore, it shall be noted that resemblance icons (e.g., shopping cart) may allow for easier recognisability for users as Efroni et al. have stated. See page 365, Efroni, Z., Metzger, J., Mischau, L., & Schirmbeck, M. (2019). Privacy Icons: *European Data Protection Law Review, 5*(3), 352-366. doi: 10.21552/edpl/2019/3/9

[81] In its Guidelines on Transparency, the WP29 notes that that "the development of a code of icons should be centred upon an evidence-based approach and in advance of any such standardisation it will be necessary for extensive research to be conducted in conjunction with industry and the wider public as to the efficacy of icons in this context." The Researchers of the DPCSR project have established and documented a common and scientific, evidence-based methodology to be used in the development of the icons identified herein whose efficacy shall be tested by the WG.

[82] Gurría, A. Openness and Transparency - Pillars for Democracy, Trust and Progress - OECD. Retrieved 8 March 2022, from https://www.oecd.org/unitedstates/opennessandtransparency-pillarsfordemocracytrustandprogress.htm

[83] Hart, K. (2019). Privacy policies are read by an aging few. Retrieved 8 March 2022, from https://www.axios.com/few-people-read-privacy-policies-survey-fec3a29e-2e3a-4767-a05c-2cacdcbaecc8.html

may constantly record an individual's watching habits without them being aware of it. Organisations wishing to act transparently should therefore demonstrate compliance by clearly informing users when they are collecting and processing data in a way that is evident to individuals.

According to the Rule, the Organisation shall implement new modalities that render the data processing transparent by way of, for example, the use of images, standardized icons, flashing lights,[84] and sounds, or other transparency-enhancing practices. This Rule is closely related to the one that proceeds it and encourages the use of the UM-DPCSR icons, images, and other modalities appropriate to the technology under consideration to be used.[85] During processing and after consent has been provided, where appropriate, the Organisation should actively remind the individual of what is being done with their data, taking care, however, to not overwhelm or burden them with excessive notifications.

With the aim of promoting accountability, the Organisation shall make a conscious effort to ensure transparency during processing by providing information or signals to individuals when data processing is taking place. This is especially relevant in situations in which the individual may not expect their data to be processed or may not remember that processing is taking place (e.g., such as in the examples of geolocation tracking, monitoring by smart TVs, etc. provided above). This can be accomplished in certain contexts with the use of icons, animation, lights, sounds, and push notifications, among others.

The Organisation shall furthermore ensure that information notices/privacy policies (both internal and external-facing) are transparent by writing them with clear and plain language (i.e., using age and target-appropriate language, avoiding terms like 'may', 'might', 'some',[86] etc.), making use of new formats for privacy policies (e.g., displaying key terms in FAQs, using a scrollable text box, providing small amounts of information at opportune times, using illustrations and comics, nudging users to read by telling them that it is their last chance, telling individuals how long it will take them to read the policy, etc.[87]). For example,

[84] Taking relevant precautions with respect to, e.g., individuals with epilepsy.

[85] For example, for connected objects and the Internet of Things, it may be appropriate for the Organisation to use sounds or lights in order to signal that data processing is taking place.

[86] In its Guidelines on Transparency, (see para. 12) the WP29 provides the following as examples of "Poor Practice":
"We may use your personal data to develop new services (as it is unclear what the 'services' are or how the data will help develop them);
We may use your personal data for research purposes (as it is unclear what kind of 'research' this refers to); and
We may use your personal data to offer personalised services (as it is unclear what the 'personalisation' entails)."
The same WP29 also provides the following examples of good practice:
"'We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in' (it is clear that what types of data will be processed, that the data subject will be subject to targeted advertisements for products and that their data will be used to enable this);
'We will retain and evaluate information on your recent visits to our website and how you move around different sections of our website for analytics purposes to understand how people use our website so that we can make it more intuitive' (it is clear what type of data will be processed and the type of analysis which the controller is going to undertake); and
'We will keep a record of the articles on our website that you have clicked on and use that information to target advertising on this website to you that is relevant to your interests, which we have identified based on articles you have read' (it is clear what the personalisation entails and how the interests attributed to the data subject have been identified)."

[87] Behavioural Insights Team. (2019). *Best practice guide Improving consumer understanding of contractual terms and privacy policies: evidence-based actions for businesses*. London: Behavioural Insights Ltd. Retrieved from https://www.bi.team/wp-content/uploads/2019/07/BIT_WEBCOMMERCE_GUIDE_DIGITAL.pdf

privacy and security labels may be used for IoT devices to help warn users about potential risks in relation to the processing of their personal data.[88]

Principle 2. Be transparent with individuals about the collection and further processing of their data

Rule 3: Be clear about how the Organisation benefits from the processing of data and the subsequent benefit for society derived from such processing. The Organisation shall be transparent about how it benefits from the data of individuals and how it provides benefits (fair in-kind value) to individuals or society at large.

The third Rule of Principle 2 is very much related to Principle 3, Rule 1 (Carry out a Profitable and Beneficial Test). In fact, Principle 2, Rule 3 can be seen as the transparency requirement complementary to the substantial requirement set forth in Principle 3, Rule 1. Coherently, the Organisation adhering to the Framework shall be clear about:

1. how the Organisation benefits from the processing of data;
2. how the Organisation provides benefits to individuals, e.g., fair in-kind value with respect to the services and products it offers them.

The notion of providing fair in-kind value in exchange for data does not call for the Organisation to provide a financial benefit to individuals, but instead calls on the Organisation to consider the benefit it receives from the data provided by users and to make such information known to the individual.[89]

This Rule necessitates that the Organisation is transparent about the data that it collects from individuals and how it benefits from the data. This, in turn, will give individuals greater agency and control over their data. The Organisation is also required to communicate to individuals what their related benefits are or what the benefit for the society at large is (as per Principle 3 Rule 1). This can translate in fair in-kind value in terms of, e.g., better products/services being offered, thus not necessarily in terms of economic value. This also has the potential to increase consumer trust and therefore even provide the Organisation with expanded access to data thanks to such trust.

Being transparent about how Organisations benefit from the processing of data will permit for the alignment of the interests of the individuals with those of the Organisation – e.g., by understanding the benefits of data processing activities for the Organisation, the data subject or individual can understand if

[88] Shen Y., Vervier P.A. (2019). IoT Security and Privacy Labels. In: Naldi M., Italiano G., Rannenberg K., Medina M., Bourka A. (eds) Privacy Technologies and Policy. APF 2019. Lecture Notes in Computer Science, vol. 11498. Springer, Cham. https://doi.org/10.1007/978-3-030-21752-5_9

[89] This Rule has also been inspired by the California Consumer Privacy Act which establishes that businesses can offer a fair value financial incentive for the provision of personal information, requiring them to calculate the value for the business. For more information, see CCPA, 1798.125. at https://oag.ca.gov/privacy/ccpa. Also see California Attorney General Rob Bonta. (2022). *On Data Privacy Day, Attorney General Bonta Puts Businesses Operating Loyalty Programs on Notice for Violations of California Consumer Privacy Act*. Retrieved from https://oag.ca.gov/news/press-releases/data-privacy-day-attorney-general-bonta-puts-businesses-operating-loyalty

they genuinely want to agree to certain data processing, allowing them to demand fair in-kind value for the provision of their data (see Principle 2, Rules 1 and 2).

Being clear about how the Organisation benefits from data means avoiding the use of vague language and genuinely explaining to individuals how the company uses their data to generate value, especially when processing, further use, or sharing is not reasonably expected by the individual. The Organisation shall make all the purposes and the means of the processing genuinely transparent, i.e., which data is used for R&D, marketing, how the service is improved, etc. This Rule is not about endorsing the monetization of personal data, but instead is to be understood as a mechanism for increasing transparency by fostering an understanding of how data is used in the provision of services and making the benefits for the stakeholders known so that individuals can truly exercise self-determination.

Principle 2. Be transparent with individuals about the collection and further processing of their data

Rule 4: Actively test the effectiveness of institutional transparency information (outward-facing privacy and data protection documentation) with individuals. The Organisation shall regularly assess the understandability of the information provided to individuals about the use of their data.

Rule 4, Principle 2 calls on the implementing Organisation to test the effectiveness of outward facing privacy documentation with users. This is in line with what the Article 29 Working Party suggests in its Guidelines on Transparency Under Regulation 2016/679,[90] but which may not be done frequently in practice. By testing information with stakeholders of the Organisation, more genuine transparency can be achieved by Organisations, which will translate into furthered trust.

Article 12(1) GDPR calls for controllers to

> take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, **intelligible** and **easily accessible** form, using **clear and plain language**, in particular for any information addressed specifically to a child.

The testing of privacy policies can, as the Article 29 Working Party has underlined in its Guidelines on Transparency, help controllers to meet the requirement of 'intelligible' information, which is related to the provision of information using clear and plain language, essentially means that the policy should be understood by the "average member of the intended audience".[91] As Krumay and Klar note, the readability of information has the power to impact the behaviour of individuals.[92] Indeed, it is paramount for

[90] Article 29 Working Party. (2017). *Guidelines on transparency under Regulation 2016/679 Adopted on 29 November 2017 as last Revised and Adopted on 11 April 2018*. Retrieved from https://ec.europa.eu/newsroom/article29/items/622227/en

[91] Ibid. para. 9

[92] See p. 388, Krumay, B., & Klar, J. (2020). Readability of Privacy Policies. *Data And Applications Security and Privacy XXXIV*, 388-399. doi: 10.1007/978-3-030-49669-2_22. Also see Singh, R., Sumeeth, M., & Miller, J. (2011). Evaluating the Readability of Privacy Policies in Mobile Environments. *International Journal of Mobile Human Computer Interaction*, *3*(1), 55-78. doi: 10.4018/jmhci.2011010104

individuals to *comprehend* privacy information in order for them to ensure that their rights are protected and that they are able to provide, where appropriate, informed consent to data processing.

While Organisations may be familiar with their target users or audiences, it has become common knowledge that most policies are drafted by lawyers or by machines and are either ripe with language and concepts which are too technical or legal or standardised and fairly generic.[93] The state of the art of privacy policies therefore renders intelligibility a significant challenge which can be tackled in part by testing, e.g., "through mechanisms such as user panels, readability testing, formal and informal interactions and dialogue with industry groups, consumer advocacy groups and regulatory bodies, where appropriate, amongst other things".[94] Data controllers may also wish to experiment with diverse forms of user testing which may include standard accessibility and readability tests, hall tests, or by actively "seek[ing] feedback on how accessible, understandable and easy to use the proposed measure is for users".[95]

Testing in this sense can also be understood as an action that demonstrates compliance with the fundamental principle of accountability. Under this Rule, the Organisation shall establish a testing protocol with which it can verify the functionality of its privacy and data protection information with users to improve intelligibility and a genuine understanding on the part of users. Outward-facing information notices should be tested as appropriate in accordance with the testing protocol.

Principle 2. Be transparent with individuals about the collection and further processing of their data

Rule 5: Regularly publish Transparency Reports. The Organisation shall publish reports which showcase how it informs individuals about the collection and further processing of their data and the effectiveness of the means used to convey such information.

Principle 2, Rule 5 of the UM-DPCSR Framework requires the implementing Organisation to publish Transparency Reports that inform users about how the Organisation collects and further process the data of individuals, what it is doing to protect their data, and the effectiveness of the means used to provide the relevant information to them. Transparency reporting is a matter of CSR and by implementation of this Rule, becomes an authentic tool to permit individuals to measure the trustworthiness of a company. In general terms, transparency reports provide important information to users about government access requests and surveillance, making them aware of potential threats concerning the freedom of expression and privacy.[96]

[93] Ibid.

[94] See para. 9 Article 29 Working Party. (2017). *Guidelines on transparency under Regulation 2016/679 Adopted on 29 November 2017 as last Revised and Adopted on 11 April 2018*. Retrieved from https://ec.europa.eu/newsroom/article29/items/622227/en

[95] Ibid. para. 25

[96] See, e.g., AccessNow. (2021). *Transparency Reporting Index*. Retrieved from https://www.accessnow.org/transparency-reporting-index/; Pegoraro, R. (2019). Tech Companies Are Quietly Phasing Out a Major Privacy Safeguard. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2019/09/what-happened-transparency-reports/599035/; and

Transparency reports can also be an important instrument to demonstrate accountability and to foster trust.[97] However, the information contained in such reports is frequently provided 'in numbers', e.g., "Company A received 2,619 requests for access from the US government in 2021"; they may be difficult to understand, and lack adequate standardization.[98] For these reasons, transparency reports often fail to successfully inform individuals about the true extent to which companies are subject to government interference and importantly, do not adequately showcase what organisations are doing to protect users and ensure respect of their fundamental rights.[99]

Transparency reports have been around for more than a decade.[100] In 2011, Google published the first ever transparency report.[101] Reports can vary in the topics covered, for example, content moderation,[102] government requests for access to data, intellectual property and copyright, removal requests, disruptions to operations, etc. Research has demonstrated that the publication of annual transparency reports is concentrated in North America and despite update in the practice since 2011, as of July 2021, a mere 88 companies in the entire world have published such reports.[103] According to the digital civil rights non-profit AccessNow, "Transparency reporting is one of the strongest ways for technology companies to disclose threats to user privacy and free expression."[104] In the context of content moderation, the relevance of such reporting is particularly evident.[105] It is clear, however, that in order for an organisation to capture the value of such reporting, the essence of the report must diverge from the inefficacious generalized 'numbers' modality discussed above which is all too common in current transparency reporting.

This Rule thus aims to stimulate Organisations to be more transparent with their stakeholders by proactively publishing UM-DPCSR Transparency Reports that do not merely demonstrate that the Organisation has received a request for access to data or removal. Instead, with this Rule, implementing Organisations will also provide relevant information on how and why certain decisions are made within the Organisation concerning data processing activities, data security and the effectiveness of the means used to provide the relevant privacy information to individuals. Such a formulation will have a greater impact and help elevate trust levels of the public.[106]

Budish, R. (2013). What Transparency Reports Don't Tell Us. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2013/12/what-transparency-reports-dont-tell-us/282529/

[97] Singh, S., & Bankston, K. (2018). *The Transparency Reporting Toolkit: Content Takedown Reporting*. New America. Retrieved from https://www.newamerica.org/oti/reports/transparency-reporting-toolkit-content-takedown-reporting/introduction-and-executive-summary

[98] Ibid.

[99] See footnote 96.

[100] AccessNow. (2021). *Transparency Reporting Index*. Retrieved from https://www.accessnow.org/transparency-reporting-index/

[101] Google Transparency Report. (2022). Retrieved 8 March 2022, from https://transparencyreport.google.com/about?hl=en

[102] Windwehr, S., & York, J. (2020). Thank You for Your Transparency Report, Here's Everything That's Missing. Retrieved 8 March 2022, from https://www.eff.org/deeplinks/2020/10/thank-you-your-transparency-report-heres-everything-thats-missing

[103] AccessNow. (2021). *Transparency Reporting Index*. Retrieved from https://www.accessnow.org/transparency-reporting-index/

[104] Ibid.

[105] Windwehr, S., & York, J. (2020). Thank You for Your Transparency Report, Here's Everything That's Missing. Retrieved 8 March 2022, from https://www.eff.org/deeplinks/2020/10/thank-you-your-transparency-report-heres-everything-thats-missing

[106] Ibid.

Organisations will implement this Rule by following best practices for transparency reporting put forward by Dr. José Tomás Llanos of the University College London and the OECD Secretariat[107] and the Transparency Reporting Toolkit. The Transparency Reporting Toolkit, a project which is the fruit of collaboration between Harvard's Berkman Klein Center for Internet & Society and the Open Technology Institute of New America,[108] provides both a template and best practices for organisations to use to report requests for data received by governments.[109] The Organisation shall furthermore complement the use of the aforementioned sources by including additional information on data security and the effectiveness of the means used to provide the relevant privacy information to individuals.

Principle 3. Balance profits with the actual benefits for citizens

Principle 3. Balance profits with the actual benefits for citizens

Rule 1: Carry out a Profitable and Beneficial Test (P&B Test). The Organisation shall carry out a P&B Test to evaluate how data processing activities benefit both the Organisation and society.

Rule 1, Principle 3 calls for the Organisation to carry out a Profitable and Beneficial Test (P&B Test) for its data processing activities. The P&B Test is a model which can be used by Organisations to identify the benefits of a specific data processing activity for the organisation and those of society/individuals, grounding such balancing in law and ethics. The P&B Test goes beyond the concept of a risk-based approach (Article 24 GDPR), Data Protection by Design/by Default (Article 25 GDPR), Data Protection Impact Assessment (Article 35 GDPR), legitimate interest (Article 6(1)(f) GDPR) assessment or compatibility test (Article 6(4) GDPR), the data subject's reasonable expectations of processing, and necessitates the identification of benefits for users and/or the greater community.

The P&B Test assists the data controller in understanding if **a data processing activity is beneficial for individuals and/or for the greater society** and in identifying in which terms the same processing is **also profitable for the Organisation**. In principle, it is recommendable to perform the Test on all processing activities logged in the Article 30 GDPR Record of Processing Activities. However, we consider it necessary for the processing activities that also require a Data Protection Impact Assessment pursuant to Article 35 GDPR. The ratio is that the benefit for the individuals and/or for the society at large shall specifically be identify when the processing activity may likely result in a high risk to the rights and freedoms of individuals. This approach is also coherent with Principle 1, Rules 4 and 5. The P&B test should be documented in

[107] Llanos, J. (2021). *Transparency reporting Considerations for the review of the privacy guidelines*. Paris: OECD Publishing. Retrieved from https://www.oecd.org/science/transparency-reporting-e90c11b6-en.htm

[108] Woolery, L., Budish, R., & Bankston, K. (2016). *Transparency Reporting Toolkit: Reporting. Guide and Template for Reporting U.S. Government Requests for User Information*. New America and the Berkman Klein Center for Internet & Society. Retrieved from https://dash.harvard.edu/bitstream/handle/1/29914191/Transparency_Reporting_Guide_and_Template-Final.pdf?sequence=1&isAllowed=y

[109] Ibid. see p. 2

writing, according to the principle of accountability, detailing the criterion in the test and the Organisation's reasoning.

The P&B Test helps to ensure that data processing activities provide a benefit to individuals and/or society in addition to generating profits for the Organisation. By carrying out a P&B Test for data processing activities and making the results available (see Principle 2, Rule 3) - i.e., how individuals will benefit from the envisioned processing activity - compliance with the principles of transparency and fairness is enhanced. Furthermore, the data controller which carries out a P&B Test for certain data processing activities goes beyond the basic requirements of lawfulness and accountability, transforming the activity into a socially responsible user-centric one in which the individual is adequately taken into consideration as a single person and/or as a member of the society, promoting the solidary behaviour of Organisations (see also Principle 5, Rule 5).

The P&B Test establishes that the profits for the Organisation derived from data processing subject to the P&B Test come with actual benefits for individuals. These benefits can be of a contractual, legal, financial, social or cultural nature. **The Test also draws a red line: only where a specific processing activity has at least one benefit for the individual or for the community/society should the processing be pursued in order for the Organisation to act in adherence to the DPCSR Framework.**

Principle 3. Balance profits with the actual benefits for citizens

Rule 2: Engage with stakeholders to understand their values and beliefs when selecting suppliers. The Organisation shall survey stakeholders to find consensus in common goals and greater objectives.

The second rule of Principle 3 calls on Organisations to engage with stakeholders to understand their values and beliefs when selecting suppliers. It is worthwhile for Organisations to invest resources, as part of regular managerial activities, to understand and address the interests of stakeholders.[110] The contemporary conceptualization of stakeholder governance and accountability in fact requires Organisations to take such interests into account and to balance the rights and interests of the stakeholders with those of the organisation.[111] In order to do so, however, light must be shed on the perspective of the relevant individuals and dialogue must take place.

By successfully engaging with stakeholders and reducing information asymmetry, the quality of the CSR initiative can be better transmitted to individuals,[112] pursuant to this Rule. The Organisation will improve the effectiveness of its DPCSR program and individuals will benefit from having their voices, interests, and

[110] O'Riordan, L., & Fairbrass, J. (2013). Managing CSR Stakeholder Engagement: A New Conceptual Framework. *Journal Of Business Ethics*, *125*(1), 121-145. doi: 10.1007/s10551-013-1913-x

[111] Ibid. p. 123

[112] See p. 2 Moratis, L. (2018). Signalling Responsibility? Applying Signalling Theory to the ISO 26000 Standard for Social Responsibility. *Sustainability*, *10*(11), 4172. doi: 10.3390/su10114172

rights heard by the Organisation. UM-DPCSR is ultimately about going beyond the legally mandated interaction with stakeholders and, includes a social dimension by definition.

When it comes to making purchases, research suggests that providing potential customers with accessible and trustworthy information (also known as 'decision simplicity') improves stickiness.[113] The willingness of a company to hear the voice of the consumers and engage in open dialogue in this sense aims to increase retention thanks to transparent dialogue. The purpose of this exercise is to increase user trust and therefore contribute to the long-term success of the Organisation. Under this Rule, the Organisation is obliged to survey stakeholders in order to find consensus in common goals and greater objectives concerning privacy, data protection, and data security.

Different stakeholders will have different expectations for how the Organisation should behave when it comes to their privacy, data protection, and security. Nonetheless, good privacy and cybersecurity compliance has already been welcomed and proven beneficial for both organisations and individuals.[114] Engaging with stakeholders to understand how they view certain data processing activities in the context of purchases or the use of services offered by the Organisation will allow for important insights to be drawn and recommendations can be made concerning data processing activities that are in line with the expectations of consumers and society.

In order to execute this Rule, the Organisation shall generally follow four material steps:

1. **identify stakeholders** (country and population specific);
2. **start dialogue with stakeholders**;
3. maintain the dialogue through dedicated measures;
4. **develop CSR communication campaigns** around specific privacy, data protection and security issues that have been assessed by the Organisation based on the dialogue.

(Also see Principle 3, Rule 5 and Principle 5, Rule 3).

Principle 3. Balance profits with the actual benefits for citizens

Rule 3: Establish trusted data processing activities (for example, for use in AI and big data analytics) that actively oppose bias and discrimination. The Organisation shall actively seek not to cause harm.

Rule 3, Principle 3 focuses on **establishing trusted data processing activities that actively oppose bias and discrimination**. This necessitates having in place checks and balances to prevent bias and discrimination

[113] Stickiness is intended as the likelihood that an individual consumer may make a purchase, recommend a product, or make multiple purchases. For more on stickiness and the study referred to see Spenner, P., & Freeman, K. (2012). To Keep Your Customers, Keep It Simple. *Harvard Business Review*, (May). Retrieved from https://hbr.org/2012/05/to-keep-your-customers-keep-it-simple

[114] Cisco. (2020). *Cisco Data Privacy Benchmark Study 2020 CISCO, From Privacy to Profit: Achieving Positive Returns on Privacy Investments*. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf?CCID=cc000160&DTID=esootr000515&OID=rptsc020143

on all levels of data processing activities. It is closely related to the concept of Fairness by design (see Principle 1, Rule 3). It can also implicate data sharing, which is further explored in Principle 4 on publishing relevant findings based on statistical/anonymized data to improve society. Data quality and accuracy[115] play vital roles in this Rule as well as the fact that datasets used for training should be as representative and complete[116] as possible in order to avoid bias[117] and discrimination.[118] These requirements should be balanced with the principles of data minimization, proportionality, and purpose limitation enshrined in the GDPR.

[115] Article 5(1)(d) GDPR calls for personal data to be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')."

[116] Lee, N., Resnick, P., & Barton, G. (2019). *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*. Brookings Institution. Retrieved from https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

[117] The High-Level Expert Group on Artificial Intelligence (AI HLEG) in its Trustworthy AI Impact Assessment tool defines algorithmic bias as describing the "systematic and repeatable errors in a computer system that create unfair outcomes, such as favouring one arbitrary group of users over others. Bias can emerge due to many factors, including but not limited to the design of the algorithm or the unintended or unanticipated use or decisions relating to the way data is coded, collected, selected or used to train the algorithm. Bias can enter into algorithmic systems as a result of pre-existing cultural, social, or institutional expectations; because of technical limitations of their design; or by being used in unanticipated contexts or by audiences who are not considered in the software's initial design. AI bias is found across platforms, including but not limited to search engine results and social media platforms, and can have impacts ranging from inadvertent privacy violations to reinforcing social biases of race, gender, sexuality, and ethnicity." See p. 23 High-Level Expert Group on AI (AI HLEG). (2020). *The Assessment List for Trustworthy Artificial Intelligence (ALTAI)*. Brussels: European Commission. Retrieved from https://futurium.ec.europa.eu/en/european-ai-alliance/document/ai-hleg-assessment-list-trustworthy-artificial-intelligence-altai?language=fr

[118] Recital 71 GDPR states that, "The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her...In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.
In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions."
Recital 75 GDPR states that, "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage".

Trust is defined by the OECD as "a person's belief that another person or institution will act consistently with their expectations of positive behaviour"[119] and represents a fundamental prerequisite for economic growth.[120] Trust is "the invisible foundation of a fair and open market",[121] and for businesses is an "imperative to achieving long-term value and profitability".[122] New and emerging technologies such as AI and machine learning, however, while possessing significant potential for revolutionizing systems, have a fundamental trust problem which must be overcome in order for society to truly benefit from such technological advancements. Problems related to trust in AI, and more generally new technologies, stem from issues that center around questions of **transparency**, **explainability**, and **accountability**, which, if successfully mitigated, may help to improve trust and therefore uptake of such technologies for the benefit of all.

It should furthermore be noted that legally compliant re-use of data and the combination of data can provide new insights that lead to both new services and improved (more informed) decision-making, which can also increase the value of data. To ensure that a technology provides the greatest benefit to society, it is necessary that the relative insights provided, for example, by big data analysis, are as accurate and as applicable to the general public as possible (avoiding non-representative data, etc.).

The Organisation shall apply the requirements of this control by actively auditing against bias and discrimination within relevant data processing activities, especially those involving AI. The Organisation should also have controls in place to prevent bias and discrimination in the offering of products and services and, where not possible, to mitigate such biases to the extent possible.[123] In addition to carrying out tests for bias and following the relevant controls which are to be implemented by the Organisation, ensuring diversity among the stakeholders involved in the activities undertaken in relation to Principle 3, Rule 2 will contribute to compliance with this Rule.

By implementing this Rule, the Organisation will be able to demonstrate its commitment to transparency, explainability, and accountability, therefore fostering trustworthy data processing activities that actively seek to avoid bias and discrimination against individuals. Such a manifestation of will to 'do good' and avoid negative outcomes will encourage trust and following economic and sociological theory, should contribute positively to the bottom line of the Organisation. Individuals, on the other hand, will benefit

[119] See p. 5 OECD (2019). *OECD Business and Finance Outlook 2019: Strengthening Trust in Business*, OECD Publishing, Paris. https://doi.org/10.1787/af784794-en.

[120] OECD Trust in Business Forum - OECD. (2019). Retrieved 8 March 2022, from https://www.oecd.org/corporate/oecd-trust-in-business-forum.htm

[121] See p. 4 OECD (2019). *OECD Business and Finance Outlook 2019: Strengthening Trust in Business*, OECD Publishing, Paris. https://doi.org/10.1787/af784794-en.

[122] Ibid.

[123] For insights on bias and discrimination, see, for example, Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A Survey on Bias and Fairness in Machine Learning. *ACM Computing Surveys*, *54*(6), 1-35. doi: 10.1145/3457607; Bellamy, R., Dey, K., Hind, M., Hoffman, S.C., Houde, S., Kannan, K., Lohia, P., Martino, J., Mehta, S., Mojsilovic, A. et al. (2018). AI fairness 360: An extensible toolkit for detecting, understanding, and mitigating unwanted algorithmic bias. arXiv preprint arXiv:1810.01943.; Berk, R., Heidari, H., Jabbari, S., Joseph, M., Kearns, M., Morgenstern, J., Neel, S., Roth, A. (2017). A Convex Framework for Fair Regression. (2017). arXiv:cs.LG/1706.02409; d'Alessandro, B., O'Neil, C., & LaGatta, T. (2017). Conscientious Classification: A Data Scientist's Guide to Discrimination-Aware Classification. *Big Data*, *5*(2), 120-134. doi: 10.1089/big.2016.0048; Baeza-Yates, R. (2018). Bias on the web. *Communications Of The ACM*, *61*(6), 54-61. doi: 10.1145/3209581; Friedman, B., & Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems*, *14*(3), 330-347. doi: 10.1145/230538.230561; González-Bailón, S., Wang, N., Rivero, A., Borge-Holthoefer, J., & Moreno, Y. (2014). Assessing the bias in samples of large online networks. *Social Networks*, *38*, 16-27. doi: 10.1016/j.socnet.2014.01.004

from the Organisation's attention towards potential negative outcomes of processing activities, lessening the unintended harm that can result from the use of new technologies and filling the gap that is left by pure data protection legal compliance which does not directly control for these factors.[124]

Principle 3. Balance profits with the actual benefits for citizens

Rule 4: Organise data processing activities in consideration of the environment and climate issues. The Organisations shall minimize data processing activities to actively contribute to the reduction of energy consumption and carbon emissions along the value chain.

The fourth Rule of Principle 3 calls for the Organisation to consider its environmental impact when taking decisions on data processing activities, e.g., to minimize data processing activities with the aim of reducing energy consumption.[125] Over the last 20 years, access to cheap computational capacity has increasingly led to the harvesting of ever-more significant quantities of personal data. This has brought about a situation in which organisations have largely been able to avoid significant costs for data storage and processing activities. For this very reason, and all too often, data sets are offhandedly replicated, databases are left unmanaged, and the same data is re-collected multiple times. Such practices create potential data protection compliance problems (for example, with respect to the principles of data minimization, accuracy, and storage limitation) and cybersecurity risks (by increasing the attack perimeter and decreasing security in unmanaged applications).

It must not be forgotten that such practices also contribute to the climate crisis. Socially responsible behaviour within the CSR and ESG domains furthermore entails that companies should reduce energy consumption, and therefore CO_2 emissions along the value chain.

With this in mind, and according to this Rule, Organisations should:

1. Pay careful attention and only collect and, more generally, process, the minimum amount of data required to pursue business goals – **data minimization**;
2. Make sure that data are kept up to date and old/inaccurate data are properly deleted – **data quality / accuracy**;

[124] Also confirmed by the Council of Europe, "it is unclear whether a normative framework regarding the use of algorithms or an effective regulation of automated data processing techniques is even feasible as many technologies based on algorithms are still in their infancy and a greater understanding of their societal implications is needed." See p. 4 Council of Europe. (2018). *Study on the Human Rights Dimensions of Automated Data Processing Techniques (In Particular Algorithms and Possible Regulatory Implications) DGI(2017)12.* Strasbourg: Council of Europe. Retrieved from https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

[125] With respect to this Rule, see Balboni, P. (2021). How data minimisation, data quality, and storage limitation can help in the fight against climate change [Blog]. Retrieved from https://www.paolobalboni.eu/index.php/2021/08/13/how-data-minimization-data-quality-and-storage-limitation-can-help-in-the-fight-against-climate-change/

3. Enforce appropriate and effective data retention rules across all systems, so to regularly delete data that are not necessary anymore – **storage limitation**;

4. Improve their data-driven businesses (by creating lean, performing, and high-quality datasets).

An approach that takes the above into consideration will not only comply with the relevant data protection principles, but also help to potentially mitigate cybersecurity risks and **actively contribute to reducing energy consumption and carbon emissions along the value chain, taking an active and socially responsible role in the fight against major concerns of our era: climate change and global warming**.

Inspiration for the controls under this Rule can be found - *mutatis mutandis* - in the EDPS proportionality guidelines[126] and the concept of only carrying out processing activities that 'genuinely meet' business objectives.[127]

Principle 3. Balance profits with the actual benefits for citizens

Rule 5: Carry out a Materiality Assessment. The Organisation shall carry out materiality assessments at regular intervals to ensure alignment with ever-changing social, economic, and environmental needs.

The fifth and final rule of Principle 3 calls upon the Organisation to carry out a Materiality Assessment.[128] By carrying out Materiality Assessments, the Organisation can understand the values and beliefs of individual stakeholders when it comes to data processing activities (also see Principle 3, Rules 1 and 2). With respect to Principle 3, Rule 2, this Rule is broader in scope and entails making such information available to the public. The materiality "principle represents the driver through which companies can identify and select issues to be included and treated in integrated and sustainability reporting, as well as in other voluntary reporting".[129] Compliance with this UM-DPCSR Rule will therefore allow the Organisation to more effectively drive its operations in a way that is compatible with the needs and values of the relevant individuals and at the same time, permit the Organisation to better direct its communication and UM-DPCSR education-related initiatives. Essentially, this Rule aims to contextualize the CSR activities of the Organisation within the wider CSR and ESG domains.

[126] European Data Protection Supervisor. (2019). *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*. EDPS. Retrieved from https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf

[127] Patterson, D., Gonzalez, J., Le, Q., Liang, C., Munguia, L. M., Rothchild, D., So, D., Texier, M. & Dean, J. (2021). Carbon emissions and large neural network training. *arXiv preprint arXiv:2104.10350*.

[128] See Calabrese, A., Costa, R., Levialdi, N., & Menichini, T. (2016). A fuzzy analytic hierarchy process method to support materiality assessment in sustainability reporting. *Journal of Cleaner Production*, *121*, 248-264. https://doi.org/10.1016/j.jclepro.2015.12.005

[129]See p. 470 Torelli, R., Balluchi, F., & Furlotti, K. (2020). The materiality assessment and stakeholder engagement: A content analysis of sustainability reports. *Corporate Social Responsibility and Environmental Management*, *27*(2), 470-484. doi: 10.1002/csr.1813

The International Organisation for Standardization's Global Reporting Initiative (GRI), perhaps the most well-known authority on sustainability reporting, stresses the relevance of the materiality principle in the G4 Guidelines to the GRI Standards.[130] Specifically, the G4 Guidelines specify that reports should cover aspects which either "Reflect the organization's significant economic, environmental and social impacts; or substantively influence the assessments and decisions of stakeholders", noting that "[r]elevant topics are those that may reasonably be considered important for reflecting the Organisation's economic, environmental and social impacts, or influencing the decisions of stakeholders."[131] To this end, and as stressed by the GRI Standards, due attention must be taken to identify themes which transparently disclose the actions and processes of the Organisation which impact sustainability, with a view to adequately consider consequences on both society and the Organisation.

As suggested in the preceding paragraphs, Materiality Assessments play a vital role in helping Organisations both in the development and in the execution of the voluntary reporting which is inherent to ESG and CSR programs. In order to implement this Rule, the Organisation must periodically carry out Materiality Assessments, also building on the initiatives of the Organisation under Principle 3, Rule 2 (Engage with stakeholders to understand their values and beliefs when selecting suppliers). To this end, the Organisation should adopt an appropriate methodology for such assessments and commit to their regular publication. Essentially, Materiality Assessments are used to guide the organisation in related external-facing communications which will improve their effectiveness.[132] Such assessments can also contribute to enhancing organisational transparency and allow the Organisation to be more accountable.[133]

Principle 4. Publish relevant findings based on statistical/anonymized data to improve society

Principle 4. Publish relevant findings based on statistical/anonymized data to improve society

Rule 1: Business to Consumer Data Sharing. The Organisation shall make findings derived from data known to consumers by way of understandable and useful Digital Society Insights Reports. **"B2C Data Sharing"**

[130] International Organization for Standardization and Stichting Global Reporting Initiative. (2014). *GRI G4 Guidelines and ISO 26000:2010 How to use the GRI G4 Guidelines and ISO 26000 in conjunction*. International Organization for Standardization and Stichting Global Reporting Initiative. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso-gri-26000_2014-01-28.pdf

[131] GRI - Materiality and topic boundary. Retrieved 8 March 2022, from https://www.globalreporting.org/how-to-use-the-gri-standards/questions-and-answers/pre-2021-gri-standards-system-faq/materiality-and-topic-boundary/

[132] See p. 470 Torelli, R., Balluchi, F., & Furlotti, K. (2020). The materiality assessment and stakeholder engagement: A content analysis of sustainability reports. *Corporate Social Responsibility and Environmental Management*, *27*(2), 470-484. doi: 10.1002/csr.1813

[133] See p. 248 Calabrese, A., Costa, R., Levialdi, N., & Menichini, T. (2016). A fuzzy analytic hierarchy process method to support materiality assessment in sustainability reporting. *Journal Of Cleaner Production*, *121*, 248-264. doi: 10.1016/j.jclepro.2015.12.005

The first rule of Principle 4 is *B2C Data Sharing*. The Organisation shall make findings derived from data known to individuals by way of understandable and useful *Digital Society Insights Reports*. Related to both the ongoing theme of transparency and 'doing good', this Rule is also closely linked to Principle 5, Rule 3, which requires Organisations to develop and execute a yearly data awareness program for citizens with clear objectives. With this Rule, the information developed in the Digital Society Insights Reports form part of the content to be shared in the related awareness programs or information campaigns.

This Rule can also be seen as a modality of stakeholder management where stakeholders of the organisation are managed "though information provision, dialogue and other forms of one- and two-way communication."[134] Under this rule, Organisations have the responsibility to make sure that their **anonymized statistical findings will be made available AND that they are *understandable* in order to render them *useful* for stakeholders** as opposed to simply publishing numbers or data in a more abstract sense.

The European Strategy for Data[135] underlines the potential for citizens to be both empowered and to make better decisions as a result of insights enabled by data. By sharing insights from non-personal and aggregated data, in fact, society will be able to "get the most out of innovation and competition",[136] reflecting the "best of Europe - open, fair, diverse, democratic, and confident."[137] The availability of data can enable innovation and competition to ensure that all members of society can benefit from a '**digital dividend**',[138] understood as additional benefits brought by the use of technologies.[139] By having access to the results of data-driven analyses, individuals are provided with added value as a result of having provided their data.

As Organisations make financial reports available on a quarterly basis, a similar approach is adopted in this Rule through the use of **Digital Insights Reports**. Digital Insights Reports are to be populated by a data-driven analysis carried out by the Organisation and will reveal patterns that can be useful to society and specifically, to the stakeholders of the Organisation adhering to the UM-DPCSR Framework. The information elaborated for the purpose of the Reports can also be communicated more broadly by the Organisation, e.g., sharing results in the press or with customers, giving them an added benefit.

To implement this Rule, the Organisation should regularly publish, at least once per year, insights elaborated as a result of its data processing activities (i.e., in the UM-DPCSR Digital Insights Report). The Digital Insights Reports make public results that are understandable and useful for consumers. For example, the individuals involved under Principle 3, Rule 2, may assist the Organisation in identifying relevant topics of interest that would be of genuine value for the consumer-stakeholder. In this way, the Organisation provides value that was not necessarily expected on the part of the individual, representing a competitive advantage for the Organisations that goes one step further to take this initiative.

---

[134] See p. 1232 Crane, A., & Glozer, S. (2016). Researching Corporate Social Responsibility Communication: Themes, Opportunities and Challenges. *Journal Of Management Studies*, *53*(7), 1223-1252. doi: 10.1111/joms.12196

[135] European Commission. (2020, February 19). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM(2020) 66 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

[136] Ibid.

[137] Ibid.

[138] Ibid.

[139] World Bank. (2016). World Development Report 2016: Digital Dividends. Washington, DC: World Bank. doi:10.1596/978-1-4648-0671-1.

Principle 4. Publish relevant findings based on statistical/anonymized data to improve society

Rule 2: Business to Business Data Sharing. The Organisation shall engage in or establish secure and transparent data collaboratives with relevant peer-stakeholders to improve the analytical potential of the data in its possession. **"B2B Data Sharing"**

The second rule of Principle 4 is *B2B Data Sharing.* Under this Rule, the Organisation shall engage in or establish secure and transparent data collaboratives with relevant peer-stakeholders in order to improve the analytical potential of the data in its possession, in line with applicable current and forthcoming legislation.[140] This Rule concerns sharing data, where possible, with fellow organisations in order to maximize the potential of the data.

It has been shown that data assets are "non-rivalrous and can be shared without diminishment. Data can even become more valuable through sharing and collaboration."[141] This assumption is supported by the European Commission, which in putting forward the proposed Data Act in February 2022 claimed that industrial data sharing while respecting EU rules "will form the cornerstone of a strong, innovative and sovereign European digital economy."[142] The aim of the Data Act is, in fact, to take advantage of the many opportunities that industrial data can offer in a context in which a whopping 80 percent of data is not used, something which, by 2028, could lead to an increase in additional GDP of €270 billion if tapped into.[143]

B2B data sharing platforms, specifically used in strategic sectors such as energy, transportation, and healthcare, have the potential to "improve healthcare outcomes, research and fuel innovation while respecting privacy and citizen trust".[144] However, in order for B2B data sharing to be successful, data must be conceptualized as a "pre-commercial, precompetitive common asset, whose value is greater for all when scaled up and widely available" in addition to providing data-sharing infrastructure[145] which may be foreseen at the European level. Data on its own does not have value, on the contrary, as a raw resource does, data becomes valuable when actors in the data economy are able to "leverage their position in data-

[140] E.g., the proposed Data Act and the Data Governance Act.

[141] Jordana J. George, Jie (Kevin) Yan & Dorothy E. Leidner (2020) Data Philanthropy: Corporate Responsibility George, J., Yan, J., & Leidner, D. (2020). Data Philanthropy: Corporate Responsibility with Strategic Value?. *Information Systems Management*, *37*(3), 186-197. doi: 10.1080/10580530.2020.1696587;
Martens, B., de Streel, A., Graef, I., Tombal, T., & Duch-Brown, N. (2020). *Business-to-business data sharing: An economic and legal analysis*. (JRC Digital Economy Working Paper Series; Vol. 2020, No. 05). European Commission. https://ec.europa.eu/jrc/sites/jrcsh/files/jrc121336.pdf

[142] European Commission. (2022). *Data Act: Commission proposes measures for a fair and innovative data economy*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

[143] Ibid.

[144] See p. 6 European Commission, Directorate-General for Communications Networks, Content and Technology, (2020). *Shaping the digital transformation in Europe*, Publications Office. https://data.europa.eu/doi/10.2759/294260

[145] Ibid. p. 30

driven services markets."[146] The more data that actors have access to, the more value they can potentially create for their Organisation and for society at large.

Organisations shall implement this Rule by making use of a sustainable data sharing model. The appropriate model to be followed will vary according to the type of Organisation and its interests, e.g., data may be open, in the form of bilateral contracts, via closed platforms, etc.[147] Under this Rule, the best practices and guidance of the Support Centre for Data Sharing shall be considered.[148] Organisations will promote Data Sharing for the common good by sharing data with other organisations in order to allow for insights that are more relevant and impactful for society.[149] Data sharing will take place in a manner that respects applicable ethics, privacy, data protection and data security principles. The Organisation's policy and selected model for data sharing shall be documented in writing.

Organisations that are able to successfully use and share data through open data, sharing of data in exchange for renumeration on a data marketplace, or through closed platforms[150] will benefit from new insights and potentially products and services that would otherwise have been too costly or resource-intensive to develop.[151] At the same time, society will benefit from new or improved products and services that have been facilitated by way of their provision of data.

Principle 4. Publish relevant findings based on statistical/anonymized data to improve society

Rule 3: Business to Government Data Sharing. The Organisation shall actively seek to provide the public sector with relevant data-based insights. **"B2G Data Sharing"**

The third Rule of Principle 4 requires Organisations to engage in business to government (B2G) data sharing. More specifically, the Organisation shall actively seek to provide the public sector with relevant data-based insights. B2G data sharing has significant potential to resolve some of the serious challenges we are facing in modern society including climate change, education, poverty, and urban planning, or as the COVID-19 pandemic has shown, health crises. The provision of private sector data to governments can

[146] Martens, B., de Streel, A., Graef, I., Tombal, T., & Duch-Brown, N. (2020). *Business-to-business data sharing: An economic and legal analysis*. (JRC Digital Economy Working Paper Series; Vol. 2020, No. 05). European Commission. https://ec.europa.eu/jrc/sites/jrcsh/files/jrc121336.pdf

[147] See p. 5 European Commission. (2018). Guidance on sharing private sector data in the European data economy, Accompanying the document Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions "Towards a common European data space", {COM(2018) 232 final}. Retrieved at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0125&rid=2

[148] Support Centre for Data Sharing. Retrieved 8 March 2022, from https://eudatasharing.eu/

[149] See p. 9, European Commission. (2018). Guidance on sharing private sector data in the European data economy, Accompanying the document Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions "Towards a common European data space", {COM(2018) 232 final}. Retrieved at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0125&rid=2

[150] Ibid. p. 5

[151] World Economic Forum. (2018). Insight Report, Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society. Retrieved from http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf

permit evidence-based policymaking which will lead to improved cost efficiency and ultimately, a fairer and more inclusive world. [152]

Business-to-Government data sharing entails that the Organisation makes insights or anonymized, aggregate data available to the public sector, whether it be on an EU, national, regional, or local level, in the interest of the public.[153] This Rule aims to promote the sharing of data by the private sector with the public sector entity of the Organisation's choosing in order to promote the common good and provide insights which otherwise would be inaccessible to the public administration. This is of particular relevance as many challenges that we currently face as a society are often too complex for the public sector/public policy to adequately address on its own.

Data from the private sector, for example, can help inform the public sector by identifying real-time patterns which can foster better decision-making and resolve public policy issues, "thus enabling more targeted interventions and improving public service delivery, amongst other possibilities."[154] Organisations should therefore share aggregated and anonymous data providing insights resulting from data analysis, with governments to help inform on issues related to, e.g., public health and safety, security online and offline, etc. This provision of information, in-turn, is both beneficial to the reputation of the Organisation and to society which in the long-term benefits from data-driven empirically based policy. Furthermore, the reputation of the Organisation may benefit from having behaved in this altruistic way.[155]

The Organisation shall implement this Rule first by identifying data that may be valuable for the public sector, and secondly, by establishing a B2G data sharing policy within the Organisation which will ensure the transmission of only high-quality and useful data. The Organisation's policy can be based, e.g., on the model contract terms and data sharing best practices made available by the European Commission[156] and/or those of the Support Centre for Data Sharing.[157] Thirdly, the Organisation is called upon to engage in B2G data sharing activities in the modality deemed most appropriate in accordance with the

[152] European Commission. (2021). Business-to-government data sharing: Questions and answers | Shaping Europe's digital future. Retrieved 8 March 2022, from https://digital-strategy.ec.europa.eu/en/faqs/business-government-data-sharing-questions-and-answers; also see Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[153] Ibid.

[154] High-Level Expert Group on Business-to-Government Data Sharing. (2020). *Towards a European strategy on business-to-government data sharing for the public interest*. European Union. Retrieved from https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/B2GDataSharingExpertGroupReport-1.pdf

[155] European Commission. (2021). Business-to-government data sharing: Questions and answers | Shaping Europe's digital future. Retrieved 8 March 2022, from https://digital-strategy.ec.europa.eu/en/faqs/business-government-data-sharing-questions-and-answers

[156] See European Commission. (2018). Guidance on sharing private sector data in the European data economy, Accompanying the document Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions "Towards a common European data space", {COM(2018) 232 final}. Retrieved at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0125&rid=2; also see p. 42 European Commission. (2018). Annex to the Commission implementing decision on the adoption of the work programme for 2018 and on the financing of Connecting Europe Facility (CEF) - Telecommunications Sector. Retrieved from https://digital-strategy.ec.europa.eu/en/news/connecting-europe-facility-cef-telecom-work-programme-2018-adopted

[157] See the Support Centre for Data Sharing's website for more information: https://eudatasharing.eu/

Organisation's policy, which will be documented in writing.[158] With this Rule, the Organisation will comply with specific controls inspired, among others, by the "Legal and practical considerations in B2G data sharing collaboration" section of the Guidance on sharing private sector data in the European data economy Commission Staff Working Document[159] and, when applicable, the legislative provisions.

Principle 4. Publish relevant findings based on statistical/anonymized data to improve society

Rule 4: Business to Research Data Sharing. The Organisation shall engage in business to scientific research data sharing to provide data to sustainable innovation initiatives, following the FAIR data principles. **"B2R Data Sharing"**

This fourth rule of Principle 4 of the UM-DPCSR Framework calls for the adhering Organisation to specifically contribute to scientific advancements and new innovations made possible thanks to data by following the FAIR data principles. FAIR is an acronym that stands for "Findability, Accessibility, Interoperability, and Reuse of digital assets".[160] This Rule is furthermore in line with initiatives of the European Commission aimed at creating a single data market.[161]

It should be noted that the FAIR data principles do not only apply to data, but also to "other digital objects including outputs of research."[162] **Data is truly valorised when it is made accessible for further research purposes which are in line with the purpose limitation principle established under the GDPR**. This means, e.g., that data shared in the context of B2R data sharing should be anonymized/aggregated and even if the further processing is established as compatible, it is still recommendable to share them in a pseudonymised form.[163]

[158] Note that, as suggested by the Irish Data Protection Commissioner, the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, and storage limitation. Irish Data Protection Commissioner. *Data Sharing in the Public Sector*. Retrieved from https://www.dataprotection.ie/en/dpc-guidance/data-sharing-in-the-public-sector

[159] European Commission. (2021). Business-to-government data sharing: Questions and answers | Shaping Europe's digital future. Retrieved 8 March 2022, from https://digital-strategy.ec.europa.eu/en/faqs/business-government-data-sharing-questions-and-answers; European Commission. (2018). Guidance on sharing private sector data in the European data economy, Accompanying the document Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions "Towards a common European data space", {COM(2018) 232 final}. Retrieved at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0125&rid=2

[160] FAIR Principles - GO FAIR. Retrieved 8 March 2022, from https://www.go-fair.org/fair-principles/

[161] European Commission. Data sharing in the EU – common European data spaces (new rules). Retrieved from https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Data-sharing-in-the-EU-common-European-data-spaces-new-rules-_en

[162] See p. 76 European Commission Expert Group on FAIR Data. (2018). *Turning FAIR into reality: Final Report and Action Plan from the European Commission Expert Group on FAIR Data*. European Commission. Retrieved from https://ec.europa.eu/info/sites/default/files/turning_fair_into_reality_0.pdf

[163] European Union Agency for Cybersecurity. (2021). *Data Pseudonymisation: Advanced Techniques and Use Cases*. ENISA. Retrieved from https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases

More specifically, where applicable, ensuring that data is findable, accessible, interoperable and reusable can generally be considered as a good data management practice.[164] Researchers have suggested, however, that Organisations largely keep data inside their own silos, preventing it from realizing its potential impact, also due to a lack of findability[165] By applying the FAIR data principles to the research data processed by the Organisation, there will be a greater potential for innovation and the development of new products and services which will benefit both the Organisation and society as a whole.[166]

While it is evident that compliance with this Rule will help the Organisation to contribute to future discoveries that may benefit society, the relevance of this Rule for its bottom line may not be so clear. An example is useful in this sense. The Cambridge Crystallographic Data Centre (CCDC), points to the pharmaceutical industry where

> one of the most valuable assets a pharma company creates is its data. Getting the most out of that investment requires attention to the FAIR Data Principles, by whatever name you might give such an effort. One clear example of this occurs every time one pharma company acquires another. If the corporate compound databases use different identifiers and representations, it might take the new company months to years to figure out exactly what their IP assets really are![167]

The implementing Organisation shall follow the FAIR data principles as illustrated in the UM-DPCSR controls to the extent applicable to the Organisation with the virtuous aim of contributing to the maximization of research initiatives. The Organisation's activities with respect to compliance with this Rule and the application of the FAIR data principles shall be documented in writing.

Principle 4. Publish relevant findings based on statistical/anonymized data to improve society

Rule 5: Business to Humanitarian Action Data Sharing. Engage in business to humanitarian aid data sharing to support humanitarian actions. **"B2H Data Sharing"**

The fifth rule of Principle 4 invites participating Organisations to engage in what we have denominated as 'B2H' data sharing, or data sharing with the objective of contributing to humanitarian aid and corresponding actions. As natural disasters, pandemics, and armed conflict plague populations throughout

[164] Wilkinson, M., Dumontier, M., Aalbersberg, I., Appleton, G., Axton, M., & Baak, A. et al. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, *3*(1). doi: 10.1038/sdata.2016.18

[165] van Vlijmen, H., Mons, A., Waalkens, A., Franke, W., Baak, A., & Ruiter, G. et al. (2020). The Need of Industry to Go FAIR. *Data Intelligence*, *2*(1-2), 276-284. doi: 10.1162/dint_a_00050

[166] See p. 277, van Vlijmen, H., Mons, A., Waalkens, A., Franke, W., Baak, A., & Ruiter, G. et al. (2020). The Need of Industry to Go FAIR. *Data Intelligence*, *2*(1-2), 276-284. doi: 10.1162/dint_a_00050

[167] Moreno, A. (2021). Why should industry care about the FAIR Data Principles? - The Cambridge Crystallographic Data Centre (CCDC). Retrieved 8 March 2022, from https://www.ccdc.cam.ac.uk/Community/blog/Why-should-industry-care-about-the-FAIR-Data-Principles/. Also see the Pistoia Alliance FAIR Toolkit, "a community of FAIR data practitioners from leading life science, pharmaceutical and software companies" which provides practical guidance and tools for industry members concerning FAIR data, available here: https://fairtoolkit.pistoiaalliance.org/who-we-are/

the world, this Rule specifically aims to assist humanitarian organisations in fulfilling their honourable missions through the sharing of data, knowledge, and technologies with such organisations where possible. As Michelle Bachelet, UN High Commissioner for Human Rights declared, "We can use encrypted communications, satellite imagery and data streams to directly defend and promote human rights. We can even use artificial intelligence to predict and head off human rights violations."[168] However, in order to do so, data and adequate tools are required.

The value of data sharing within the sector is confirmed in the usefulness of the Humanitarian Data Exchange (HDX) of the United Nations Office for the Coordination of Humanitarian Affairs (OCHA).[169] HDX is a data sharing platform which was launched in 2014 with the aim of facilitating access and use of humanitarian data.[170] Organisations which are legal entities can become members of an organisation and contribute datasets to the HDX. Organisations must be verified to "ensure they are trusted and have relevant data to share with the HDX user community".[171]

It should also be underlined that data sharing and effective collaboration within this sector represents a known challenge, especially due to the sensitive nature of data[172] which may result in serious risks to concerned data subjects. For example, in the context of a political crisis, while it may be useful for a telecommunications company or a social media network to receive data on the location of individuals, e.g., where a large number of people are gathered, malicious actors could easily misuse such data to harm the opposition.

Under this Rule, where appropriate, the Organisation is called upon to regularly consider potential opportunities to share relevant data, metadata, and where applicable, useful technologies, with humanitarian organisations in the manner considered most appropriate by the Organisation. All data shared shall, as a rule, be anonymous and/or aggregated with the objective of reducing potential harms to individuals and should take other risks into consideration. To this end, the Organisation's data sharing agreements, arrangements, policies, and actions under this Rule shall be documented in writing. For this reason, **as with the other data sharing rules included in the UM-DPCSR Framework, it is necessary that the sharing party approaches all data sharing with due caution and in compliance with the applicable legal provisions and other rules in the Framework**.

[168] Bachelet, M. (2019). *Human rights in the digital age - Can they make a difference?*. Speech, Japan Society, New York. Retrieved from https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25158&LangID=E

[169] Gazi, T. (2020). Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR. *Journal Of International Humanitarian Action*, *5*(1). doi: 10.1186/s41018-020-00078-0

[170] Humanitarian Data Exchange. Frequently Asked Questions. Retrieved 8 March 2022, from https://data.humdata.org/faq

[171] Humanitarian Data Exchange. Organisations. Retrieved 8 March 2022, from https://data.humdata.org/faq#body-faq-Organisations

[172] United Nations Office for the Coordination of Humanitarian Affairs and the Global Food Security Cluster. *Field Guide to Data Sharing*. Retrieved from https://fscluster.org/sites/default/files/documents/field_guide_to_data_sharing.pdf

Principle 5. Devote a portion of revenues to awareness campaigns for citizens with regards to the data-centric society

Principle 5. Devote a portion of revenues to awareness campaigns for citizens with regards to the data-centric society

Rule 1: Invest in digital social capital to promote social enterprise within the Organisation. The Organisation shall make use of digital and data-driven tools to engage internal stakeholders with the aim of positively contributing to the Organisation.

The first Rule of Principle 5 requires adhering Organisations to invest in digital social capital in order to promote social enterprise within the Organisation. For the purposes of the UM-DPCSR Framework, 'social enterprise' is to be understood as the integration of economic and social value creation within the Organisation, meaning that the objective of the Organisation is both to make profit and to contribute positively to society.[173] At the same time, digital social capital is fundamental in order to create a social enterprise.[174]

Business enterprises are being transformed into social enterprises as the societal impact of businesses with respect to their employees, customers, and more generally, society and 'doing good' is becoming more important for younger generations.[175] Investing in digital social capital can allow Organisations to improve how they engage with their stakeholders online or in ways that involve data, improving the quality of virtual interactions. In doing so, the social enterprise contributes positively to increasing the participation of individuals in their local environment, the workplace, and its greater context.

The approach taken in this Rule leverages pro-bono (philanthropic approach represented in the last part of Carroll's triangle[176] - see Figure 5) but goes beyond it, as it is specifically aimed to mitigate divergence between shareholders and external stakeholders.

[173] In the literature, there are various definitions of social enterprise which are put forward and which also vary according to the geographical context in which they are found, e.g., Europe or the United States (for more on this matter, see Kerlin, J. (2009). *Social Enterprise: A Global Comparison*. Medford, Massachusetts: University Press of New England). The definition of social enterprise for the intentions of the UM-DPCSR Framework is more aligned with the American perspective which combines the 'good doing' with the mission of the corporation which is inherently to generate financial capital.

[174] Lahiri, G. (2018). *Introduction: The rise of the social enterprise, 2018 Global Human Capital Trends*. Deloitte. Retrieved from https://www2.deloitte.com/us/en/insights/focus/human-capital-trends/2018/introduction.html

[175] See p. 2 Deloitte. (2018). *The Rise of Social Enterprise, 2018 Global Human Capital Trends*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/pa/Documents/human-capital/2018/2018-HCTrends_Rise-of-the-social-enterprise.pdf

[176] Carroll, A. B. (2016). Carroll's pyramid of CSR: taking another look. *International Journal of Corporate Social Responsibility*, *1*(1). https://doi.org/10.1186/s40991-016-0004-6

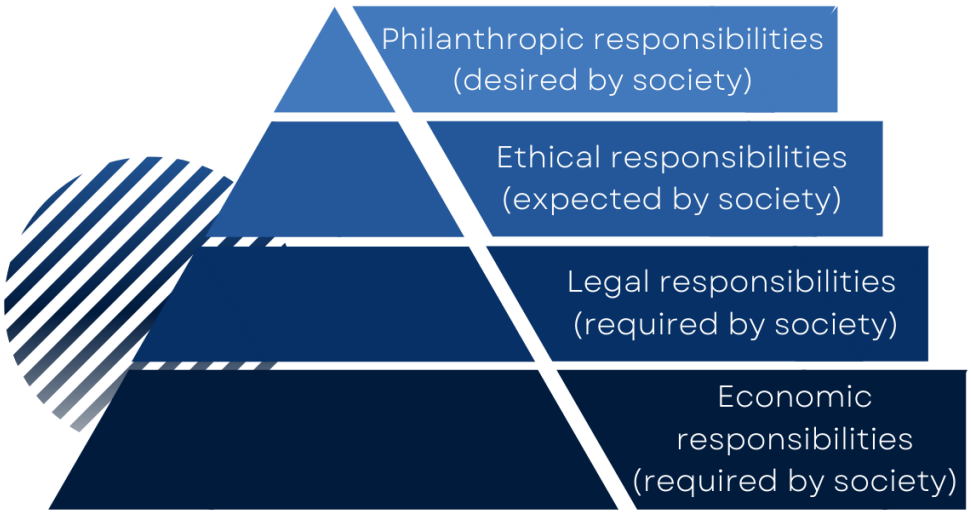


Figure 5: Carroll's CSR Triangle[177]

Under this Rule, the Organisation shall encourage the engagement of its internal stakeholders by investing in being a good corporate citizen, promoting collaboration and trust among stakeholders for a common good in support of the larger stakeholder network. This can be accomplished through the fostering, in the digital arena, of personal relationships, social network support, civic engagement, and the fostering of trust and engagement.[178] Bourdieu defined social capital as "the aggregate of the actual or potential resources which are linked to possession of a durable network of more or less institutionalized relationships of mutual acquaintance or recognition".[179] Digital social capital, a budding concept, can then be seen as the metamorphosis of traditional social capital in the digital milieu. It has been established that inside of organisations, "trusting relationships with key stakeholders that evolve from enhancing social capital are keys to competitive success" [180] and that

> Companies without social capital risk their stakeholder relationships. For example, without relationships built on trust, companies can face erosion of employee loyalty (a problem during employee shortages). They can experience negative responses from local communities that provide the necessary infrastructure. They can alienate their customers.[181]

Digital social capital operates like financial capital in that using it creates more of it.[182] But instead of goods and services, it is personal relationships and positive affective bonds that are used and created through digital means. Digital social capital is essentially the "process of building digital communities through

[177] See "Figure 1", p. 5 in Carroll, A. B. (2016). Carroll's pyramid of CSR: taking another look. *International Journal of Corporate Social Responsibility, 1*(1). https://doi.org/10.1186/s40991-016-0004-6

[178] Stiglitz, J., Fitoussi, J., & Durand, M. (eds.) (2018). *For Good Measure: Advancing Research on Well-being Metrics Beyond GDP*. Paris: OECD Publishing. https://doi.org/10.1787/9789264307278-en.

[179] See p. 84 Bourdieu, P. "The forms of capital." in Granovetter, M., & Swedberg, R. (2018). *The Sociology of Economic Life*. Boulder: Routledge.

[180] See p. 20 Waddock, S. (2001). How Companies Build Social Capital. *Reflections: The Sol Journal, 3*(1), 18-24. doi: 10.1162/152417301750406086

[181] Ibid. pp. 20-21

[182] Williams, D. (2006). On and off the 'Net: Scales for Social Capital in an Online Era. *Journal Of Computer-Mediated Communication, 11*(2), 593-628. doi: 10.1111/j.1083-6101.2006.00029.x

planning practice, specifically public participation processes that embrace Internet tools."[183] In this Rule, digitally enhanced social relationships that comprise and fulfil individual and collective goals and needs **are brought into the information age, which has significantly changed the way that people and organisations interact. Digital social capital is therefore the logical continuation of traditional social capital, only in the digital and data society realm**.

For the purposes of the UM-DPCSR Framework, this means that the Organisation shall **use technology to enhance greater stakeholder participation, both in and outside of the Organisation**. In implementing this Rule, the Organisation shall furthermore look towards the five design principles[184] for the social enterprise as inspiration for the growth of digital social capital:

1. **Purpose and meaning**: which stresses the importance of employees and other relevant stakeholders having a purpose and motivation with respect to the Organisation;
2. **Ethics and fairness**: which calls for using data and more generally, technologies in an ethical way, which is also supported by the UMDPCSR project, with the goal of making fair decisions;
3. **Growth and passion**: means providing jobs and implementing Organisational missions in a way that makes people happy, allowing them to be creative and grow within the Organisation;
4. **Collaboration and personal relationships**: which stresses that the Organisation should place emphasis on the important human connections;
5. **Transparency and openness**: promoting transparency in terms of information, looking at mistakes as opportunities for growth.[185]

Principle 5. Devote a portion of revenues to awareness campaigns for citizens with regards to the data-centric society

Rule 2: Allocate a portion of revenue to be devoted to awareness campaigns, in and outside of the Organisation. The Organisation shall implement a metric/model that will identify an adequate portion of revenue to be devoted to awareness campaigns.

The second rule of Principle 5 calls on the Organisation to allocate a portion of revenue to be devoted to awareness campaigns, in and outside of the Organisation itself. More precisely, the Organisation is requested to implement a specific model or metric that allows it to identify the correct portion of revenue which the same organisation will devote to both internal and external awareness campaigns in relation to

[183] See p. 123 Mandarano, L., Meenar, M., & Steins, C. (2010). Building Social Capital in the Digital Age of Civic Engagement. *Journal Of Planning Literature*, *25*(2), 123-135. doi: 10.1177/0885412210394102

[184] See p. 5 Deloitte. (2019). *Leading the social enterprise: Reinvent with a human focus, 2019 Deloitte Global Human Capital Trends*. Deloitte. Retrieved from https://www2.deloitte.com/content/dam/insights/us/articles/5136_HC-Trends-2019/DI_HC-Trends-2019.pdf

[185] Ibid.

UM-DPCSR. This Rule can easily be understood in relation to the rules that precede and follow it in Principle 5, insofar as the Organisation must allocate a specific budget to the implementation of programs that aim to better digital society.

This Rule does not in any way promote the commercialization of data. It furthermore aims to move away from the widely diffused accusations that CSR where organisations flaunt that 'x' amount of money has been spent on 'y' cause or by engaging in merely promotional campaigns disclosing that 'a', 'b', and 'c' have been done in the name of CSR. Instead, **the objective of this Rule and more generally of the whole UM-DPCSR Framework, is to cultivate genuine data awareness programs that promote digital rights, while at the same time making such investments auditable**.

Benlemlih and Bitar have shown that "high CSR involvement decreases investment inefficiency and consequently increases investment efficiency" and has the potential to increase organisations' competitive advantages in terms of image, reputation, segmentation, and long-term cost savings. [186]

The implementing Organisation shall therefore identify and follow the metric/model that will allow the Organisation to identify the correct portion of its revenue to be devoted to awareness campaigns, in and outside of the Organisation and allocate such amount accordingly. In order to adhere to the requirements of this Rule, the Organisation must first evaluate its current CSR budget. Secondly, the Organisation should estimate the relevant costs of the communication and stakeholder engagement-related activities under the UM-DPCSR Framework. Third, the Organisation should evaluate the appropriateness of its allocated budget considering the communication and stakeholder engagement required under the UM-DPCSR Framework. These steps shall be documented by the DPCSR Coordinator in line with the principle of accountability adopted by the Framework.

Principle 5. Devote a portion of revenues to awareness campaigns for citizens with regards to the data-centric society

Rule 3: Develop a yearly data awareness program. The Organisation shall make a programme available to individuals with clear objectives regarding data protection and cyber-/data-security literacy.

Rule 3 of Principle 5 calls on the Organisation to develop and execute a yearly data awareness program for individuals with clear objectives. The purpose of this Rule is both to educate stakeholders with respect to data protection and cyber-/data-security issues they should be aware of and to successfully communicate the UM-DPCSR initiative of the Organisation. Without communicating the initiative, the value and investments made to adhere to the Framework cannot be taken advantage of by the Organisation.

[186] See p. 647 Benlemlih, M., & Bitar, M. (2018). Corporate social responsibility and investment efficiency. *Journal of Business Ethics*, *148*(3), 647-671. https://doi.org/10.1007/s10551-016-3020-2

As part of the more general CSR/ESG communication strategy of the Organisation, a specific initiative should be developed annually to ensure that privacy, data protection and cyber-/data-security aspects are dealt with and communicated to the Organisation's stakeholders and the public. The Organisation shall determine the content of messaging, which should be related to its sector/area of expertise, the channel used to disseminate the message, and identify the facts that impact the effectiveness of the DPCSR communication.[187]

Good CSR communication is fundamental to create value and reap the benefits (and ROI) of any CSR program. Low awareness and "**unfavourable attributions towards companies' CSR activities remain critical impediments in companies' attempts to maximize business benefits from their CSR activities, highlighting a need for companies to communicate CSR more effectively to stakeholders**".[188] The actions to be undertaken according to this Rule also represent a form of stakeholder management though information provision and one-way communication.[189]

To implement this Rule, on an annual basis the Organisation shall determine the desired content of messaging, the channel which will be used to disseminate the message and identify the facts that impact the effectiveness of the DPCSR communication. Each of these steps should be documented in accordance with the principle of accountability. Under this Rule, initiatives of the Organisation may be global, national or local, and may be aimed, e.g., at helping individuals to recognize relevant trends, threats or risks (which may be in general or with specific reference to the Organisation's activity). The focus of the awareness program may also be targeted at employees in accordance with Principle 5, Rule 1.

Principle 5. Devote a portion of revenues to awareness campaigns for citizens with regards to the data-centric society

Rule 4: Contribute to digital educational initiatives for youth. The Organisation shall carry out concrete actions to further education about data protection rights and cybersecurity hygiene for youngsters.

Rule 4 of Principle 5 specifically calls for the Organisation to positively impact youth by contributing to education about data protection rights and cybersecurity hygiene. This can be accomplished in a number of ways, e.g., by school outreach programs, community outreach programs, and more. As cybersecurity and data protection risks continue to grow, it is important for the Organisation to actively contribute to

[187] See p. 9 Du, S., Bhattacharya, C., & Sen, S. (2010). Maximizing Business Returns to Corporate Social Responsibility (CSR): The Role of CSR Communication. *International Journal of Management Reviews*, *12*(1), 8-19. doi: 10.1111/j.1468-2370.2009.00276.x

[188] Ibid. p. 8

[189] Crane, A., & Glozer, S. (2016). Researching Corporate Social Responsibility Communication: Themes, Opportunities and Challenges. *Journal Of Management Studies*, *53*(7), 1223-1252. doi: 10.1111/joms.12196

initiatives that support education in this area for future leaders and consumers to protect themselves against threats.

In January 2022, Skuola.net carried out a Computer Assisted Web Interview of 2,600 Italian 11 to 24 year-olds on behalf of the Italian Data Protection Authority.[190] The survey found that nine out of ten young Italians are interested in the question of online privacy and would like to participate in dedicated learning sessions on such topics.[191] The survey also tackled the question of awareness of rights and the rules that govern digital services.[192] Other key numbers from the survey include:

- two out of three respondents signed up for social networks before they were old enough to do so;
- when signing up for a new online service or accessing a new app, approximately 66 percent of respondents accept the terms of service without ever reading them, 16% occasionally check the privacy policy of the services they use and 18% try to understand more;
- 50% of respondents 18 and above systematically ignore privacy policies;
- only 43% of respondents are aware that victims of cyberbullying can request the removal of content that concerns them, and that if the platform ignore their request, they can contact the Italian Data Protection Authority.[193]

These numbers clearly demonstrate that there is a significant need to educate children, teenagers, and young adults about privacy, data protection, and data security issues. By contributing to educational initiatives for youth to further education about data protection rights and cybersecurity hygiene, the Organisation will help to ensure that future adults are more aware of their rights, but also about data security risks. In the long term, this has the potential to provide for a safer and more conscious digital society.

In order to implement this Rule, on a yearly basis the Organisation shall identify topics related to its activities where privacy, data protection, and data security risks may be posed to youngsters. Where no such risks are identified, instead of organizing specific programs for youth related to the Organisation's business, the Organisation shall adhere to this Rule by, e.g., funding other appropriate and established initiatives in this area. Where relevant risks are identified, under this Rule the Organisation must identify the most appropriate manner to communicate such risks to youth. For example, the Organisation may establish a youth training program at its own premises, work with schools to organize informational events, provide schools with relevant materials, execute targeted media campaigns, etc.

[190] www.skuola.net. (2022). *"Interessati, ma poco consapevoli. I giovani chiedono alla scuola di parlare di privacy" Analisi Dati Web Survey erogata sul portale www.skuola.net*. Retrieved from https://www.gpdp.it/documents/10160/0/Survey+su+privacy+online+-+Giornata+europea+della+protezione+dei+dati+personali+2022.pdf/4fa353a9-f26a-45a5-afce-e07de5f54622?version=1.3

[191] Ibid.

[192] See Ibid. pp. 2-3

[193] Ibid.

Principle 5. Devote a portion of revenues to awareness campaigns for citizens with regards to the data-centric society

Rule 5: Actively promote the protection of individuals in relation to data practices. The Organisation shall devise specific outreach programs on disinformation, fake news, and data-driven threats.

The fifth rule of Principle 5 concerns and seeks to mitigate online, technologically driven data protection, cyber, and democratic risks. More specifically, this Rule calls on the Organisation to contribute to combatting cyber incidents, disinformation, fake news, and other data-driven threats via dedicated outreach programs funded in accordance with Rules 2, 3, and 4 of Principle 5. This Rule therefore concerns three primary domains: cybersecurity,[194] disinformation, and misinformation.

Cybersecurity awareness-raising should be understood as initiatives which bring attention to the question of cybersecurity to permit individuals to identify related risks and respond in an appropriate manner.[195] This can be accomplished, e.g., through dedicated awareness-raising activities which could range from material published on the Organisation's website to online, radio or television advertisements, etc.

In addition, in order to appreciate this Rule, it is necessary to define both disinformation and misinformation (fake news). Disinformation is defined as "verifiably false or misleading information created, presented and disseminated for economic gain or to intentionally deceive the public".[196] On the other hand, misinformation "is verifiably false information that is spread without the intention to mislead, and often shared because the user believes it to be true."[197]

The European Commission has highlighted the threats which disinformation and misinformation have on democracy due to their very nature which tend to polarize debates and even threaten public health and the security of the EU.[198] To this end, the EU has put forward several initiatives which aim to combat such threats including the Code of Practice on Disinformation, the European Digital Media Observatory, and the European Democracy Action Plan, among others.[199]

In order to implement this Rule, the Organisation shall first identify potential data security, disinformation, and misinformation threats in relation to the Organisation's activities. Such threats should be mapped on a regular basis as necessary, and no less than one time per year. Following the identification and documentation of the relevant threats, the Organisation must identify the target group it wishes to reach

[194] Where other rules, e.g., Principle 5, Rule 4, concern cybersecurity, this rule also takes threats such as disinformation and misinformation into consideration.

[195] National Institute of Standards and Technology. Awareness. *Computer Security Resource Center*. Retrieved from https://csrc.nist.gov/glossary/term/awareness

[196] European Commission. Online disinformation. Retrieved 8 March 2022, from https://digital-strategy.ec.europa.eu/en/policies/online-disinformation

[197] European Commission. Online disinformation. Retrieved 8 March 2022, from https://digital-strategy.ec.europa.eu/en/policies/online-disinformation

[198] Ibid.

[199] Ibid.

and determine the most appropriate and effective means for its outreach program(s) under this Rule. The Organisation may, for example, decide to engage in email and postal mail campaigns, radio advertisements, publish newspaper editorials, make posters or flyers available to customers, use large-scale print advertisement (billboards), etc. Identified risks, target groups, and the execution of the campaign shall be documented by the DPCSR Coordinator as appropriate.

7. About the Stakeholders, contributions and acknowledgments

In January 2020, a two-year research project on Data Protection as a Corporate Social Responsibility was launched under Prof. Dr. Balboni's direction at the European Centre on Privacy & Cybersecurity (ECPC) within the Maastricht University Faculty of Law. Since then, Mrs. Kate Francis (PhD candidate) and Dr. Balboni have worked together to concretize the concept and create the Framework. Regular meetings were held on a monthly basis with a group of Data Protection Stakeholders, Intergovernmental Stakeholders, and Business Stakeholders in which open discussions took place to discuss and validate the established rules. This dialogue with both European authorities and bodies and industry is considered to have increased the robustness and feasibility of the Framework both from the legislative and business points of view. The UM-DPCSR project has been executed in accordance with high academic and ethical standards and that the research has been carried out independently. Business Stakeholders, while contributing their perspectives on the UM-DPCSR Rules were prohibited impose outcomes on the research. The ECPC has received contribution (financial and in kind) from Business Stakeholders involved in the project.

Data Protection Stakeholders

Wojciech Wiewiórowski, Data Protection Supervisor – European Data Protection Supervisor (EDPS)

Prokopios Drogkaris, Network and Information Security Expert – European Union Agency for Cybersecurity (ENISA)

Sophie Nerbonne, Director of Economic Co-Regulation – Commission nationale de l'informatique et des libertés (CNIL)

Munish Ramlal, Former Head of System Supervision – Dutch Data Protection Authority (Autoriteit Persoonsgegevens)

Manon Korthals, Senior Strategy Advisor – Dutch Data Protection Authority (Autoriteit Persoonsgegevens)

Anamarija Mladinić, Senior Adviser Specialist – Croatian Data Protection Authority (Agencija za zaštitu osobnih podataka – AZOP)

Sophia Ignatidou, Principal Policy Adviser – Technology – United Kingdom Information Commissioner's Office (ICO)

Ellis Parry, Former Data Ethics Adviser - United Kingdom Information Commissioner's Office (ICO)

Miriam Wimmer, Director - Brazilian Data Protection Authority – Brazilian Data Protection Authority (ANPD)

Thiago Guimaraes Moraes, Coordinator of Technology & Research and Data Protection Officer Specialist – Brazilian Data Protection Authority (ANPD)

Albena Kuyumdzhieva, Stakeholder from the European Innovation Council and SMEs Executive Agency (EISMEA)

Aleš Lipičnik, President of the Broadcasting Council of the Republic of Slovenia – National Broadcasting Council of the Republic of Slovenia

Davide Baldini, Researcher working on the limits of profiling and automated decision making in EU Data Protection Law – University of Florence

Edith Sheila Vásquez Núnez, Doctoral candidate working on Privacy by Design in the context of connected cars – University of Oldenburg

Many thanks also to the Italian Data Protection Authority for acknowledging our data protection icons and especially thanks to:

Baldo Meo, Head, Public Outreach and Media Relations Department – Italian Data Protection Authority (Garante per la Protezione dei Dati Personali)

Emiliano Germani, External Relations and Media Service – Web and Social Media Editorial Office – Italian Data Protection Authority (Garante per la Protezione dei Dati Personali)

Intergovernmental Stakeholders

Mariya Koleva, Data Protection Officer – European Patent Office

Simona Barbieri, Data Protection Legal Advisor – European Patent Office

Gloria Folguera, Data Protection Officer – European Union Intellectual Property Office

Leena Van Der Made, Compliance & Data Protection Officer – European Space Agency

Rosemarie Leone, Information Technology Team Lead – European Space Agency

Business Stakeholders

Sarah Bakir, Privacy Coordinator CIOO - CIOO First Line Risk – Center of Expertise Risk – Rabobank

Rachid Quadai, Privacy Coordinator – Rabobank

Luuk Beursgens, UX Strategist – Rabobank

Joost Haar, UX Designer – Rabobank

Fabio Masini, Chief Technology Officer and Data Privacy Expert – Diennea S.r.l.

Valentina Fiorendi, Visual – UX/UI Designer – Diennea S.r.l.

Michela Parziale, Digital Consultant Manager – Diennea S.r.l.

Camilla Murtas, Legal Counsel – Maserati S.p.A.

The Maastricht European Centre on Privacy and Cybersecurity (ECPC)

Cosimo Monda, Director – European Centre on Data Privacy and Cybersecurity (ECPC)

Joyce Groneschild, Project Manager – European Centre on Data Privacy and Cybersecurity (ECPC)

Annex A

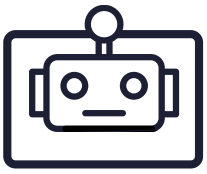
UM DPCSR Data Protection Icons for high-risk processing activities

Marketing

Your data will be used to send you marketing communications via [Organisation to indicate marketing methods].

Fully Automated processing

Your data will be used to evaluate certain personal aspects about you and make automated decisions.



Transfer

Your data will be transferred to a country outside the European Economic Area (EEA) which does not guarantee a high level of data protection.

Data Sharing in Exchange for Direct Profit/Value

We will share your data with other parties, including third parties, in exchange for direct profit and/or value.

Sensitive data

We will process your sensitive data including [Organisation to list types of sensitive data processed].

Systematic monitoring

We are monitoring your activities.

Annex B

Complete set of Arts. 13 and 14 GDPR Data Protection Icons for Information Notices

The UM-DPCSR Icons displayed above represent the complete set of Article 13 and Article 14 GDPR data protection icons in both their 'filled' and 'stroke' iterations to better facilitate their visualization according to the background colour of the website, app, etc. where they are placed.

Article 13 GDPR Information Notice Icons

Contact details of the Organisation

Art. 13(1)(a) GDPR

"a) the identity and the contact details of the controller and, where applicable, of the controller's representative;"

Contact details of the DPO

Art. 13(1)(b) GDPR

"b) the contact details of the data protection officer, where applicable;"

Purpose of Processing and Legal Basis

Art. 13(1)(c) GDPR

"c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;"

Legitimate Interest

Art. 13(1)(d) GDPR

"d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

Recipients of Data

Art. 13(1)(e) GDPR

"e) the recipients or categories of recipients of the personal data, if any;"

Data Transfer

Art. 13(1)(f) GDPR

"f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available."

Storage Period

Art. 13(2)(a) GDPR

"a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;"

Data Subject Rights

Art. 13(2)(b) GDPR

"b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;"

Consent Withdrawal

Art. 13(2)(c) GDPR

"c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;"

Lodge Complaint with a Supervisory Authority

Art. 13(2)(d) GDPR

"d) the right to lodge a complaint with a supervisory authority;"

Provision of Data for Contractual or Other Requirement

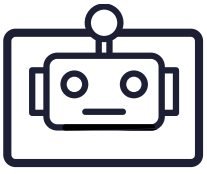
Art. 13(2)(e) GDPR

"e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;"

Automated Decision-making and Profiling

Art. 13(2)(f) GDPR

"f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."



Different Purposes of Processing

Art. 13(3) GDPR

"3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2."

Article 14 GDPR Information Notice Icons

Contact details of the Organisation

Art. 14(1)(a) GDPR

"a) the identity and the contact details of the controller and, where applicable, of the controller's representative;"

Contact details of the DPO

Art. 14(1)(b) GDPR

"b) the contact details of the data protection officer, where applicable;"

Purpose of Processing and Legal Basis

Art. 14(1)(c) GDPR

"c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;"

Categories of Data

Art. 14(1)(d) GDPR

"d) the categories of personal data concerned;"

Recipients of Data

Art. 14(1)(e) GDPR

"e) the recipients or categories of recipients of the personal data, if any;"

Data Transfer

Art. 14(1)(f) GDPR

"f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available."

Storage period

Art. 14(2)(a) GDPR

"a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;"

Legitimate Interest

Art. 14(2)(b) GDPR

"b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;"

Data Subject Rights

Art. 14(2)(c) GDPR

"c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;"

Consent Withdrawal

Art. 14(2)(d) GDPR

"d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;"

Lodge Complaint with a Supervisory Authority

Art. 14(2)(e) GDPR

"e) the right to lodge a complaint with a supervisory authority; "

Source of Data

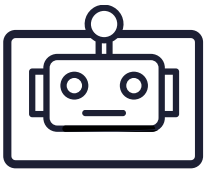
Art. 14(2)(f) GDPR

"f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;"

Automated Decision-making and Profiling

Art. 14(2)(g) GDPR

"g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."



Different Purposes of Processing

Art. 14(4) GDPR

"4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2."

Bibliography

AccessNow. (2021). *Transparency Reporting Index*. Retrieved from https://www.accessnow.org/transparency-reporting-index/

Anderson, J., & Rainie, L. (2020). Concerns about democracy in the digital age. *Pew Research Center Internet & Technology*. Retrieved from https://www.pewresearch.org/internet/2020/02/21/concerns-about-democracy-in-the-digital-age/

Article 29 Working Party. (2017). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018* and Global Privacy Assembly. (2021). *Working Group on Ethics and Data Protection in Artificial Intelligence Report*. Retrieved from https://edps.europa.eu/system/files/2021-10/1.3f-version-4.0-ethics-and-data-protection-in-ai-working-group-adopted_en_0.pdf

Article 29 Working Party. (2017). *Guidelines on transparency under Regulation 2016/679 Adopted on 29 November 2017 As last Revised and Adopted on 11 April 2018*. Retrieved from https://ec.europa.eu/newsroom/article29/items/622227/en

Behavioural Insights Team. (2019). *Best practice guide Improving consumer understanding of contractual terms and privacy policies: evidence-based actions for businesses*. London: Behavioural Insights Ltd. Retrieved from https://www.bi.team/wp-content/uploads/2019/07/BIT_WEBCOMMERCE_GUIDE_DIGITAL.pdf

Bachelet, M. (2019). *Human rights in the digital age - Can they make a difference?*. Speech, Japan Society, New York. Retrieved from https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25158&LangID=E

Baeza-Yates, R. (2018). Bias on the web. *Communications Of The ACM*, *61*(6), 54-61. doi: 10.1145/3209581

Friedman, B., & Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions On Information Systems*, *14*(3), 330-347. doi: 10.1145/230538.230561

Balboni, P., Botsi, A., Francis, K., Taborda Barata, M. (2020). Designing Connected and Automated Vehicles around Legal and Ethical Concerns – Data Protection as a Corporate Social Responsibility. *In Proceedings of SETN 2020 Workshop on AI, Law and Ethics hosted by the 11th Hellenic Conference on AI special events section*.

Balboni, P. (2009). *Trustmarks in E-Commerce: The Value of Web Seals and the Liability of their Providers*. T.M.C. Asser Press.

Balboni, P. (2018). Cambridge Analytica and the Concept of Fairness By Design [Blog]. Retrieved from https://www.paolobalboni.eu/index.php/2018/07/16/cambridge-analytica-and-the-concept-of-fairness-by-design/

Balboni, P. (2021). How data minimisation, data quality, and storage limitation can help in the fight against climate change [Blog]. Retrieved from https://www.paolobalboni.eu/index.php/2021/08/13/how-data-minimization-data-quality-and-storage-limitation-can-help-in-the-fight-against-climate-change/

Balboni, P. (2020). AI & Cybersecurity: Reflections on a multidimensional relationship [Blog]. Retrieved from https://www.paolobalboni.eu/index.php/2020/10/20/ai-cybersecurity-reflections-on-a-multidimensional-relationship/

Balboni, P., & Francis, K. (2020). Maastricht University Data Protection as a Corporate Social Responsibility (UM DPCSR) Research Project: UM DPCSR Icons Version 1.0. Retrieved 8 March 2022, from https://www.maastrichtuniversity.nl/maastricht-university-data-protection-corporate-social-responsibility-um-dpcsr-research-project-um

Balboni, P., & Francis, K. (2021). Help us improve transparency online and build a better digital society - Help us improve transparency online and build a better digital society - Maastricht University. Retrieved 8 March 2022, from https://www.maastrichtuniversity.nl/help-us-improve-transparency-online-and-build-better-digital-society

Balboni, P., & Francis, K. (2021). Easy privacy information via icons? Yes, you can! - Easy privacy information via icons? Yes, you can! - Maastricht University. Retrieved 8 March 2022, from https://www.maastrichtuniversity.nl/easy-privacy-information-icons-yes-you-can

Balkin, J. (2020). The Fiduciary Model of Privacy. *Harvard Law Review Forum*, *134*(11). Retrieved from https://harvardlawreview.org/wp-content/uploads/2020/10/134-Harv.-L.-Rev.-F.-11.pdf

Baldini, D. (2019). Article 22 GDPR and prohibition of discrimination. An outdated provision?. Retrieved 8 March 2022, from https://www.cyberlaws.it/2019/article-22-gdpr-and-prohibition-of-discrimination-an-outdated-provision/

Belgian Data Protection Authority against IAB Europe: Belgian Data Protection Authority. (2022). *The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR*. Retrieved from https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr

Bellamy, R., Dey, K., Hind, M., Hoffman, S.C., Houde, S., Kannan, K., Lohia, P., Martino, J., Mehta, S., Mojsilovic, A. et al. (2018). AI fairness 360: An extensible toolkit for detecting, understanding, and mitigating unwanted algorithmic bias. arXiv preprint arXiv:1810.01943.

Berk, R., Heidari, H., Jabbari, S., Joseph, M., Kearns, M., Morgenstern, J., Neel, S., Roth, A. (2017). A Convex Framework for Fair Regression. (2017). arXiv:cs.LG/1706.02409

Bashir, M., Hayes, C., Lambert, A. D., & Kesan, J. P. (2015). Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology*, *52*(1), 1-10. https://doi.org/10.1002/pra2.2015.145052010043

Benlemlih, M., & Bitar, M. (2018). Corporate social responsibility and investment efficiency. *Journal of Business Ethics*, *148*(3), 647-671. https://doi.org/10.1007/s10551-016-3020-2

Bourdieu, P. "The forms of capital." in Granovetter, M., & Swedberg, R. (2018). *The Sociology of Economic Life*. Boulder: Routledge.

Budish, R. (2013). What Transparency Reports Don't Tell Us. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2013/12/what-transparency-reports-dont-tell-us/282529/

Calabrese, A., Costa, R., Levialdi, N., & Menichini, T. (2016). A fuzzy analytic hierarchy process method to support materiality assessment in sustainability reporting. *Journal Of Cleaner Production*, *121*, 248-264. doi: 10.1016/j.jclepro.2015.12.005

California Attorney General Rob Bonta. (2022). *On Data Privacy Day, Attorney General Bonta Puts Businesses Operating Loyalty Programs on Notice for Violations of California Consumer Privacy Act*. Retrieved from https://oag.ca.gov/news/press-releases/data-privacy-day-attorney-general-bonta-puts-businesses-operating-loyalty

Carroll, A. B. (2016). Carroll's pyramid of CSR: taking another look. *International Journal of Corporate Social Responsibility*, *1*(1). https://doi.org/10.1186/s40991-016-0004-6

Cheffins, B. (2001). Does Law Matter? The Separation of Ownership and Control in the United Kingdom. *The Journal of Legal Studies*, *30*(2), 459-84, as seen on p. 1077 in Rauterberg, G., & Talley, E. (2017). Contracting Out of the Fiduciary Duty of Loyalty: An Empirical Analysis of Corporate Opportunity Waivers. *Columbia Law Review*, *117*(5), 1075-151

Cisco. (2020). *2020 Data Privacy Benchmark Study: Discover how organisations are benefiting from data privacy investments*. Retrieved from https://www.cisco.com/c/en_uk/products/security/security-reports/data-privacy-report-2020.html#~data-privacy-report

Cisco. (2020). *Cisco Data Privacy Benchmark Study 2020, From Privacy to Profit: Achieving Positive Returns on Privacy Investments*. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf?CCID=cc000160&DTID=esootr000515&OID=rptsc020143

Coldewey, D. (2019). Racial bias observed in hate speech detection algorithm from Google. *TechCrunch*. Retrieved from https://techcrunch.com/2019/08/14/racial-bias-observed-in-hate-speech-detection-algorithm-from-google/

Council of Europe. (2017). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data adopted January 2017. Strasbourg, France: Council of Europe. Retrieved fromhttps://rm.coe.int/16806ebe7a.

Council of Europe. (2018). *Study on the Human Rights Dimensions of Automated Data Processing Techniques (In Particular Algorithms and Possible Regulatory Implications) DGI(2017)12*. Strasbourg: Council of Europe. Retrieved from https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

Council of Europe. (2019). *Council of Europe study DGI(2019)05,* Responsibility and AI (pp. 29-98). Council of Europe. Retrieved from https://rm.coe.int/responsability-and-ai-en/168097d9c5

Council of Europe. (2019). Unboxing Artificial Intelligence: 10 steps to protect Human Rights. Retrieved from https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

Council of Europe. (2020). Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. Retrieved from https://hcav.am/en/recommendation-coe/

Council of Europe. (2019). Responsibility and AI study DGI (2019) 05. Retrieved from https://rm.coe.int/responsability-and-ai-en/168097d9c5

Consent. (2022). Retrieved 8 March 2022, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

Crane, A., & Glozer, S. (2016). Researching Corporate Social Responsibility Communication: Themes, Opportunities and Challenges. *Journal Of Management Studies*, *53*(7), 1223-1252. doi: 10.1111/joms.12196

d'Alessandro, B., O'Neil, C., & LaGatta, T. (2017). Conscientious Classification: A Data Scientist's Guide to Discrimination-Aware Classification. *Big Data*, *5*(2), 120-134. doi: 10.1089/big.2016.0048

Deloitte. (2018). *The Rise of Social Enterprise, 2018 Global Human Capital Trends*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/pa/Documents/human-capital/2018/2018-HCTrends_Rise-of-the-social-enterprise.pdf

Deloitte. (2019). *Leading the social enterprise: Reinvent with a human focus, 2019 Deloitte Global Human Capital Trends*. Deloitte. Retrieved from https://www2.deloitte.com/content/dam/insights/us/articles/5136_HC-Trends-2019/DI_HC-Trends-2019.pdf

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Retrieved from https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Du, S., Bhattacharya, C., & Sen, S. (2010). Maximizing Business Returns to Corporate Social Responsibility (CSR): The Role of CSR Communication. *International Journal Of Management Reviews*, *12*(1), 8-19. doi: 10.1111/j.1468-2370.2009.00276.x

Efroni, Z., Metzger, J., Mischau, L., & Schirmbeck, M. (2019). Privacy Icons: *European Data Protection Law Review, 5*(3), 352-366. doi: 10.21552/edpl/2019/3/9

European Commission. (n.d.). Online disinformation. Retrieved 8 March 2022, from https://digital-strategy.ec.europa.eu/en/policies/online-disinformation

European Commission. (n.d.). Corporate social responsibility & Responsible business conduct. Retrieved from https://ec.europa.eu/growth/industry/sustainability/corporate-social-responsibility-responsible-business-conduct_en

European Commission. (n.d.). Data protection in the EU. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

European Commission. (2018). Guidance on sharing private sector data in the European data economy, Accompanying the document Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions "Towards a common European data space", {COM(2018) 232 final}. Retrieved at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0125&rid=2

European Commission. (2018). European Group on Ethics in Science and New Technologies Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems. Brussels, Belgium: European Commission. Retrieved from https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

European Commission. (2018). Guidance on sharing private sector data in the European data economy, Accompanying the document Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions "Towards a common European data space", {COM(2018) 232 final}. Retrieved at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0125&rid=2;

European Commission. (2018). Annex to the Commission implementing decision on the adoption of the work programme for 2018 and on the financing of Connecting Europe Facility (CEF) - Telecommunications Sector. Retrieved from https://digital-strategy.ec.europa.eu/en/news/connecting-europe-facility-cef-telecom-work-programme-2018-adopted

European Commission. (2018). *Ethics and data protection*. Retrieved from https://ec.europa.eu/info/sites/default/files/5._h2020_ethics_and_data_protection_0.pdf

European Commission. (2020, February 20). Data sharing in the EU – common European data spaces (new rules). Retrieved from https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Data-sharing-in-the-EU-common-European-data-spaces-new-rules-_en

European Commission. (2020, February 19). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM(2020) 66 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

European Commission, Directorate-General for Communications Networks, Content and Technology, (2020). *Shaping the digital transformation in Europe*, Publications Office. https://data.europa.eu/doi/10.2759/294260

European Commission. (2000, December 16). Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final). Retrieved from https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission. (2020). White Paper On Artificial Intelligence - A European approach to excellence and trust. COM (2020) 65 final.

European Commission. (2021). Business-to-government data sharing: Questions and answers | Shaping Europe's digital future. Retrieved 8 March 2022, from https://digital-strategy.ec.europa.eu/en/faqs/business-government-data-sharing-questions-and-answers

European Commission. (2022, February 23). A European Strategy for data. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/strategy-data

European Commission (2022, February 23). Just and sustainable economy: Commission lays down rules for companies to respect human rights and environment in global value chains. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1145

European Commission. (2022). *Data Act: Commission proposes measures for a fair and innovative data economy*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

European Commission. Data sharing in the EU – common European data spaces (new rules). Retrieved from https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Data-sharing-in-the-EU-common-European-data-spaces-new-rules-_en

European Commission Expert Group on FAIR Data. (2018). *Turning FAIR into reality: Final Report and Action Plan from the European Commission Expert Group on FAIR Data*. European Commission. Retrieved from https://ec.europa.eu/info/sites/default/files/turning_fair_into_reality_0.pdf

European Data Protection Board. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020*. EDPB. Retrieved from https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

European Data Protection Supervisor. (2016). *Opinion 9/2016 on Personal Information Management Systems: Towards more user empowerment in managing and processing personal data*. Brussels: EDPS. Retrieved from https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

European Data Protection Supervisor. (2018, January 25). Report Towards a digital ethics – EDPS Ethics Advisory Group. Brussels, Belgium: EDPS. Retrieved from: https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

European Data Protection Supervisor. (2019). *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*. EDPS. Retrieved from https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf

European Data Protection Supervisor. (2022). *The EDPS Strategy 2020-2024: Shaping a Safer Digital Future*. Brussels: EDPS. Retrieved from https://edps.europa.eu/press-publications/publications/strategy/shaping-safer-digital-future_en

European Union Agency for Cybersecurity. (2016). *Guidelines for SMEs on the security of personal data processing*. European Union Agency for Cybersecurity. Retrieved from https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

European Union Agency for Cybersecurity. (2020). *Artificial Intelligence: Cybersecurity Essential for Security & Trust*. Retrieved from https://www.enisa.europa.eu/news/enisa-news/artificial-intelligence-cybersecurity-essential-for-security-trust

European Union Agency for Cybersecurity. (2021). *Data Pseudonymisation: Advanced Techniques and Use Cases*. ENISA. Retrieved from https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases

European Union Agency for Cybersecurity. (2022). *Data Protection Engineering: From Theory to Practice*. European Union Agency for Cybersecurity. Retrieved from https://www.enisa.europa.eu/publications/data-protection-engineering

FAIR Principles - GO FAIR. Retrieved 8 March 2022, from https://www.go-fair.org/fair-principles/

Fiduciary. (2022). *Oxford Reference*. Retrieved from https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095816799

Gazi, T. (2020). Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR. *Journal Of International Humanitarian Action*, *5*(1). doi: 10.1186/s41018-020-00078-0

Gallula, D. and Frank, A.J. (2014). User Empowering Design. In Proceedings of the 2014 European Conference on Cognitive Ergonomics (ECCE '14). *Association for Computing Machinery*, New York, NY, USA, Article 38, 1–3. DOI:https://doi.org/10.1145/2637248.2742999

Gold, Andrew S., The Loyalties of Fiduciary Law (December 20, 2013). Philosophical Foundations of Fiduciary Law, Andrew S. Gold & Paul B. Miller, eds., Oxford University Press, 2014, Forthcoming, Available at SSRN: https://ssrn.com/abstract=2370598

González-Bailón, S., Wang, N., Rivero, A., Borge-Holthoefer, J., & Moreno, Y. (2014). Assessing the bias in samples of large online networks. *Social Networks*, *38*, 16-27. doi: 10.1016/j.socnet.2014.01.004

Goodman, B. (2016). Discrimination, Data Sanitisation and Auditing in the European Union's General Data Protection Regulation. *European Data Protection Law Review*, *2*(3). doi: https://doi.org/10.21552/EDPL/2016/4/8

Google Transparency Report. (2022). Retrieved 8 March 2022, from https://transparencyreport.google.com/about?hl=en

GRI - Materiality and topic boundary. Retrieved 8 March 2022, from https://www.globalreporting.org/how-to-use-the-gri-standards/questions-and-answers/pre-2021-gri-standards-system-faq/materiality-and-topic-boundary/

Gurría, A. Openness and Transparency - Pillars for Democracy, Trust and Progress - OECD. Retrieved 8 March 2022, from https://www.oecd.org/unitedstates/opennessandtransparency-pillarsfordemocracytrustandprogress.htm

Hart, K. (2019). Privacy policies are read by an aging few. Retrieved 8 March 2022, from https://www.axios.com/few-people-read-privacy-policies-survey-fec3a29e-2e3a-4767-a05c-2cacdcbaecc8.html

High-Level Expert Group on Artificial Intelligence (AI HLEG). (2020). *The Assessment List for Trustworthy Artificial Intelligence (ALTAI)*. Brussels: European Commission. Retrieved from https://futurium.ec.europa.eu/en/european-ai-alliance/document/ai-hleg-assessment-list-trustworthy-artificial-intelligence-altai?language=fr

High-Level Expert Group on Business-to-Government Data Sharing. (2020). *Towards a European strategy on business-to-government data sharing for the public interest*. European Union. Retrieved from https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/B2GDataSharingExpertGroupReport-1.pdf

Humanitarian Data Exchange. Frequently Asked Questions. Retrieved 8 March 2022, from https://data.humdata.org/faq

Humanitarian Data Exchange. Organisations. Retrieved 8 March 2022, from https://data.humdata.org/faq#body-faq-Organisations

Hung, C. (2021, September 23). Three Reasons Why CSR and ESG Matter to Businesses. *Forbes.* Retrieved from https://www.forbes.com/sites/forbesbusinesscouncil/2021/09/23/three-reasons-why-csr-and-esg-matter-to-businesses/#:~:text=Both%20terms%20relate%20to%20the,or%20quantify%20such%20social%20efforts.

Information Commissioner's Office. (2018). *Investigation into the use of data analytics in political campaigns Investigation update*. Retrieved from https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf

Informative chiare. (2021). Retrieved 8 March 2022, from https://www.garanteprivacy.it/temi/informativechiare

International Conference of Data Protection and Privacy Commissioners. (2018). *Declaration on Ethics and Data Protection in Artificial Intelligence*. Brussels. Retrieved from https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_ai-declaration_adopted_en_0.pdf

International Organization for Standardization and Stichting Global Reporting Initiative. (2014). *GRI G4 Guidelines and ISO 26000:2010 How to use the GRI G4 Guidelines and ISO 26000 in conjunction*. International Organization for Standardization and Stichting Global Reporting Initiative. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso-gri-26000_2014-01-28.pdf

Irish Data Protection Commissioner. Data Sharing in the Public Sector. Retrieved from https://www.dataprotection.ie/en/dpc-guidance/data-sharing-in-the-public-sector

Jordana J. George, Jie (Kevin) Yan & Dorothy E. Leidner (2020) Data Philanthropy: Corporate Responsibility George, J., Yan, J., & Leidner, D. (2020). Data Philanthropy: Corporate Responsibility with Strategic Value?. *Information Systems Management*, *37*(3), 186-197. doi: 10.1080/10580530.2020.1696587

Kerlin, J. (2009). *Social Enterprise: A Global Comparison*. Medford, Massachusetts: University Press of New England

Krumay, B., & Klar, J. (2020). Readability of Privacy Policies. *Data And Applications Security And Privacy XXXIV*, 388-399. doi: 10.1007/978-3-030-49669-2_22.

Ladner, R. (2015). Design for User Empowerment. *Interactions*. Retrieved from https://dl.acm.org/doi/pdf/10.1145/2723869

Lahiri, G. (2018). *Introduction: The rise of the social enterprise, 2018 Global Human Capital Trends*. Deloitte. Retrieved from https://www2.deloitte.com/us/en/insights/focus/human-capital-trends/2018/introduction.html

Lee, N., Resnick, P., & Barton, G. (2019). *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms*. Brookings Institution. Retrieved from https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

Llanos, J. (2021). *Transparency reporting Considerations for the review of the privacy guidelines*. Paris: OECD Publishing. Retrieved from https://www.oecd.org/science/transparency-reporting-e90c11b6-en.htm

Maastricht University. (2019). *Inaugural lecture Paolo Balboni*. Retrieved from https://www.maastrichtuniversity.nl/news/inaugural-lecture-paolo-balboni

Mandarano, L., Meenar, M., & Steins, C. (2010). Building Social Capital in the Digital Age of Civic Engagement. *Journal Of Planning Literature*, *25*(2), 123-135. doi: 10.1177/0885412210394102

Mantelero, A. (2014). The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. *Computer Law & Security Review*, *30*(6), 643-660. doi: 10.1016/j.clsr.2014.09.004

Martens, B., de Streel, A., Graef, I., Tombal, T., & Duch-Brown, N. (2020). *Business-to-business data sharing: An economic and legal analysis*. (JRC Digital Economy Working Paper Series; Vol. 2020, No. 05). European Commission. https://ec.europa.eu/jrc/sites/jrcsh/files/jrc121336.pdf

Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A Survey on Bias and Fairness in Machine Learning. *ACM Computing Surveys*, *54*(6), 1-35. doi: 10.1145/3457607

Moratis, L. (2018). Signalling Responsibility? Applying Signalling Theory to the ISO 26000 Standard for Social Responsibility. *Sustainability*, *10*(11), 4172. doi: 10.3390/su10114172

Moreno, A. (2021). Why should industry care about the FAIR Data Principles? - The Cambridge Crystallographic Data Centre (CCDC). Retrieved 8 March 2022, from https://www.ccdc.cam.ac.uk/Community/blog/Why-should-industry-care-about-the-FAIR-Data-Principles/

Morgan Stanley Institute for Sustainable Investing. (2019). *Sustainable Signals: Individual Investor Interest Driven by Impact, Conviction and Choice*. Retrieved from https://www.morganstanley.com/pub/content/dam/msdotcom/infographics/sustainable-investing/Sustainable_Signals_Individual_Investor_White_Paper_Final.pdf

National Institute of Standards and Technology. Awareness. *Computer Security Resource Center*. Retrieved from https://csrc.nist.gov/glossary/term/awareness

New Global Research from Accenture Interactive Urges CMOs to Put People Before Data Collection to Deliver a Better Digital Advertising Experience. Accenture. (2019, October 16). Retrieved from https://newsroom.accenture.com/news/new-global-research-from-accenture-interactive-urges-cmos-to-put-people-before-data-collection-to-deliver-a-better-digital-advertising-experience.htm

New York Times. (2020). What's Going On in This Graph? | Internet Privacy Policies. Retrieved from https://www.nytimes.com/2020/01/02/learning/whats-going-on-in-this-graph-internet-privacy-policies.html#:~:text=Privacy%20policies%20describe%20data%20that,1400%20(high%20college%20level.

OECD (2019). *OECD Business and Finance Outlook 2019: Strengthening Trust in Business*, OECD Publishing, Paris. https://doi.org/10.1787/af784794-en.

OECD Trust in Business Forum - OECD. (2019). Retrieved 8 March 2022, from https://www.oecd.org/corporate/oecd-trust-in-business-forum.htm

O'Riordan, L., & Fairbrass, J. (2013). Managing CSR Stakeholder Engagement: A New Conceptual Framework. *Journal Of Business Ethics*, *125*(1), 121-145. doi: 10.1007/s10551-013-1913-x

Patterson, D., Gonzalez, J., Le, Q., Liang, C., Munguia, L. M., Rothchild, D., So, D., Texier, M. & Dean, J. (2021). Carbon emissions and large neural network training. *arXiv preprint arXiv:2104.10350*.

Pegoraro, R. (2019). Tech Companies Are Quietly Phasing Out a Major Privacy Safeguard. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2019/09/what-happened-transparency-reports/599035/

Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN

Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN

Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final. Retrieved from https://ec.europa.eu/info/sites/default/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf

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 Legislative Acts, COM/2021/206 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN

Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, COM/2020/829 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN

Rauterberg, G., & Talley, E. (2017). Contracting Out of the Fiduciary Duty of Loyalty: An Empirical Analysis of Corporate Opportunity Waivers. *Columbia Law Review, 117*(5), 1075-1152. Retrieved from https://columbialawreview.org/content/contracting-out-of-the-fiduciary-duty-of-loyalty-an-empirical-analysis-of-corporate-opportunity-waivers/

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)

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881

Rossi, A., & Palmirani, M. (2019). DaPIS: a Data Protection Icon Set to Improve Information Transparency under the GDPR. Bologna: Università di Bologna, CIRSFID. Retrieved from http://gdprbydesign.cirsfid.unibo.it/wp-content/uploads/2019/01/report_DaPIS_jan19.pdf

Richards, N., & Hartzog, W. (2016). Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review, 431*(9), 431-471

Schönherr, N., Findler, F., & Martinuzzi, A. (2017). Exploring the interface of CSR and the Sustainable Development Goals. *Transnational Corporations,* 24(3): 33-49.

Shen Y., Vervier P.A. (2019). IoT Security and Privacy Labels. In: Naldi M., Italiano G., Rannenberg K., Medina M., Bourka A. (eds) Privacy Technologies and Policy. APF 2019. Lecture Notes in Computer Science, vol. 11498. Springer, Cham. https://doi.org/10.1007/978-3-030-21752-5_9

Singh, S., & Bankston, K. (2018). *The Transparency Reporting Toolkit: Content Takedown Reporting*. New America. Retrieved from https://www.newamerica.org/oti/reports/transparency-reporting-toolkit-content-takedown-reporting/introduction-and-executive-summary

Singh, R., Sumeeth, M., & Miller, J. (2011). Evaluating the Readability of Privacy Policies in Mobile Environments. *International Journal Of Mobile Human Computer Interaction*, *3*(1), 55-78. doi: 10.4018/jmhci.2011010104

Smith, A. (2022). Making the Case for the Competitive Advantage of Corporate Social Responsibility. *Business Strategy Series*, *8*, 186-195. doi: http://dx.doi.org/10.1108/17515630710684187.

Spenner, P., & Freeman, K. (2012). To Keep Your Customers, Keep It Simple. *Harvard Business Review*, (May). Retrieved from https://hbr.org/2012/05/to-keep-your-customers-keep-it-simple

Stiglitz, J., Fitoussi, J., & Durand, M. (eds.) (2018). *For Good Measure: Advancing Research on Well-being Metrics Beyond GDP*. Paris: OECD Publishing. https://doi.org/10.1787/9789264307278-en.

Support Centre for Data Sharing's website for more information: https://eudatasharing.eu/

Torelli, R., Balluchi, F., & Furlotti, K. (2020). The materiality assessment and stakeholder engagement: A content analysis of sustainability reports. *Corporate Social Responsibility And Environmental Management*, *27*(2), 470-484. doi: 10.1002/csr.1813

United Nations Office for the Coordination of Humanitarian Affairs and the Global Food Security Cluster. *Field Guide to Data Sharing*. Retrieved from https://fscluster.org/sites/default/files/documents/field_guide_to_data_sharing.pdf

van Vlijmen, H., Mons, A., Waalkens, A., Franke, W., Baak, A., & Ruiter, G. et al. (2020). The Need of Industry to Go FAIR. *Data Intelligence*, *2*(1-2), 276-284. doi: 10.1162/dint_a_00050

Wachter, S. (2019). Data Protection in the Age of Big Data. *Nature Electronics, 2*.

Waddock, S. (2001). How Companies Build Social Capital. *Reflections: The Sol Journal*, *3*(1), 18-24. doi: 10.1162/152417301750406086

Wilkinson, M., Dumontier, M., Aalbersberg, I., Appleton, G., Axton, M., & Baak, A. et al. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, *3*(1). doi: 10.1038/sdata.2016.18

Williams, D. (2006). On and Off the 'Net: Scales for Social Capital in an Online Era. *Journal Of Computer-Mediated Communication*, *11*(2), 593-628. doi: 10.1111/j.1083-6101.2006.00029.x

Windwehr, S., & York, J. (2020). Thank You For Your Transparency Report, Here's Everything That's Missing. Retrieved 8 March 2022, from https://www.eff.org/deeplinks/2020/10/thank-you-your-transparency-report-heres-everything-thats-missing

Woolery, L., Budish, R., & Bankston, K. (2016). *Transparency Reporting Toolkit: Reporting. Guide and Template for Reporting U.S. Government Requests for User Information*. New America and the Berkman Klein Center for Internet & Society. Retrieved from https://dash.harvard.edu/bitstream/handle/1/29914191/Transparency_Reporting_Guide_and_Template-Final.pdf?sequence=1&isAllowed=y

World Bank. (2016). World Development Report 2016: Digital Dividends. Washington, DC: World Bank. doi:10.1596/978-1-4648-0671-1.

Word Economic Forum. (2018). Insight Report, Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society. Retrieved from http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf

www.skuola.net. (2022). *"Interessati, ma poco consapevoli. I giovani chiedono alla scuola di parlare di privacy" Analisi Dati Web Survey erogata sul portale www.skuola.net*. Retrieved from https://www.gpdp.it/documents/10160/0/Survey+su+privacy+online+-+Giornata+europea+della+protezione+dei+dati+personali+2022.pdf/4fa353a9-f26a-45a5-afce-e07de5f54622?version=1.3

Contact

European Centre on
Privacy & Cybersecurity

Minderbroedersberg 4-6
6211 LK Maastricht
The Netherlands

paolo.balboni@maastrichtuniversity.nl

© Maastricht University European Centre on Privacy & Cybersecurity 2022