ethos

Ethos Engagement Paper

Corporate digital responsibility

>20 YEARS | OF SOCIALLY RESPONSIBLE INVESTMENT

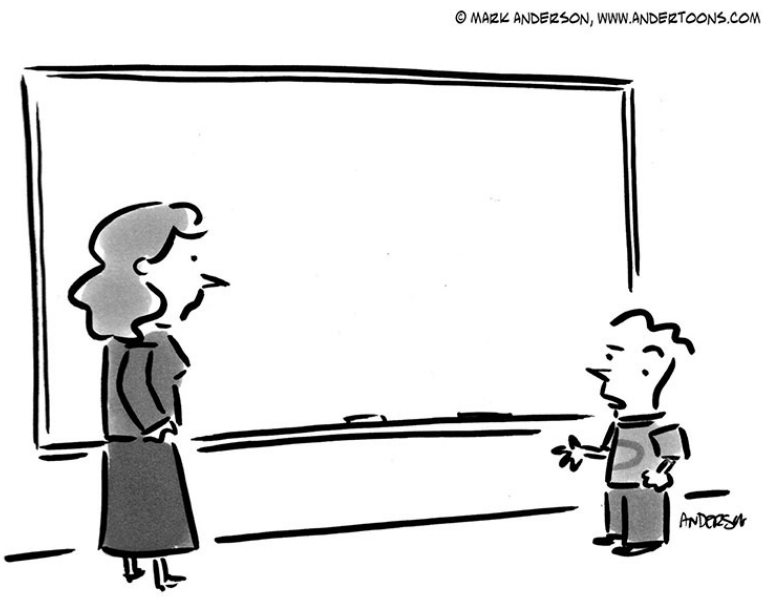
November 2020

The Ethos Foundation is composed of more than 220 tax-exempt Swiss pension funds and institutions. Founded in 1997, its aim is to promote socially responsible investment and to foster a stable and prosperous socio-economic environment.

Ethos Services SA provides management and advisory services in the field of socially responsible investments. Ethos Services offers socially responsible investment funds, analyses of shareholders' general meetings with voting recommendations, a programme of dialogue with companies as well as environmental, social and corporate governance ratings and analyses. Ethos Services is owned by the Ethos Foundation and several members of the Foundation.

www.ethosfund.ch

This engagement paper is predominantly based on the research conducted by Jean-Henry Morin (Université de Genève), Johan Rochel (Ethix Lab for Innovation Ethics) and Eva Thelisson (AI Transparency Institute). White paper, *Towards a Digital Responsibility Index*, to be published in December 2020.



"Before I write my name on the board, I'll need to know how you're planning to use that data."

Printed on "RecyStar", 100% recycled paper without optical brightener.

Table of content

1 Introduction

1.1 Background

Digitalisation is one of the three major societal challenges of the 21st century, alongside climate change and growing social inequalities. It offers considerable potential for economic development for companies and their shareholders, which is why the phenomenon is often referred to as the fourth industrial revolution. Above and beyond the productivity improvements of traditional industries, in 20 years, digitalisation has enabled the emergence of the technology giants commonly known in the United States as GAFAM (Google, Amazon, Facebook, Apple and Microsoft). At the end of September 2020, the cumulative market capitalisation of GAFAM companies reached nearly USD 6,000 billion and represented 14% of the MSCI World Index, while the 54 companies in the energy sector have a combined market capitalisation representing less than 3% of the same index.

This digital revolution is also bringing new challenges for companies and their shareholders. Numerous scandals, including the Cambridge Analytica case, have highlighted the abuses that can result from the exploitation of private data for commercial and political purposes. This implies new ethical, legal, financial and reputational risks.

In view of the impact of digitalisation on the economy and society in general, Ethos considers that this issue has become a major topic of responsible investment and environmental, social and governance (ESG) analysis. Companies in all sectors of activity must be proactive and implement digital responsibility policies. This concept requires companies to identify the challenges of digitalisation in a broad and comprehensive manner and to put in place management and transition policies that respect the interests of all their stakeholders.

1.2 Overview of Ethos' expectations

The Ethos Foundation aims to promote socially responsible investment and to foster a stable and prosperous socio-economic environment. As such, it attaches particular importance to business ethics and good governance issues.

Ethos thus advocates the implementation of a comprehensive corporate digital responsibility strategy that addresses all the issues listed in Chapter 2 of this document. Ethos' various expectations with regard to companies are laid out in detail in Chapter 3.

Ethos' principles on digital responsibility

1. Establish a digital responsibility code
2. Ensure transparency with stakeholders on digital practices and footprint
3. Comply with the highest standards of data processing and data protection
4. Establish ethical principles for the use of artificial intelligence (AI)
5. Exclude sensitive activities related to digitalisation
6. Ensure a fair and responsible social transition
7. Help reduce the environmental footprint of digital technology

2 Challenges of digitalisation

2.1 Digital governance

The definition of strategy and the identification of business risks must take digitalisation into account. This implies adapting corporate governance and ensuring regular monitoring by the Board of Directors of technological developments that may affect the company. This concerns the company's products and services as well as the modes of production, supply and distribution. Finally, it involves monitoring the relevance of the strategy by regularly integrating the risks and opportunities related to digitalisation.

In view of the "disruptive" nature and rapid evolution of technology, the Board of Directors must ensure that the company invests sufficient resources in this area, while complying with the highest ethical, environmental and social standards. Given the complexity of the issue, the Board of Directors must ensure that it has the necessary knowledge to understand these issues. It must also make certain that management handles the various issues and implements policies and procedures compliant with best practices.

2.2 Digital transparency

Companies must inform users and concerned parties of the personal data collection they carry out. This transparency is indispensable, yet by no means widespread. Users are not always aware of the storage and use of data concerning them. Businesses need to be forward-looking and transparent in order to create a trust-based relationship. Stored data should be obtained by free and informed consent ("opt in").

Companies must allow users of the various data-related services to easily consult and interact with (modify or delete) data collected concerning themselves. This user autonomy must be facilitated by companies to the maximum possible extent.

Certain data can be very valuable. It is therefore essential that the companies holding this data implement the highest security standards to prevent it from being marketed, leaked or stolen.

If, despite this, the data may have been used by an unauthorised third party, the companies must undertake to inform the holders of the data without delay. The latter must indeed be able to take steps to avoid being a victim of misuse of their personal data (fraud, ransoming, use of passwords, credit card passwords, profiling, etc.).

2.3 Data management and cybersecurity policy

Today, data has become an essential resource for many companies. While companies active in the technology and advertising sectors are the main ones concerned, they are by no means the only ones. Indeed, any company with data on its customers, employees, suppliers, shareholders or competitors is concerned by the use or even potential marketing of the data.

The importance of data for business and the economy creates a cybersecurity and regulatory challenge.

A. Data protection regulations

The misuse of private data has led some states to impose new rules on how data is stored, managed and used. In Europe, the "General Data Protection Regulation - GDPR[1]" came into force in 2018. This European law goes much further than most legislation around the world and recognises the sensitivity of the subject. Companies operating within the European Union (EU) or processing data from EU nationals must ensure that they comply with this legislation. Violation of the GDPR can lead to significant fines of up to EUR 20 million or 4% of overall turnover.

After more than three years of discussions, in September 2020 the Swiss Parliament approved a modernisation of the "Federal Act on Data

[1] http://gdpr-text.com/read/article-1/

Protection (FADP)[2]" with the aim of making it compatible with the GDPR regime. The Swiss law strengthens the framework for user protection and the information obligation of companies. Both texts agree on certain principles related to data collection. These concern lawfulness, good faith, proportionality, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, security and transparency, as well as accountability. However, the two laws diverge on several aspects, in particular with regard to sanctions. The FADP also sets financial penalties that are much lower than those foreseen in the European legislation. It is not clear at this stage whether the EU will accept the principle of equivalence of the two laws. Swiss companies therefore have a clear interest in complying with best practices and the highest regulatory standards and thus voluntarily aligning themselves with the GDPR.

California has also legislated in the area of data protection with the entry into force on January 1st 2020 of the California Consumer Privacy Act[3], which incorporates several key elements of the GDPR, including transparency obligations with respect to data collection, data theft, and the protection of private data.

B. Privacy Policy

The use of the data by companies makes it possible to offer personalised services to users or to make this data available to third parties for commercial purposes. The exploitation of private data has indeed enabled some companies to develop new business models and has notably revolutionised the service industry. This personalisation can be positive and beneficial to users, but it is often be carried out at the expense of data privacy. Targeted advertising is an example of the data usage often conducted in violation of the privacy of the company's stakeholders. In less than a decade, the private data available to Google and Facebook has enabled them to become the main advertising players, now sharing the bulk of the sector's revenue

Personalisation of services based on the use of private data should be a choice of the user and not the default option of the services ("privacy by default"). Devices and services using private data should be designed in such a way that they respect privacy and cannot automatically exploit the data ("privacy by design"). This concept is also a key element of the GDPR.

C. Data minimisation

The privacy by design principle requires that data processing systems should be designed to process as little personal data as possible (data minimisation). This principle of data minimisation entails applying privacy-friendly default settings, limiting access to personal information to what is strictly necessary to provide the service, as well as implementing tools enabling users to better protect their personal data (access controls, encryption, etc.).

D. Cybersecurity

Cybercrime is one of the major risks currently faced by organisations of all sizes and in all sectors. Cyberattacks can go so far as to jeopardise the very survival of certain companies and require the mobilisation of significant resources to ensure cybersecurity and system recovery plans.

Cybercrime can have several origins, ranging from malicious intent to espionage. The most frequent targets are organisations that may be of financial interest, such as banks for example, or organisations that collect and store large amounts of data. However, all businesses can be victims of embezzlement, data encryption for ransom, breaches of payment systems or destruction of key company databases and programmes.

The cybersecurity strategy of companies must also enable the swift provision of information to authorities and users in the event of a cyberattack compromising data security and confidentiality. The GDPR thus provides that any data leakage must be reported to the supervisory authority within 72 hours.

---

[2] https://www.parlament.ch/centers/eparl/curia/2017/20170059/Texte%20pour%20le%20vote%20final%203%20NS%20F.pdf

[3] http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

2.4 Algorithms and artificial intelligence

Artificial intelligence (AI) encompasses a set of theories and techniques to develop complex computer programs capable of simulating certain traits of human intelligence (reasoning, learning, natural language, movement, etc.). Today, AI is mainly based on very advanced machine learning technologies which aim to give computers the ability to "learn" from data, i.e. to improve their performance in solving tasks without being explicitly programmed for each of them. The method which currently yields the most results is "deep learning". This is a class of automatic learning algorithms using several hidden layers of artificial neural networks capable of extracting, analysing and classifying increasingly abstract characteristics from the data presented to them.

AI can provide high added value in the areas of health, productivity and the environment. In the medical field, for example, the high-tech brand of radiology was an early adopter of 'smart' technology, which for more than ten years now has made it possible to detect lung tumours using a computer algorithm. [4]

The rapid development of these technologies in recent years has been particularly facilitated by an explosion of the computing power of machines as well as growth in the amount of data available to feed the algorithms.

These simultaneous developments enable machines to surpass humans in certain areas, for example in the case of the board game Go. Beyond the performance of the computer, it is the fact that the programme – based on an artificial neural network – learned to play alone that is significant in the evolution of AI. The latter indeed develops autonomously from its "human" programming, which no longer allows its designer to explain its decision-making process. An inexplicable AI can therefore potentially take decisions that go against its programming or the general interest.

The potential impact of algorithms on our daily lives (self-driving cars, facial recognition, voice assistant, etc.) open up an important debate on the responsibility and ethics associated with these machines.

To date, there are no regulations governing the operation of AI and ensuring that these programmes, which have become autonomous and independent of human beings, do not violate ethical rules. However, certain ethical expectations around AI are beginning to emerge requiring to adopt four principles (transparency, impartiality, responsibility and positive impact).

A. Transparency

Civil society has high expectations of the transparency of AI systems. Today, companies are expected to be transparent about the programmes they use and how they are used. This may be the case in many areas, such as human resources, customer services, medical diagnosis, credit or insurance allocation or the selection of service providers. The potential use of such technologies should be transparent. In particular, it should be possible to know how and why a system has made a decision or acts in such a way (explainable AI).

B. Equality of treatment / impartiality

The functioning of AI systems is often opaque, particularly in the field of "deep learning". Decisions or recommendations made with the help of programmes using artificial intelligence can also come up against moral and ethical dilemmas. Traceability of the decision-making mechanism is therefore essential to ensure that decisions made by AI are free of ethnic, gender or other biases ("unbiased AI"). This neutrality must be the basis for the design of programmes that can lead to autonomous decision-making mechanisms. It depends not only on the code of the algorithm, but above all on the data that will feed the algorithms. Companies are therefore responsible for checking that AI results or predictions are not biased, in particular due to poor quality or unrepresentative basic data. If such neutrality cannot be guaranteed, then the commissioning of such software should not be possible.

C. Responsibility

The impartiality of AI is central but does not necessarily resolve all the moral dilemmas that

[4] https://medicalforum.ch/fr/article/doi/fms.2019.08035

artificial intelligence could face. It is therefore essential that human intervention remains possible at all times. In the event of a problem, the question of responsibility must also be clarified. Does the responsibility lie with the seller, the owner, the designer of the algorithm, or does it pass directly to the system?

The current ethical principles surrounding AI propose a framework within which a precondition for the development of AI is that it must be conducted in a responsible, safe and useful manner; that the machines retain the status of tools; and that legal or corporate entities retain control and responsibility for them at all times.

D. Positive impact

AI can be a central element in addressing some of today's challenges such as climate change, biodiversity loss, health or inequalities. Above all, AI should be developed with the aim of having a positive environmental and social impact.

2.5 Sensitive products and services

The rapid development of new technologies enables certain activities that Ethos considers incompatible with its Charter and the foundations of sustainable development. This notably concerns surveillance activities using facial recognition or aimed at restricting freedom of expression as well as the development or use of autonomous weapons, the promotion of sensitive or prohibited content, and even activities aimed at influencing behaviour in a hidden way.

A. Surveillance

New image analysis and processing technologies can help prevent the dissemination of violent and sensitive content on the Internet or detect attacks in public places. However, these systems can also be used to monitor citizens and, in the case of use by authoritarian regimes, undermine freedom of expression and human rights. Companies must therefore be vigilant about how their technologies and services are used by customers. They should define acceptable limits to ensure that their products and services will not directly or indirectly harm human rights.

B. Autonomous weapons

AI enables the development of new types of autonomous weapons that select and engage targets without human intervention. The stakes are high: autonomous weapons have been described as the third revolution in warfare, after gunpowder and nuclear weapons.

Unlike nuclear weapons, stand-alone weapons do not require expensive or hard-to-obtain raw materials, so they could quickly find their way onto the black market and into the hands of terrorists, dictators seeking to better control their populace, warlords wishing to perpetrate ethnic cleansing, etc. Being devoid of humanity, autonomous weapons would be ideal for tasks such as assassination or destabilizing nations, as well as subduing populations and even genocide[5].

Companies must ensure that their products, technologies or intellectual property do not contribute specifically, directly or indirectly, to the development of autonomous weapons.

2.6 Social impact

Technological developments have and will continue to have a major impact on employment and current societal patterns. As AI systems develop and new business models emerge, jobs or types of tasks will disappear or be significantly reorganised. The beneficiaries of this digital revolution could be companies and shareholders who will benefit from increased productivity. However, the gains for shareholders may be limited in the short term if the transition is not carried out in a responsible manner. In particular, the Swiss pension system could suffer if the number of working people falls drastically or if the development of the service economy ("gig economy") transforms employees into independent entrepreneurs ("uberisation").

To ensure a fair transition, it is essential to put in place corporate policies that ensure corporate responsibility for job losses and displacement, such as retraining programmes, continuing education and job change opportunities. In this respect, a technology monitoring enables adequate foresight with regard to technical

[5] https://futureoflife.org/open-letter-autonomous-weapons/

developments and the corresponding skills requirements. This monitoring would thus make it possible to ensure a responsible transition of skills.

AI systems, together with the wider transition to the digital economy, will require that workers at all levels and in all occupations have access to social security and lifelong learning to remain employable. It is the responsibility of States and businesses to find solutions that ensure that all workers, in all forms of work, have the right and access to both.

Moreover, in a world where the precariousness and individualisation of work is increasing, all workers, whatever their form of employment, must have equal and solid social and fundamental rights. All AI systems must provide a checks-and-balances system in order to ensure that their deployment and growth are consistent with workers' rights as defined in human rights provisions, International Labour Organization (ILO) conventions and collective bargaining agreements.

2.7 Environmental impact

The current digital revolution also involves important environmental issues at a time when our society must drastically reduce its CO_2 emissions to limit global warming. Nonetheless, the digital revolution is experiencing exponential growth of its carbon footprint and a steep increase in its environmental impact.

A study by GreenIT.fr[6] has estimated that in 2019, the digital universe will consist of 34 billion items of equipment (smartphones, televisions, computer screens and connected objects, etc.). Taking into account the entire life cycle of IT equipment, the contribution of the digital footprint to humanity's footprint is far from negligible. According to GreenIT.fr, these 34 billion items of IT equipment, the various networks (11 billion DSL/fibre boxes, 10 million 2G to 5G relay antennas and around 200 million other active WAN network equipment), together with the several thousand data centres (with more than 67 million servers hosted) contributed to humanity's ecological footprint in 2019 in the following way:

- 4.2% of primary energy consumption (6,800 TWh)
- 3.8% of greenhouse gas emissions (1,400 million tonnes of GHG)

The coronavirus crisis, which has led more than three billion people to remain confined to their homes and call upon IT services, has only increased this trend with an even greater explosion in data flows.

Given the unbridled growth in the use of connected objects, computer networks and a data-centric economy, the digital footprint will continue to grow exponentially in the coming years. Action is needed by businesses, consumers and governments.

[6] https://www.greenit.fr/wp-content/uploads/2019/10/2019-10-GREENIT-etude_EENM-rapport-accessible.VF_.pdf

3 Ethos' expectations

Ethos expects companies in which it is a shareholder or represents other institutional investors that they adopt the following 7 principles.

Ethos' principles on digital responsibility

1. Establish a digital responsibility code
2. Ensure transparency with stakeholders on digital practices and footprint
3. Comply with the highest standards of data processing and protection
4. Establish ethical principles for AI use
5. Exclude sensitive activities related to digitalisation
6. Ensure a fair and responsible social transition
7. Help reduce the environmental footprint of digital technology

Principle 1: Establish a public digital responsibility code

The Board of Directors must ensure that the company has a Digital Responsibility Code covering the main issues facing the company and weighing their materiality in relation to the sector of activity and the specific features of the company. The Board of Directors is responsible for covering all digital issues and verifying annually that the coverage is relevant. The code should cover at least the following issues:

- **Governance**: The way in which the company's digital issues are managed must be set out in the code. The Board of Directors must deal with the issue on a regular basis and ensure that its members understand the opportunities, risks and challenges of digitalisation. The executive management should appoint a dedicated Chief Digital Officer and be responsible for the implementation of the code and compliance with it.
- **Technology monitoring**: The code should set out how the board of directors and management of the company monitors technological developments relevant to the company's activities. This implies constant monitoring and taking account of developments in the definition of the company's strategy and risks.
- **Cybersecurity**: The code should include a section on how the company manages this risk. The cybersecurity strategy should be reviewed by the audit committee and management should appoint a "Chief Security Officer". Given the sensitivity of the subject matter, it is obvious that the details of the security policy must remain confidential. However, it is important for the company to confirm that security audits are carried out on a regular basis and that awareness is raised among all system users.
- **Privacy and data protection**: Companies must confirm in their code that they are committed to respecting the data protection and privacy of their stakeholders (see Principle 3 below).
- **Ethical rules for the use of artificial intelligence (AI)**: The code should provide a detailed section or reference to more specific principles on the rules for the use of AI (see Principle 4 below).
- **Social responsibility for the digital transition**: The impact of the digital transition on the company's employees should also be part of the code (see Principle 6 below).
- **Principle of reducing the digital environmental footprint**: Companies should stipulate in their digital responsibility code how the environmental impacts of digital goods and services as well as company data and networks are minimised (see Principle 7 below).

Principle 2: Ensure transparency with stakeholders

The implementation of the digital responsibility code should be verifiable by the company's stakeholders (customers, suppliers, shareholders, civil society, etc.). This requires full transparency through information that is easily accessible on the website and in the annual report, as well as being easily understandable, particularly with regard to the following points:

- The digital responsibility code should be **available on the internet** and in the languages of the countries in which the company operates.

- Users need to know what data is collected and be able to consult it. The storage locations of the data must also be communicated, as well as the way in which private data is encrypted.
- Data privacy rules must be **intelligible and easily accessible to** users.
- **The use of AI** in decision-making processes must be clearly communicated.
- An attack compromising data security must be **reported without delay.** Users whose data has been compromised must also be informed.

Principle 3: Comply with the highest standards of data processing and protection

Companies must apply the highest standards in this area to minimise legal and financial risks. In particular, companies should comply with the following points:

- The products and services of companies must be designed in such a way that the privacy of users can be respected at all times ("**privacy by design**") and always offer a privacy-friendly default mode ("**privacy by default**").
- The persons whose data is collected must expressly give their free and informed consent before their data is used ("**opt in**").
- Companies should not use private data for behavioural surveillance.
- No data should be collected and stored without a specific reason (purpose).
- Businesses must respect the principle of a strictly minimal collection and possession of data (proportionality). They should put in place technologies that enable them to ensure that this principle is respected (Privacy Enhancing Technologies or PETs) in their online services and websites.

Principle 4: Establish ethical principles for AI use

The use of AI requires the establishment of a code of ethics and deontology which should address the following principles:

- Companies that develop AI systems must ensure that they are developed with the aim of having a **positive impact on society and the planet**.
- Stand-alone technologies may reflect and reinforce certain biases or prejudices depending on the quality of the programming and data that feed the algorithms. **Companies must ensure equal treatment and non-discrimination of** the **AI** they develop and use. AI should not have unfair effects on individuals, particularly those related to sensitive characteristics such as race, ethnicity, gender, nationality, income, sexual orientation, ability and political or religious orientation ("unbiased AI").
- Companies must be able to **explain at any time how their AI systems work** and be able to trace the decision-making process (explainable AI).
- The use of an AI decision by the company should be subject to **human approval** and to a right of appeal ("human in the loop").
- Companies must ensure that it is possible to select a **manual mode** in the programmes at any time and that this mode has the upper **hand** over the standalone mode.
- Companies **should regularly test** the performance and quality of their AI systems.
- Companies must ensure that the development of AI is responsible, safe and useful, that **machines retain tool status and** that people maintain control and responsibility for them.

Principle 5: Exclude sensitive activities related to the digital transition

Companies must define which AI-related activities should be prohibited. Ethos is of the opinion that companies' risk management systems must take into account that such goods, services or programmes should not contribute to the development or operation of the following activities in particular:

- People tracking systems that infringe fundamental rights.
- Systems to limit or reduce freedom of expression.
- Systems designed to create addictions.
- Autonomous weapons.

- Systems serving to manipulate a market or influence the behaviour of a market or population in a covert way.
- Systems disseminating sensitive, racist, sexist or illegal content or allowing access to content and activities inappropriate for minors.

Principle 6: Ensure a fair and responsible social transition

To ensure a fair transition, it is essential to put in place policies that ensure corporate accountability for job displacements or job losses:

- Companies must provide for personal development and retraining programmes by offering continuing education systems, as well as opportunities for job change.
- Companies must provide AI systems that serve people and limit job cuts by distributing productivity gains equitably.
- In the case of the use of employee data or AI in human resources management, employees must be informed and have the right to demand transparency of the decisions and results of AI systems and the underlying algorithms. [7]
- The development of new business models through digital transformation and AI should not allow companies to evade their obligations to employees or be used to circumvent collective agreements or social security systems.
- Companies must conduct a technology monitoring activity to plan their skills needs and give priority to retraining and skills transitions.

Companies should devote part of the sustainability report to explaining their approaches to preserving employment (number of retraining programmes, number of hours of continuing training, number of jobs eliminated or replaced by systems, and measures to redistribute productivity gains).

Principle 7: Help reduce the environmental footprint of digital technology

The digital revolution is having a major environmental impact, particularly when you consider the footprint of connected products throughout their lifecycle and the explosion in the amount of data stored and consumed. The large-scale use of complex algorithms also implies ever-increasing computing power and, consequently, exponential energy consumption. Companies can all take action to reduce the environmental footprint of their digital solutions. These notably include:

- Increasing the life of the equipment and extending the legal guarantee period.
- Reducing the need for digital services through their eco-design.
- Promoting the reuse and recycling of digital products.
- Providing for the use of efficiently designed data storage centres powered by renewable energy.
- Raising customer awareness on how to use connected business products in a way that minimises their environmental footprint.
- Publishing relevant data in the sustainability report such as recycling, average life of connected products, energy consumed by IT. systems, amounts of data stored or other relevant environmental indicators to enable comparison and evolution over time.
- Regularly evaluating and taking account of the environmental impact when deciding whether to internalise or outsource IT services.

[7]Top 10 principles for Ethical artificial intelligence, UNI Global Union, Principle 1

Ethos
Place de Pont-Rouge 1
P.O. Box 1051
1211 Geneva 26
Switzerland

T + 41 (0) 22 716 15 55
F + 41 (0) 22 716 15 56

Zurich office
Bellerivestrasse 3
8008 Zurich
Switzerland

T + 41 (0) 44 421 41 11
F + 41 (0) 44 421 41 12

info@ethosfund.ch
www.ethosfund.ch