NTT DATA
Trusted Global Innovator

Trustworthy AI

A guide to support CDOs and CIOs
to attain an ethical and compliant AI

CONTENTS

Trustworthy AI
JANUARY 2023

INTRODUCTION

Organizations are betting on more responsible AI by supporting ethical principles and regulations

Artificial Intelligence (AI) has become the cornerstone of the Fourth Industrial Revolution as well as the driver of organizations' competitive strategy. We are all aware of the benefits derived from AI. However, the use of huge amounts of data, the automation of decisions that affects directly people, and the perception of AI as a Black box can create mistrust among citizens. That´s the reason why a growing number of institutions, entities, and organizations are seeking to regulate, and define a common threshold and standard guidelines for all developers and vendors of these state-of-the-art technologies.

This paradigm shift is generating much expectation and the first organizational movements towards the creation of a responsible and ethical AI. But, at the same time, it is posed as a challenge for CDOs and CIOs leading to many open fronts to tackle.

For that reason, high-level executives seek to leverage the most appropriate tools tailored to the needs of their companies, allowing them to be compliant with the new regulatory framework that revolves around AI, aligned with the principles for a reliable AI.

That is why NTT DATA launched in 2021 "Getting ready for trustworthy AI regulation", a guide to anticipate the regulatory framework introduced by the AI Act.

Now, we want to go one step further, supporting CDOs and CIOs to develop a trustworthy, responsible, ethical and compliant (T.R.E.C) AI in compliance with the threshold set forth by the entire AI framework.

Chapter 1

Unified efforts toward an ethical AI

PATHWAY TO GLOBAL ETHICAL AI POLICIES

How is ethical AI regulated around the world?

According to the lasts report published by the market research firm IDC projected that the global AI market will reach a size of over 1.5 trillion U.S. dollars by 2030 (*). For that, a global race is underway to develop a fully-fledged regulatory framework that safeguards the fundamental rights of citizens, while fostering thriving economic and social growth.

We support CDOs and CIOs to keep track of the emergence of Global AI Policies, and so, focus on those regulations that are shaping and leading the AI industry.

1 January 1, 2021

National AI Initiative Act

It is a bipartisan legislation (1) embedded across the entire Federal government to accelerate AI research and application for the Nation's economic prosperity and national security, ensure continued U.S. leadership in AI R&D, lead the world in the development and use of trustworthy AI in the public and private sectors, and prepare the present and future U.S. workforce for the integration of AI systems across all sectors of the economy and society.

2 March 1, 2022

Regulations on Algorithm Recommendations for Internet Information Services

China's AI algorithm Rec. (2) requires AI-powered recommendation services to be moral, ethical, fair, accountable, and transparent. On top of that, it requires businesses to provide explainable AI algorithms and be transparent about their purposes, such as for recommending products or services.

3 March 2019

Social Principles of Human-Centric AI

The Japanese Government has set the goal of leading the AI-Ready Society (3) worldwide. And for that, it starts with establishing a social framework based on the 7 Principles implemented across Japanese society, including national and local government. These principles are based on the philosophy of dignity, diversity, inclusion, and sustainability to achieve the realization of Society 5.0 driven by a Human-centric AI.

4 December 7, 2018

Coordinated Plan on Artificial Intelligence

It is a joint commitment among the European Commission and the Member States to accelerate, act and align the policies, strategies, and investments in AI technologies to drive economic and social recovery (4).

5 April 8, 2019

Ethics guidelines for trustworthy AI

The concept of trustworthiness of artificial intelligence is introduced for the first time, which relies on 3 components that must be satisfied throughout the system's lifecycle: 1) Lawful; 2) Ethical, and 3) Robust. Furthermore, the Guidelines put forward a set of 4 principles and 7 key requirements that AI systems should meet in order to be deemed trustworthy (5).

6 February 19, 2019

White paper on AI: A European approach to excellence and trust

Actions of different nature are described to ensure an ecosystem of excellence and trust aiming to promote Europe's innovation capacity in the AI sector, and to encourage development, but always under the adoption of ethical and reliable AI in all member states (6).

7 July 17, 2020

Assessment List for Trustworthy AI (ALTAI)

It is a practical tool that helps businesses and organizations to self-assess the trustworthiness of their AI systems under development, taking the principles stated in the Ethics guidelines for trustworthy AI as the central axis of the tool (7).

8 April 21, 2021

EU Artificial Intelligence Act Proposal

A common AI Regulatory Framework for all EU member states is set, establishing the basis of what is to be understood by an AI system, categorizing its use cases according to their level of risk, and establishing horizontal requirements for compliance, ensuring all along both safety and fundamental rights protection (8).

9 February 23, 2022

Data Act

It is a horizontal proposal regulation that harmonizes rules on fair access to and use of data, fostering basic rules for all sectors and ensuring fairness in the allocation of value from data among actors in the data economy, by clarifying who can create value from data and under which conditions (9).

THE INTERNATIONAL AI STRATEGIC LANDSCAPE

How are governments approaching the critical need for AI capabilities?

National governments all around the world recognize artificial intelligence capabilities as the lever that will lead the future's developments and global competitiveness.

For example, countries look forward to enhancing their medical, education, transportation, law and enforcement, and even technology itself by harnessing AI, while protecting equity, privacy, transparency, accountability, and compliance of technologies towards the citizens and environment.

To achieve these long-term objectives, states must disaggregate them by designing actionable plans and strategies (10) with attainable milestones to achieve results in the short term.

To this end, public administrations, private sector companies, academia, and citizens will be expected to collaborate and engage in the execution of these strategies.

Therefore, similar to what happens with global AI policies, CDOs and CIOs will have to keep an eye on national strategic plans and stay in the loop to foster society's higher-end goals.

USA
National Artificial Intelligence R&D Strategic Plan (11) is based on 8 pillars: 1) Make long-term investments in AI research. 2) Develop effective methods for human-AI collaboration. 3) Understand and address the ethical, legal, and societal implications of AI. 4) Ensure the safety and security of AI systems. 5) Develop shared public datasets and environments for AI training and testing. 6) Measure and evaluate AI technologies through standards and benchmarks. 7) Better understand the national AI R&D workforce needs. 8) Expand public-private partnerships to accelerate advances in AI.

CANADA
Pan-Canadian AI Strategy (15), the Government is investing in efforts to drive the adoption of AI across Canada's economy and society.

GERMANY
The National AI Strategy (12) sets out a framework for a holistic policy on the future development and application of AI in Germany to make Germany and Europe a leading center for AI and help safeguarding Germany's future competitiveness.

ITALY
AI STRATEGIC PROGRAMME (13): Strengthening skills and attracting talents to develop an AI ecosystem in Italy; increasing funding for advanced research in AI; and the adoption of AI and its applications both in public administrations and in the private sector.

JAPAN
AI STRATEGY (14), to specify the environment and measures conducive to effective future utilization of AI for the purposes of contributing to the solution of global issues through the realization of Society 5.0 and overcoming the issues facing Japanese society.

AI PORTUGAL 2030 - NATIONAL STRATEGY FOR AI (16) seeks to bolster economic development, R&D and innovation excellence, and people's progress using AI.

SPAIN
National AI Strategy (17) looks to generate an environment of trust regarding the development of inclusive and sustainable Artificial Intelligence (AI), placing citizens at its heart.

Look more into it on the next page

→

THOROUGH CASE

Look under the microscope of the Spanish National Artificial Intelligence Strategy (ENIA)

As an example of how international policies have been translated into a national strategy, in Spain, on December 2, 2020, the new National Artificial Intelligence Strategy (in Spanish, ENIA) (18) was unveiled as a result of an inter-ministerial commission coordinated between the Ministry of Economic Affairs and Digital Transformation and the Secretary of State for Digitalization and Artificial Intelligence of the Government of Spain. ENIA is aimed at 6 different strategic lines of action:

ENIA strategic lines of action

- **PROMOTE** scientific research, technological development, and innovation in AI.
- **FOSTER** digital capabilities, empower national talent, and attract global skills in the field of AI.
- **DEVELOP** data platforms and technological infrastructures in support of AI.
- **INCORPORATE** AI into value chains to transform the economic fabric.
- **ENHANCE** the use of AI in government administration and in national strategic missions.
- **ESTABLISH** an ethical and regulatory framework that reinforces the protection of individual and collective rights, in order to guarantee inclusion and social welfare.

Bringing the AI regulation forward through the Spanish Regulatory Sandbox Initiative

Artificial Intelligence has an enormous potential to transform society and lead growth. For that, AI is a priority for Spain and for Europe.

The regulatory sandbox (19) piloted and led by Spain aims to create the conditions for a smooth implementation of the present and future regulatory rules applying on the AI, such as the AI Act, both at a national & EU levels.

The Spanish sandbox will facilitate the testing of specific technical solutions and compliance procedures while at the same time supporting not only companies and SMEs to avoid uncertainty and unnecessary burdens, but also contributing to the fostering a human-centered, trustworthy, and inclusive AI.

The piloting process is expected to set up an operational framework for all interested organizations and create synergies with other national initiatives, as well as, strengthen the bonds with the rest of the EU state members.

Milestones

June, 2022
Presentation and kick-off

Setting-up

November, 2022
Open call to companies

Selection of solutions and three month pilot and development of deliverables

November, 2023
Publication of first results

How the does the regulatory sandbox pilot work?

During the 3 months pilot, two Spainish focus groups will test and evaluate high-risk AI systems, carrying out iterative work and procedures, that later on will be translated and influence the final guidelines delivered at the end of the process.

- **The first group** is a practical set up of the sandbox (legal framework, testing, technology set up). It is formed by the Secretary of State, the Spanish Data Protection Agency, and industry experts
- **The second group** will look at the outcomes of the practical team, and translate that into guidelines, practices and toolkits, leading to an enormous potential to transform society and lits growth.

On top of that, in order to guarantee synergies between these two groups, it will be put in place a Governance body to oversee interactive work.

This Regulatory sandbox follows two fundamental goals:

• **1 EU global success:** facilitate the development of AI and give confidencitizensizents that AI will respect rights.

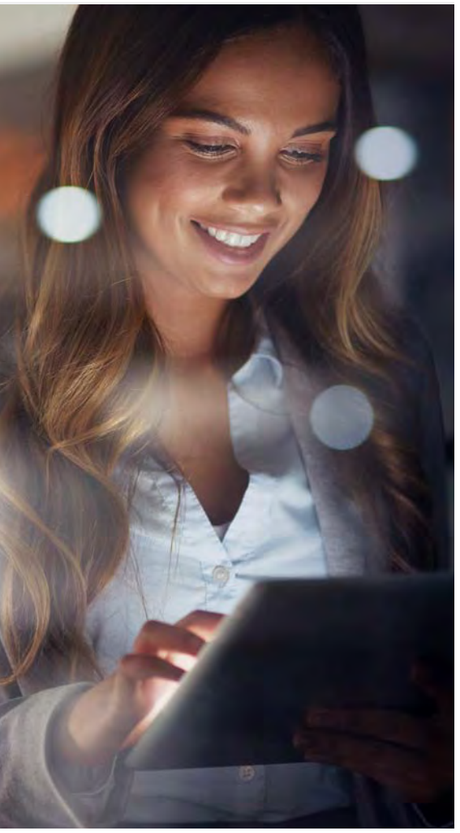
• **2 Aim to provide a safe environment** for AI providers and developers to comply with future regulations.

Chapter 2

Paramount publications

TWO MOST RELEVANT EU PUBLICATIONS FOR ORGANIZATIONS

2.1 ETHICS GUIDELINES FOR TRUSTWORTHY AI

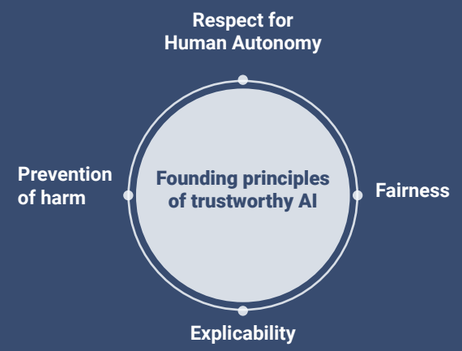


In 2019, the Independent High-Level Expert Group on Artificial Intelligence established by the European Commission published the Ethical Guidelines for Trustworthy AI (20), whose purpose is to promote trustworthy Artificial Intelligence at the European level.
In order to gain the trust of people in Europe, AI must rely on three components that must be satisfied throughout the system's lifecycle: respect all applicable laws and regulations (**lawful AI**), ensure its adherence to ethical principles and values (**ethical AI**) and be robust from both a technical and social point of view (**robust AI**), since AI systems, even if the intentions are good, can cause accidental harm.

Each of these components is in itself necessary but not sufficient for the achievement of trustworthy AI. Ideally, they should all act simultaneously with each other and in harmony with the rest of the regulatory framework.

The guideline applies in particular to AI systems that interact directly with users, and is aimed primarily at developers and deployers of AI systems. Given the application-specific nature of AI systems, it will be necessary to examine each specific use case and context in which these systems operate.

Therefore, these guidelines will outline a framework for achieving trusted AI and its key components by providing guidance at different levels along three fundamental axes.



01. Foundations

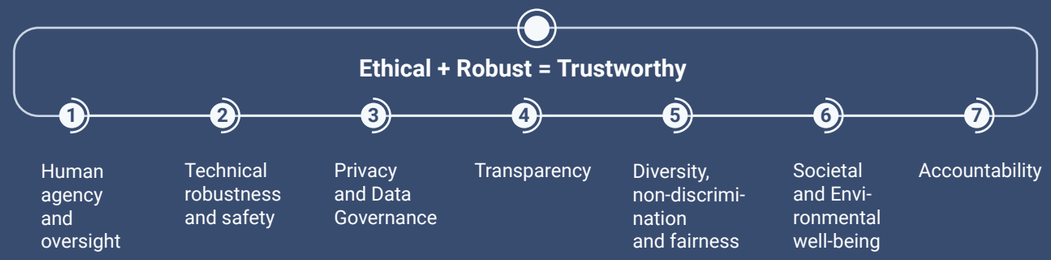
The first axis presents the foundations of an AI of trust, which is rooted in fundamental rights and reflected in the Four Ethical Principles:

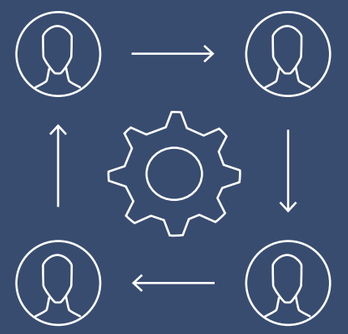
1. Respect for human autonomy
2. Prevention of harm
3. Fairness
4. Explicability

These principles pay special attention to vulnerable groups such as children and the elderly, as they have special needs that must be addressed.

02. Implementation and Achievement

The second axis focuses on the implementation and achievement of a trusted IA by establishing Seven Key Requirements that revolve around the 4 Ethical Principles.





03. Stakeholder Early Involvement

The Independent High Level Expert Group on Artificial Intelligence understands that, when introducing new procedures, the acceptance and validation of these procedures are higher if stakeholders are involved in them from their development.
These ethical principles will ensure a smooth implementation of AI in our society, ensuring that the benefits outweigh the potential risks.

THE PRINCIPLE OF RESPECT FOR HUMAN AUTONOMY

Self-determination, individuals' choices, and self-awareness have been protected over the years in ample international policies regarding human rights and freedoms.

Therefore, individuals who interact with AI systems must be guaranteed their **full and effective autonomy,** keep self-determination over themselves and be able to participate in the democratic process.

For that reason, it is no wonder why human autonomy has been acknowledged as one of the key principles for Artificial Intelligence designs and uses, as AI has the power to promote people's autonomy if designed properly.

That is why the distribution of functions between Human and Machine systems should follow **human-centric design principles**, and leave plenty of opportunities for individuals' choice.

In other words, it is understood that AI systems should not subordinate, coerce, deceive, manipulate, condition, or direct humans in an unjustified manner.

Instead, AI systems should be designed in ways that **augment, complement, and enhance** people's cognitive, social and cultural skills.

So that Augmenting the intelligence and perspective of people through the capabilities and recommendations of AI ("Augmented Intelligence") is necessary to address the requirement of human agency and oversight.

However, when creating autonomous learning algorithms systems that will impact human's decision-making processes, all come to a conundrum:

Is it possible for AI systems to respect or disrespect the autonomy of a person?

REQUIREMENT OF HUMAN AGENCY AND OVERSIGHT

AI systems should operate both as enablers of a democratic, prosperous and equitable society, supporting human action and promoting fundamental rights, as well as empowering human oversight.

FUNDAMENTAL RIGHTS

- AI can equally promote fundamental rights as well as jeopardize them.
- In situations where risks exist, an assessment of the impact on fundamental rights should be carried out.
- In addition, mechanisms should be put in place to allow external views on AI systems that may infringe on fundamental rights.

HUMAN AGENCY

- A decision based solely on automated processes should not be given when such a decision produces effects on users.
- Users should be able to make autonomous decisions regarding AI systems.
- They should be provided with the necessary knowledge and tools to understand AI systems and interact with them successfully.

HUMAN OVERSIGHT

- Human Oversight helps ensure that an AI system does not undermine human autonomy or cause other adverse effects.
- Oversight can be accomplished through governance mechanisms, such as human-in-the-loop (HITL), human-on-the-loop (HOTL), or human-in-command (HIC) methodologies.
- The lower the level of oversight, the more demanding the verifications and governance.

THE PRINCIPLE OF PREVENTION OF HARM

AI systems should not cause harm nor adversely injure human beings in any other way.

This entails the protection of human dignity, as well as physical and mental integrity. In this regard, vulnerable individuals should receive greater attention and be involved in the development and deployment of AI systems from the beginning of the AI lifecycle.

From the system perspective
All AI systems and environments must be secure. They should also be technically robust, and it should be ensured that they cannot be put to malicious uses.

So particular attention should also be paid to situations where AI systems may cause adverse effects (or aggravate existing ones) due to power or information asymmetries.

The Principle of prevention of harm encompasses the requirement of technical robustness and safety, which requires AI systems to be developed with a proactive approach to risks.

For that, the guidelines recommend a four-pronged approach: Resilience to attach; Fallback plan, Accuracy, Reliability and Reproducibility.

REQUIREMENT OF TECHNICAL ROBUSTNESS AND SAFETY

Technical robustness requires that IA systems are developed with a precautionary approach to risks, so that they always perform as expected and minimize unintended and unforeseen hazards and avoid causing unacceptable damage.

FALLBACK PLAN AND GENERAL SAFETY

- AI systems must have safeguards in place to allow for a fallback plan in the unlikely event of problems.
- There is a need to ensure that the system will perform as expected without causing harm to living beings or the environment. Therefore, processes for monitoring and evaluating the system should be established.

RESILIENCE TO ATTACK AND SECURITY

For AI systems to be considered safe, it is necessary to take into account:

- The potential unforeseen applications of AI.
- The potential abuse of an AI system by malicious actors.
- Take measures to prevent and mitigate these risks.

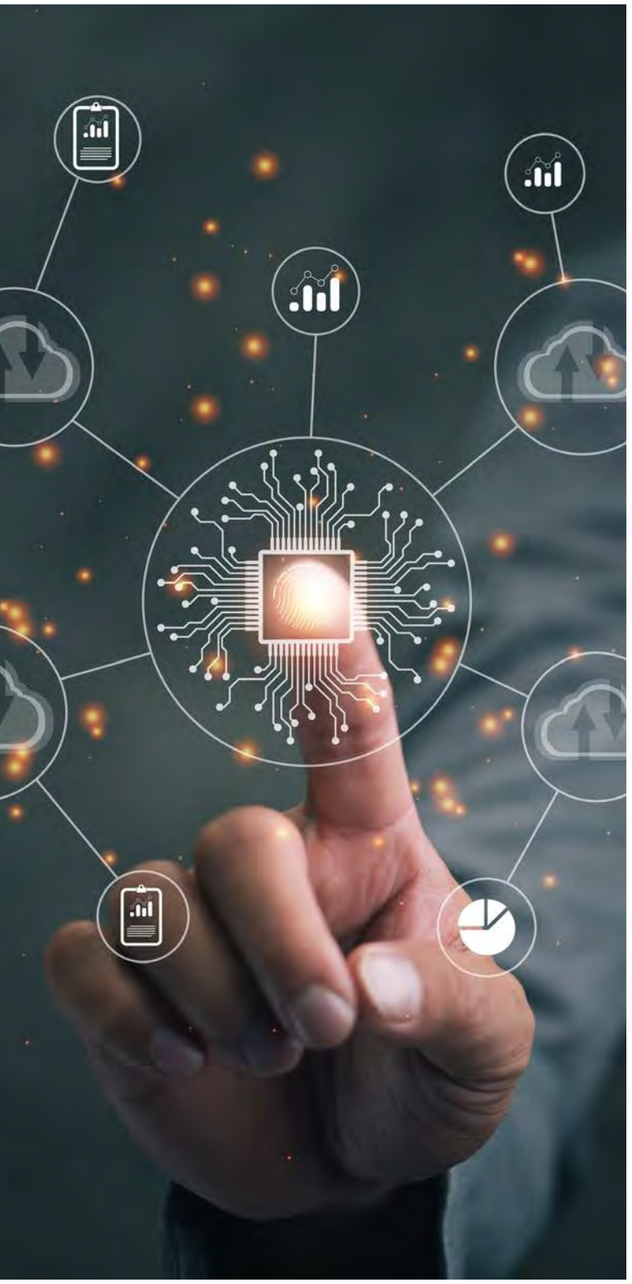
ACCURACY

- Accuracy is related to the ability of an AI system to make correct judgments.
- A properly designed development and evaluation process can support, mitigate and correct for unforeseen risks associated with incorrect predictions.
- Otherwise, the system must be able to indicate the likelihood of errors occurring.

RELIABILITY AND REPRODUCIBILITY

- A reliable AI system is one that performs adequately with a set of information and in a variety of situations. .
- Reproducibility describes whether an AI experiment shows the same behavior when repeated several times under the same conditions.
- This makes it possible to describe exactly what AI systems do.

THE PRINCIPLE OF FAIRNESS



The development, deployment, and use of AI systems must pursue a fair approach, both from the substantive and procedural dimensions.

The procedural dimension of equity entails the ability to oppose decisions made by AI systems and to explain decision-making processes.

While the substantive dimension involves a commitment to ensuring fair distribution and that individuals and groups do not suffer unfair bias, discrimination, or stigmatization. Furthermore, the use of AI systems should never lead to misleading (end) users or limit their freedom of choice.

In order to achieve the objectives set by the principle of equity, it is structured in two requirements for a better fulfillment:

The requirement of diversity, non-discrimination and fairness and the requirement of Societal and environmental well-being.

On the one hand, diversity, non-discrimination and fairness seeks to ensure inclusion and diversity throughout the AI systems lifecycle.

On the other hand, societal and environmental well-being promotes AI systems that seek sustainability and ecological responsibility and encourage research into solutions that respond to the Sustainable Development Goals.

As AI systems become more sophisticated fairness becomes more critical so that vías and discrimination are avoided in the decision-making process.

1. REQUIREMENT OF DIVERSITY, NON-DISCRIMINATION, AND FAIRNESS

Inclusion and diversity throughout the entire lifecycle of AI systems must be guaranteed and maintained. In addition to ensuring the participation of individuals across the entire process, it is also necessary to grant equal access by inclusive design processes.

AVOIDANCE OF UNFAIR BIAS

- Data sets used by AI systems may have unforeseen historical biases, gaps, or incorrect management models.
- This can be combated through monitoring processes that allow the system's purpose, constraints, requirements and decisions to be analyzed and addressed in a transparent and straightforward manner.

STAKEHOLDER PARTICIPATION

- In order to develop reliable AI systems, it is advisable to consult with stakeholders who may be affected by the system
- Regular feedback should be sought even after the deployment of AI systems.
- And so, it is paramount to establish mechanisms for long-term stakeholder involvement.

ACCESSIBILITY AND UNIVERSAL DESIGN

- Systems should be user-centered and designed in a way that enables all people to use AI products or services regardless of their age, gender, abilities or characteristics.
- Moreover, AI systems should be adaptive and take into account Universal Design principles to serve as many users as possible.

2. REQUIREMENT OF SOCIETAL AND ENVIRONMENTAL WELL-BEING

It should be taken into account as stakeholders throughout the entire lifecycle of AI society as a whole, other living beings, and the environment, promoting the sustainability and ecological responsibility of AI systems and encouraging research into solutions that respond to the United Nations Sustainable Development Goals (SDG).

SUSTAINABLE AND ENVIRONMENTALLY FRIENDLY AI.

- AI systems must seek to address societal problems by ensuring that they do so in the most environmentally friendly way possible.
- Measures should be promoted to ensure that all links in the supply chain regarding AI technologies are respectful of the environment.

SOCIAL IMPACT

- Although AI systems can be used to improve social skills, they can also contribute to their deterioration.
- This can affect the physical and mental well-being of individuals.
- Therefore, the effects of such systems will need to be taken into account and closely monitored.

SOCIETY AND DEMOCRACY

- The impact should also be assessed from a societal perspective, taking into account its effects on institutions, democracy and society as a whole.
- The use of AI systems should be studied especially in situations related to the democratic process, such as in electoral contexts.

THE PRINCIPLE OF EXPLICABILITY

Explainability (XAI) is crucial to get users to trust AI systems and to preserve that trust. This implies attaining transparency throughout the AI processes, carrying out an open communication of the capabilities and purpose of AI systems, and providing an explanation of the algorithms' decision-making process.

However, it is not always possible to explain why a model has generated a result. Such cases are called "black box" algorithms. So, it is necessary to take other measures related to explainability, such as traceability, auditability or transparent communication of system performance.

Thus, the level of need for explainability depends to a large extent on the context and the seriousness of an erroneous or inadequate result attained by an AI system.

In order to achieve high levels of explainability, three requirements must be addressed:

- **Privacy and Data** Governance protection must be ensured by covering everything from proper data management to access protocols and the ability to process data without violating privacy.
- **Transparency:** The data, system, and models of AI systems must be transparent and explainable to stakeholders.
- **Accountability:** mechanisms must be established to ensure responsibility and accountability for AI systems and their results.

Explainable AI (XAI) is essential to completely remove the concept of the "black box" and create an ecosystem of trust that fosters the Human-Machine Collaboration Model.

1. REQUIREMENT OF PRIVACY AND DATA GOVERNANCE

Privacy is a fundamental right that is particularly vulnerable when it comes to AI systems. Therefore, privacy and data protection must be guaranteed throughout the entire life cycle, from proper data management to access protocols and the ability to process data without violating privacy.

PRIVACY AND DATA

- AI systems must ensure privacy and data protection throughout the lifecycle of a system.
- To enable individuals to have confidence in the data collection process, it is required to ensure that the information collected about them won't be used to unfairly or unlawfully discriminate against them.

QUALITY AND INTEGRITY

- The quality of the data sets used is paramount to the performance of AI systems.
- The introduction of malicious data into an AI system can alter its behavior, especially if it is a self-learning system.
- The processes and data sets used must be tested and documented at every step.

ACCESS TO DATA

- In any organization that handles personal data, protocols governing access to the data should be established.
- These protocols should describe who can access the data and under what circumstances.
- Thus, only appropriately qualified personnel should be allowed access to personal data.

2. REQUIREMENT OF TRANSPARENCY

The data, system and models of AI systems must be transparent and explainable to stakeholders, in other words, humans must be informed when interacting with an AI system and be aware of its capabilities and limitations.

TRACEABILITY

- The data sets and processes that result in the AI system's decision, including those related to data collection and labeling as well as the algorithms used, should be documented in order to enable traceability and increase transparency.
- This will make it possible to identify the reasons for an erroneous decision by the system, which in turn could help prevent future errors.

EXPLAINABILITY

- Technical explainability concerns the ability to explain both the technical processes of an AI system and the associated human decisions.
- Such explanation should be adequate and adapted to the level of expertise of the stakeholder.
- In addition, it should be possible to have explanations of the extent to which the AI system conditions the decision-making process.

COMMUNICATION

- People have the right to know that they are interacting with an AI system.
- In addition, when necessary, the user should be offered the choice of whether he or she prefers to interact with an AI system or with another person.
- Information about the capabilities and limitations of the AI system should be provided to practitioners or end users.

3. REQUIREMENT OF ACCOUNTABILITY

This requirement calls for the establishment of mechanisms to ensure responsibility and accountability for the IA systems and their results, both before and after implementation.

AUDITABILITY

- Auditability is the ability to evaluate algorithms, data, and design processes.
- Evaluation by internal and external auditors, and even independent auditors, as well as the availability of corresponding evaluation reports can contribute to the reliability of AI.

MINIMISATION AND REPORTING OF NEGATIVE IMPACTS.

- Both the ability to report on the actions or decisions of the systems must be ensured.
- Proper identification, assessment, reporting and minimization of potential negative effects of IA systems is essential.

TRADE-OFFS

- When applying ethical requirements, tensions may arise and a balance must be struck.
- Therefore, the balance must be made explicit and assessed in terms of the risk to ethical principles, including fundamental rights.

REDRESS

- When unfair adverse effects occur, accessible mechanisms should be provided to ensure adequate compensation.
- In addition, a system of reparations for the IA system is crucial to ensure the confidence of the most vulnerable individuals and groups.

TWO MOST RELEVANT EU PUBLICATIONS FOR ORGANIZATIONS

2.2 THE AI ACT PROPOSAL

The second most relevant publication to regulate AI from an ethical and legal point of view is known as THE AI ACT, which was released on April 21.

The AI Act (21) is presented as a proposed regulatory framework that seeks to regulate - rather than the technology itself - the uses of AI in terms of its risks and dangers, pursuing at all times a more trustworthy AI.

The provisions of The AI Act apply to anyone who wants to develop, distribute and import AI systems into the EU market or who has an impact on users located in the European territory.

So, let's take as an example the big tech giants such as Google, Facebook or Amazon, which, despite being American companies, will be required to comply with this regulation, since their services are also performed within the EU Member States and affect users within the territory.

MAIN NOVELTIES INTRODUCED BY THE AI ACT

01 A common definition of Artificial Intelligence is introduced for the first time ever to all stakeholders. The definition is based on 3 pillars:

- **Legally robust & reliable**
- **Technological neutral**
- **Future proof & adaptive**

02 **The classification** of the AI use cases according to their level of risk is the central axis of this new regulation, since upon this paramount 4level classification, the Act will establish horizontal proportional risk-based approach requirements that will ensure the development of trustworthy AI systems.

03 **The concept of a voluntary Code of Conduct**, drawn up by the companies and suppliers that design or develop low-risk systems and wish to apply the mandatory requirements voluntarily.

"An AI system means a software that is developed with one or more of the techniques and approaches and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with "

AI SYSTEMS RISK CLASSIFICATION

UNNACCEPTABLE-RISK AI SYSTEMS

In this category, it has been identified AI use cases that will be banned, because they **CONTRAVENE EU VALUES** and violate fundamental rights state in the Charter Of Fundamental Rights Of The European Union.

PROHIBITED USES CASES

- Systems for assessing or classifying natural persons done by public authorities
- Systems that exploits any vulnerabilities of specific vulnerable groups, causing them psychological or physical harm.
- Systems that manipulate persons beyond their consciousness through subliminal techniques, distorting their behaviour and causing them psychological or physical harm.
- Use of real time remote biometric identification systems in publicly accessible spaces for law enforcement purposes.

PROPORTIONALITY REQUIREMENTS

Non-compliance with the prohibition of the AI practices will be subject to administrative fines, whichever is higher, of:

1. Up to 30 000 000 EUR
2. Up to 6 % of the annual turnover for the financial year, providing the offender is company

For deciding the amount of the administrative fine, the competent national courts and authorities of the Member States must take into account all relevant circumstances of each case:

- The nature, gravity and duration of the infringement
- Whether administrative fines have been already applied before
- The size and market share of the operator committing the infringement

HIGH-RISK AI SYSTEM

High-risk AI systems used as a safety component of a product or a stand-alone product, that **CREATE AN ADVERSE IMPACT ON PEOPLE'S** safety. However, they are permitted on the European market if they comply with specific mandatory requirements and an ex-ante conformity assessment.

The classification of an AI system as high-risk is **use case oriented** based on the following 8 domains:

USE CASE DOMAINS:

- Biometric identification and categorization of natural persons
- Management and operation of critical infrastructure
- Education and vocational training
- Employment, workers management and access to self-employment
- Access to and enjoyment of essential private services and public services and benefits
- Law enforcement
- Migration, asylum and border control management
- Administration of justice and democratic processes

PROPORTIONALITY REQUIREMENTS

STEP 1

Comply with technical & documentation requirements

- Risk Management Methodology
- Data and Data governance
- Technical Documentation
- Record-keeping
- Transparency & Provision of Information to Users
- Human Oversight
- Accuracy, Robustness & Cybersecurity

STEP 2

Follow an ex-ante Conformity assessment verifying compliance with documentation

STEP 3

Registration of stand-alone AI systems in the EU database

STEP 4

Place the HRAIS on the market or put it into service

AI SYSTEMS RISK CLASSIFICATION

LIMITED-RISK AI SYSTEM

USE CASE EXAMPLES	LIMITED RISK AI SYSTEM DEFINITION
Chatbots	AI systems that interact with humans
Biometric Social Categorisation	AI systems that are used to detect emotions or characteristics through automated means
Emotion Recognition Systems	AI systems that determine association with social categories based on biometric data.
Deepfakes	AI system that are used to generate or manipulate image, audio or video content that appreciably resembles existing persons, places or events and would falsely appear to a person to be authentic.

PROPORTIONALITY REQUIREMENTS

In order to place the limited risk AI system in the market or put it into service, it is required to comply with the **MINIMUM TRANSPARENCY OBLIGATIONS:**

Chatbots	Natural persons must be informed when they are interacting with an AI system, unless this is obvious.
Biometric Social Categorisation & Emotion Recognition Systems	Natural persons must be informed of the operations made by an emotion recognition system or a biometric categorization system when they are exposed.
Deepfakes	Natural persons must be disclosed the image, audio or video content, that has been artificially generated or manipulated by an AI system.

LOW-RISK AI SYSTEM

The rest of the AI systems are framed in the category of "**NON-HIGH-RISK AI SYSTEMS**" which presents only minimal or no risk for citizens' rights or safety.
Thus, non-high-risk AI systems are not attached to the mandatory restrictions presented in The AI Act.

However, companies are highly recommended to implement a **VOLUNTARY CODE OF CONDUCT** to apply voluntarily the mandatory requirements for high-risk AI systems.

PROPORTIONALITY REQUIREMENTS

Providers of non-high-risk AI systems are encouraged to create **codes of conduct** to foster the voluntary application of the HRAIS' mandatory requirements

Voluntary Technical Requirements

- Risk Management
- High Quality Data
- Documentation and Traceability
- Transparency
- Human Oversight
- Accuracy and Robustness

Other Voluntary Commitments

- Environmental sustainability
- Accessibility for persons with disability
- Stakeholders' participation in the design and development of AI systems
- Diversity of development teams

TODAY'S CDOS & CIOS CHALLENGES

The AI Act identifies eight different mandatory provisions to design and develop trustworthy High-Risk AI systems, that designers and developers of high-risk AI systems must look them up in order to be compliant with the future regulation.

- **Risk Management** — Art. 9
- **Data and Data Governance** — Art. 10
- **Record-keeping** — Art. 12
- **Transparency and Provision of Information to Users** — Art. 13
- **Human Oversight** — Art. 14
- **Accuracy, Robustness and Cybersecurity** — Art. 15
- **Technical Documentation** — Art. 11
- **Conformity Assessment** — Art. 19

TODAY'S CDOS & CIOS CHALLENGES

RISK MANAGEMENT SYSTEM

What does this provision consist of?

Perils arising across the AI lifecycle may have considerable consequences on business areas, IT, customers and potentially affect organizations' reputation.

In order to develop a trustworthy AI system free of errors and hazards, the regulation pays special attention to the proper management of risks and biases throughout the entire AI system's lifecycle, from the birth of the AI-driven initiative until the monitoring phase.

Thus, the model's risk management system should be defined from a strategic positioning since it would be the backbone of the mechanisms to be implemented along the AI lifecycle.

OBJECTIVES IT PURSUES

- **Boost the general understanding and acknowledgement** of risks and biased that can infringe upon the AI system.
- **Save future costs**, by deploying early control mechanisms, allowing an early detection and evaluation of the potential perils.
- **Support AI systems to remain efficient and risk-free**, by mitigating, eliminating and protecting it against biases along the entire lifecycle of HRAIS.

Regulation guidelines

1. **Definition**
   Identification of the known and foreseeable risks.
   Analysis and evaluation of the risks.
   Testing the AI system to identify the better risk management measures.
2. **Implementation**
   Select and implement the most appropiate measures.
3. **Ongoing assessment**
   Evaluation of other possibly arising risks based on the post-market monitoring system .

TODAY'S CDOS & CIOS CHALLENGES

DATA AND DATA GOVERNANCE

What does this provision consist of?

Over the years, it has been demonstrated that many AI systems end up being biased and discriminatory against the most vulnerable groups. The current AI Act disposition concerns that some AI systems are poised to expedite and ultimately exasperate these issues.

This provision defines the elements and characteristics to be considered for achieving high-quality data when creating the model's training and testing sets. It, as wel demands organizations to deploy a responsible data governance that oversees the end-to-end data lifecycle.

OBJECTIVES IT PURSUES

- **Build resilient AI models and reliable solutions, from risk-free, inclusive, and trustworthy data sets that** integrate inclusive data, respect data privacy, and avoid unrepresentative customer data beyond its intended and stated use.
- **Create a common threshold for data quality criteria** scalable across the entire organization, so each expert knows which criteria to comply with, avoiding quality disparities among AI models.

Regulation guidelines

DATA QUALITY CRITERIA

Relevant	Suitable	Inclusive	Compilant
Relevant, representative, free of errors and complete data.	Integrate appropriate statistical properties regarding the individuals on which the HRAIS is intended to be used.	Include the specific geographical, behavioral or functional characteristics or elements within which the HRAIS is intended to be used.	Comply with the rest of the EU laws (such as GDPR) to appropriate safeguard the individuals' fundamental rights and freedoms.

TODAY'S CDOS & CIOS CHALLENGES

RECORD KEEPING

What does this provision consist of?

It is paramount that in the design and development stages of High-risk AI systems, organizations include capabilities for enabling the automatic recording of events and activities ('logs') while the AI system is operating.

Regulation Guidelines

1. **Record keeping capabilities** must be included since the design / development of the HRAIS, in order to:
   - **Level up** traceability functioning of the AI system's
   - **Monitor all occurrence of situations**, risks, and events that may result in any substantial modifications
   - **Facilitate post-market monitoring**
2. Logs have to present **recognizable minimun standards** and minimun common specifications, such as:
   - **Recording of the period**
   - **Reference database**
   - **Input data**
   - **Identification of the natural persons involved in the verification of the results**

OBJECTIVES IT PURSUES

- **Smooth** the recording and monitoring processes for all the events and occurrences of risks and pitfalls generated by the model throughout its lifecycle.
- **Perform** a better traceability of the AI system's functioning throughout its entire lifecycle according to its intended purpose.
- **Support** the model maintenance.
- **Facilitate** both internal and external audit trails for AI systems.
- **Ease** the post-market monitoring and documentation process to **evaluate the continuous compliance of AI systems.**
- **Save both time and resources**, by creating actionable notifications that alert experts about the modeling disfunction before it happens.

TODAY'S CDOS & CIOS CHALLENGES

TRANSPARENCY AND PROVISIONS OF INFORMATION TO USERS

What does this provision consist of?

To avoid explanatory and interpretable model problems, the transparency obligation provides information needed about the model's processing, both the origin of the data, the algorithm properties, limitations and performance.

Furthermore, the disposition looks to attain higher transparency levels by attaching complete instructions or manuals of use with all the relevant information to ensure the appropriate usage of the AI system.

Regulation Guidelines

The AI system's instructions must include the following:

- **Identity and the contact details of the provider**
- **Characteristics, capabilities and limitations of performance**
- **Description of the changes & performance**
- **Description of the human oversight measures**
- **Expected lifetime of the system**
- **Description of maintenance measures to ensure the proper functioning**

OBJECTIVES IT PURSUES

- **Avoid** loopholes or black boxes, which result in hazards, damages or harms to the stakeholder who are in interaction with such model.
- **Make** IA model more accessible, understandable and explainable for both developers and users to interpret the system's output.
- **Enhance** model's security, by setting a common knowledge background about what it is and how it works.

TODAY'S CDOS & CIOS CHALLENGES

HUMAN OVERSIGHT

What does this provision consist of?

With the advances in technology, AI systems' decision-making processes are becoming increasingly autonomous, leading little to no human intervention required along its operating lifetime.

However, the regulation urges to keep humans in the loop, not as an alternative, but as a necessity to oversee the system's operations, verify its outcomes, and intervene, when necessary, through appropriate human-machine interface tools.

Regulation Guidelines

As a result, human oversight measure should help individuals to:

- Fully understand the capacities, limitations and risks of the high-risk AI system.
- Correctly interpret the high-risk AI system's output.
- Decide not to use the system.
- Interrupt the system through a "stop" button.

OBJECTIVES IT PURSUES

- **Better support** AI systems' design, development and operations.
- **Avoid causing harm** to the health, safety or fundamental rights of people, as well as **minimize the potential risks** throughout its entire lifecycle.
- **Gain maturity in the overall AI Teams structure**, as the organization has clearly identified all stakeholders' roles and responsibilities and assigned adequate human-machine interface tools, when each agent intervenes in the models' process.
- **Quickly identify accountable responsables** when the AI systems provoques vulnerabilities against any stakeholder.

TODAY'S CDOS & CIOS CHALLENGES

ACCURACY, ROBUSTNESS AND CYBERSECURITY

What does this provision consist of?

As vulnerabilities are becoming stronger and ruthless, organizations and providers of high-risk AI systems need to establish a homogeneous compliance threshold that prevents the model from outside threats by defining a set of measures and KPIs regarding accuracy, robustness and cybersecurity.

Regulation Guidelines

- High-risk AI systems shall be designed and developed in such a way that they perform consistently in those respects throughout their lifecycle.
- The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.
- Shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates.
- Shall be resilient as regards attempts by unauthorised third parties to alter their use or performance.

OBJECTIVES IT PURSUES

The provision looks to achieve building resilient AI models that are protected against risks, inconsistencies and external vulnerabilities when running operations, in order to:

- Avoid future bias & risks.
- Protect the model against external vulnerabilities.
- Save monetary costs and other expenses associated to the loss of information and access breached .
- Boost the AI lifecycle management (MLOps).
- Scale AI across production environments.

TODAY'S CDOS & CIOS CHALLENGES

TECHNICAL DOCUMENTATION

What does this provision consist of?

To demonstrate high-risk AI system compliance with the mandatory provisions, the Regulation proposes to document the technical processes involved throughout the end-to-end AI systems lifecycle.

This documental information is required for all HRAI models in production, under development or decommissioned, and must fulfill specific requirements across five domains within a centralized Model Registry.

Regulation Guidelines

According to this requirement, the technical documentation must be drawn up before the AI system or component is commercialized or put into service.

Technical documentation should cover a number of specific categories providing the necessary information to assess the compliance of the AI Act and provide national competent authorities and notified bodies with all this necessary information to assess the compliance of the AI system with the requirements.

OBJECTIVES IT PURSUES

Organizations must place the technical documentation as a compass when designing and developing High-risk AI systems, supporting them to:

- **Remain** compliant with the mandatory requirements
- **Ensure** a homogeneous methodology for the proper documentation of all AI systems across the organization
- **Facilitate** traceability, monitoring & auditability
- **Achieve** a better market positioning
- **Enhance** the organization's reputation
- **Avoid** regulatory constrains and legal claims and suits
- **Increase** AI solution's time-to-market

MODEL REGISTRY – DOCUMENTATION CATEGORIES

BASIC INFO	Model Status Model Type Product Related Model Approval Date	Model Use Scope Data Sources Model Risk Rating Model Version
STAKEHOLDERS	Model Owner Model Developer Model Approver	Model User Model Maintenance
MODEL METHODOLOGY	Model Parameters Model Configuration Feature Pipeline	Training Dataset Validation Dataset
MODEL QUALITY	Model Validation Reports Model Dependencies Model Infrastructure	Model Impact Assessment Data Quality Reports
MONITORING	Performance KPIs Functional KPIs Alerts Defined	Model Issues Log Model Adjustment Logs

TODAY'S CDOS & CIOS CHALLENGES

CONFORMITY ASSESSMENT

What does this provision consist of?

Organizations and providers of high- risk AI systems must verify that their AI systems successfully meet all provisions and standards, not only prior to putting it into service, but also after being distributed in the marketplace.

Thus, the Conformity Assessment is a written verification process of compliance that agrees and ensures with all the following:

Regulation Guidelines

1. Comply with the harmonized standards published in Official Journal of the EU & comply with the technical documentation requirements
2. Compliance verification with the quality management system
3. Compliance verification with the post-market monitoring system
4. Draw up an EU declaration of conformity
5. Affix the CE marking of conformity

OBJECTIVES IT PURSUES

The conformity procedure relies on running automatic periodic verifications to examine the quality management system, as well as, the information contained in the technical documentation, smoothing the post-market monitoring processes.

Also, developing an internal audit procedure translates into higher transparency and consistency in the internal verification methodology.

In other words, aligning all AI Act's requirements to achieve a true conformity, leveraging internal control mechanisms, ensures ongoing compliance with the regulation and trustworthy AI systems.

Chapter 3

Guide to Start AI AUDIT TOOL

AI AUDIT TOOL

Ensure a trustworthy and compliant AI

At NTT DATA, we are aware of the dilemma CDOs and CIOs face in overcoming the challenges, especially when adapting the AI systems' design and development processes to each of the new regulatory provisions when attaining trustworthy and compliant AI systems.

Approaching all the AI policies' provision can be overwhelming, as each one of them presents different complexities and require unique approaches to comply with them successfully.

For that reason, as the first step, we support CDOs and CIOs anticipating their needs to address the upcoming EU AI regulation by building an AI Act Audit Tool that assesses the existing gaps in meeting each requirement.

In other words, this is a key asset that oversees the degree of compliance maturity of their AI models with the new European AI Act regulation, aligned with the Guidelines for a Trustworthy AI.

"We look forward to supporting the CDOs and CIOs of the organizations to start ahead by leveraging our AI Audit Tool to comply with the regulation successfully"

AI Act Audit Tool

This tool is mainly aimed at managers and executives, who:

- Have to audit AI-based solutions
- Seek to offer guarantees on their AI products and solutions
- Want to comply with the regulatory framework
- Foster the organization's efforts and synergies toward a trustworthy AI
- Gain global positioning and recognition in the market as a developer of ethical and compliant AI
- Look to unlock the value of AI for societies to excel

Although the mandatory requirements are only applicable to High-Risk Artificial Intelligence Systems (HRAIS), NTT DATA's Audit Tool can be useful for all AI models as a best practice guide, especially when adapting the AI systems' design and development processes to each of the new regulatory provisions when attaining trustworthy AI systems.

At NTT DATA, we support CDOs and CIOs anticipating their needs to comply with the upcoming EU AI regulation by building an AI Act Audit Tool to assess the existing gaps in meeting each requirement.

AI AUDIT TOOL

How does it work?

01 The AI Audit Tool is a comprehensive instrument that supports non-legal experts **to grasp the knowledge and understand the complex provisions** of the AI Act and the regulatory context it is embedded within.

02 Moreover, by leveraging the AI Audit tool, CDOs and CIOs will be able to **classify their AI developments according to the four levels of risk** linked to the safety and protection of a person's fundamental rights.

03 Additionally, NTT DATA experts will conduct a **thorough evaluation that assesses the level of compliance** with each one of the provisions (Risk Management; Data and Data Governance; Record-keeping; Transparency and Provision of Information to Users; Human Oversight; Accuracy, Robustness and Cybersecurity; Technical Documentation; and Conformity Assessment).

04 And finally, co-design hand in hand with our clients a **tailored action plan** to successfully be compliant with the regulatory framework that revolves around Artificial Intelligence, such as the AI Act and the Guidelines for a Trustworthy AI.

ABOUT NTT DATA

DATA & INTELLIGENCE CENTER OF EXCELLENCE

NTT DATA has launched the Data and Intelligence Center of Excellence (D&I CoE) to support clients in addressing challenges and tackling hurdles when embedding D&I technologies.

The CoE is composed of a multidisciplinary team of experts who developed end-to-end D&I top-notch projects.

In this way, the D&I CoE has the mission of being a:

- Know-how leader in the latest D&I technologies
- Global innovation booster through a comprehensive offering based on our full-fledged expertise
- Active contributor in the Open D&I ecosystem, fostering knowledge democratization and social impact

LINES OF ACTION

Strategy

Solution ideation and design capabilities, the definition of responsible governance, and innovation support.

Architecture

Design and implement D&I architectures that allow easy development and scaling of solutions.

Solutions

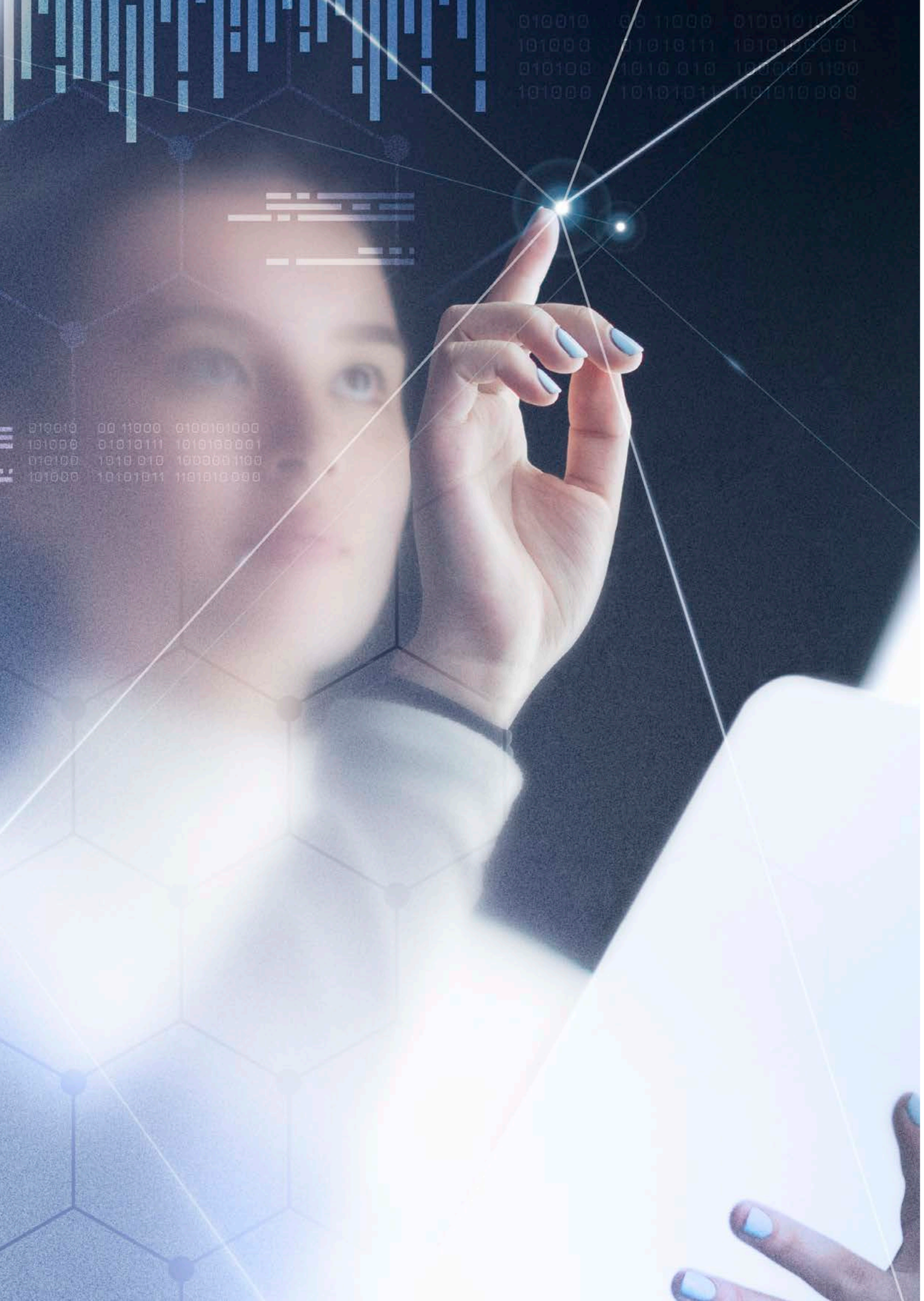
Advisory, support, and development of D&I solutions tailored to the client's needs.

Experimentation

Trend observatory tasks, testing of new technologies and development of functional prototypes.

Ecosystem

Participation in the D&I open ecosystem, performing knowledge democratization actions, and developing collaborative innovation projects.



About NTT DATA

For 2022 Gartner's Magic Quadrant, NTT DATA has been named a Challenger service provider. This supports NTT DATA's goal to help clients maximize their business value through technology implementation expertise, innovation practices, and trustworthy Data and Intelligence (D&I).
The company shares the Innovation DNA as part of NTT Group, which boosts the innovation in the open ecosystem and fosters responsible AI across its operations.
As a trusted global innovator, our values come from "consistent belief" to shape the future society with clients and "courage to change" the world with innovative digital technologies.
Key Contacts

Key Contacts

DAVID PEREIRA PAZ
Head of Data & Intelligence Europe

JACINTO ESTRECHA
Head of Artificial Intelligence Spain

MARC SANGUESA PUIGVENTOS
Data & Intelligence CoE Manager

Authors

MOHAMMED ADIL MOUJAHID
Technical Manager

MARTA PASTOR
Expert Analyst

ROSE BARRAGAN
AI Analyst

LEIRE ECHEVARRIA
Jr. Analyst

JANUARY 2023

BIBLIOGRAPHY

***)** Statista. (n.d.). Artificial Intelligence market size/revenue comparisons 2020. [online] Available at: https://www.statista.com/statistics/941835/artificial-intelligence-market-size-revenue-comparisons/.

1) Parker, L. (2022). National Artificial Intelligence Initiative Artificial Intelligence and Emerging Technology Inaugural Stakeholder Meeting. [online] Available at: https://www.uspto.gov/sites/default/files/documents/National-Artificial-Intelligence-Initiative-Overview.pdf

2) DigiChina. (n.d.). Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022. [online] Available at: https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/.

3) Social Principles of Human-Centric AI. (n.d.). [online] Available at: https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/humancentricai.pdf

4) digital-strategy.ec.europa.eu. (n.d.). Coordinated Plan on Artificial Intelligence | Shaping Europe's digital future. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/plan-ai

5) digital-strategy.ec.europa.eu. (2021). Ethics guidelines for trustworthy AI | Shaping Europe's digital future. [online] Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

6) On Artificial Intelligence -A European approach to excellence and trust White Paper on Artificial Intelligence A European approach to excellence and trust. (n.d.). [online] Available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

7) futurium.ec.europa.eu. (n.d.). Futurium | European AI Alliance - Welcome to the ALTAI portal! [online] Available at: https://futurium.ec.europa.eu/en/european-ai-alliance/pages/welcome-altai-portal.

8) Europa.eu. (2021). EUR-Lex - 52021PC0206 - EN - EUR-Lex. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

9) digital-strategy.ec.europa.eu. (n.d.). Data Act | Shaping Europe's digital future. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/data-act.

10) www.holoniq.com. (n.d.). 50 National AI Strategies - The 2020 AI Strategy Landscape. [online] Available at: https://www.holoniq.com/notes/50-national-ai-strategies-the-2020-ai-strategy-landscape

11) Executive Office of the President of the United States (2019). The National Artificial Intelligence research and development strategic plan. [online] Select Committee on Artificial Intelligence of the National Science & Technology Council. Available at: https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf.

12) oecd.ai. (n.d.). OECD AI Policy Observatory Portal. [online] Available at: https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-24114

13) oecd.ai. (n.d.). OECD AI Policy Observatory Portal. [online] Available at: https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-27222

14) AI Strategy 2022 (Overview). (2022). [online] Available at: https://www8.cao.go.jp/cstp/ai/senryaku/10kai/sanko1.pdf

15) ised-isde.canada.ca. (2022). Pan-Canadian Artificial Intelligence Strategy - Home. [online] Available at: https://ised-isde.canada.ca/site/ai-strategy/en

16) oecd.ai. (n.d.). OECD AI Policy Observatory Portal. [online] Available at: https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-24270

17) oecd.ai. (n.d.). OECD AI Policy Observatory Portal. [online] Available at: https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-27013

18) Version 1.0 0. PROLOGUE. (n.d.). [online] Available at: https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/National-Strategy-on-AI.pdf.

19) Landing - Sandbox Spain (n.d). Available at: https://sandboxspain.com/en/landing/

20) Directorate-General for Communications Networks, C. and T. (European C. and Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji (2019). Directrices éticas para una IA fiable. [online] Publications Office of the European Union. LU: Publications Office of the European Union. Available at: https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-es

21) Europa.eu. (2021). EUR-Lex - 52021PC0206 - EN - EUR-Lex. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

JANUARY 2023

NTT DATA Corporation

Novus Building, Cam. Fuente de la Mora, 1, 28050
Madrid, Spain

www.nttdata.com