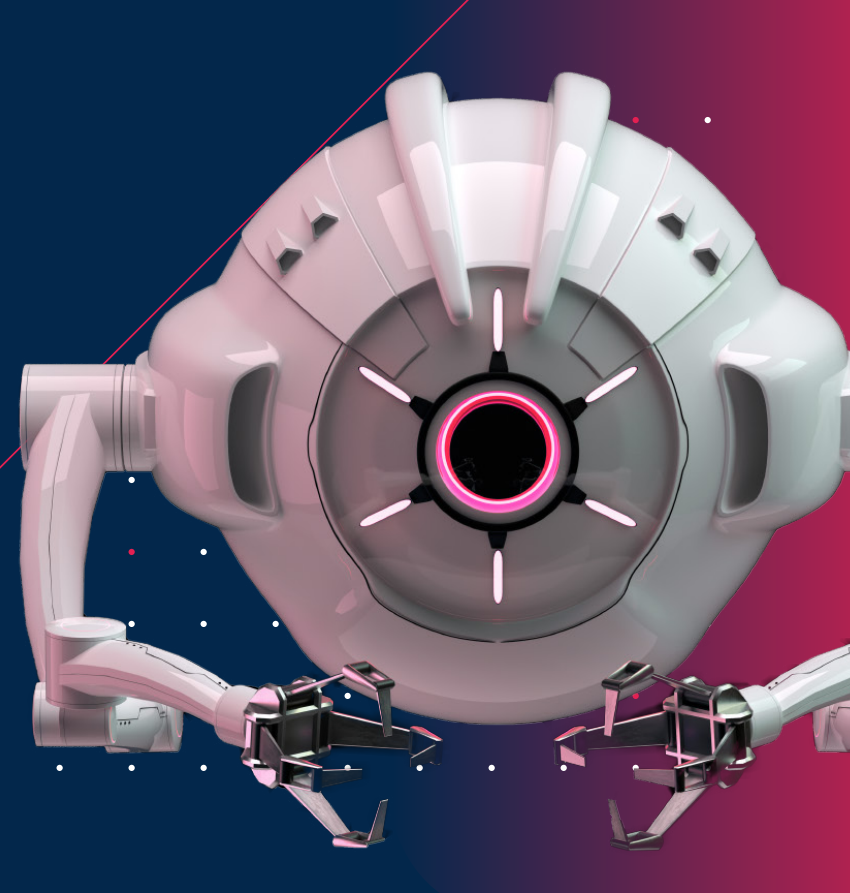
Robotics4EU
Boosting Wider Adoption of Robotics in Europe

Factsheet #9.

Privacy And Cyber Security In Responsible Robotics



Disclaimer
This factsheet is based on research conducted by the Robotics4EU, as well as second-hand data collected by the project team from desktop research.

The use of data, privacy and cyber security is something that has a significant impact on how citizens and stakeholders view robots and robotic technology in general. Robotics4EU carried out a series of citizen and stakeholder engagement activities that yielded useful insights about how people see and feel about privacy and cyber security when talking about robots. The views and opinions of citizens and stakeholders that were involved in the project activities are summarised in the factsheet at hand.

Citizen Consultations and Robot Validation Surveys Reveal a Fear of Misuse and Vulnerability of Data

According to the GlobalSay citizen consultations, the highest ranking worries revolve around ***what kind* of data as well *as how much* data** the robots we encounter in our daily lives collect and share. Virtual assistant technologies like Alexa or Echo were mentioned as particular instances of something people consider capable of secretly gathering or stealing personal information or being hacked by third parties.

Privacy concerns vary according to the type of robot discussed. A general theme, however, is the extent to which data is collected and whether it's done **considering privacy, security, and safety issues.** When setting up robots that can either deliberately or unintentionally collect data on people through cameras and sensors they are connected to, proper data management practice needs to be in place to offer transparency in the use and storage of data to the citizens affected by it.

Data Management in Agri-food

- Robotic solutions in agri-food often utilise cameras and/or sensory equipment to perform their tasks, which leads to the need to specify whether and how the data collected by the robots is shared with **third parties**.
- Workers need to be made comfortable and safe working in close vicinity to robotic solutions. Any discrepancy between the necessity for extensive data collection on people working with the robot and the actual sharing of information with third parties, **even if unintended**, is a significant barrier to adopting robots at the workplace.
- Consider how companies can ensure that workers are not being **unknowingly monitored** (e.g., on the quality of their work). One of the solution is to **make data available to the workers or the public** to show what data is being collected about whom and when.
- Workers should be involved in the implementation of a new robotic solution to **learn first-hand how data is collected and used**, for example through specific interactive training courses.
- The company could build the technologies around it that make sure that all data that is being collected by the robot stays within their control. The amount of **data collected should be limited and anonymised.**

Data Management in Healthcare

- Robots that are working in close vicinity of patients while holding cameras, sensors and other data collection equipment, the collection, storage and **handling of sensitive data is of utmost importance.**
- Telepresence robotics are expected to be applied in novel ways: by doctors to conduct virtual patient consultations, by caregivers to remotely monitor patients and by students who are unable to physically attend school to participate in classes and interact with teachers and peers.
- The vast amount of data collected by telepresence robots, such as facial images, voice recordings, personal identifying information, and health-related details **require strict adherence to best practices.**
- Health data makes **patients especially vulnerable to hackers** with malicious intents. Developers must therefore prioritise addressing privacy and security concerns for robots to be trusted by patients and their close ones.

Data Management in Agile Production

- Robots in this sector **differ vastly in how much data they collect**, raising very different concerns regarding privacy and cybersecurity. Some solutions in this sector hardly collect data at all, while others collect vast amounts of data in order to properly operate (e.g., cameras and motion capture is used to navigate and measure activities in the operating environment, which guides further action by the robot).
- **Clear guidelines for how data is stored and handled is paramount** in order to foster trust in robotic solutions. If such guidelines are not implemented and followed, workers might be more cautious around these robots as they fear that they are being monitored and that personal data about them might be collected unwillingly or without consent. To solve this, an encrypted cloud structure for storing data could be incorporated.

Data Management in Inspection and Maintenance

- Robots in this sector **often collect data in multiple ways at a time** with several cameras or sensors located at various places on the robot. This is often the case with robots designed to perform (automatic or controller-operated) inspection of different areas where cameras and/or sensors are needed for navigation and mapping the terrain.
- Regardless, whether the robot collects data locally or on a cloud infrastructure, the guidelines and rules needed for **ensuring data security are a common practice**. Companies also utilise the most reliable equipment available. The only issues lie with selected instances that might befall these solutions.
- Human workers' experience working in close vicinity with robots that utilise cameras and sensors are a priority. In these cases, **data could be divided into different categories** so that information that is non-essential for operation could be anonymised (e.g. blurring out faces). This could potentially help increase trust in the robot and broader acceptance of the robot in a work environment.

Recommendations from Citizen Consultations

Collecting Data Requires Clear Guidelines for Use

Citizens emphasised the need for creating and implementing clear guidelines on how data is stored and handled to foster trust in robotic solutions. Implementing comprehensive plans and cybersecurity protocols was suggested to address concerns about data security and trust.

Enhance Human-Robot Interaction

Considerations should be given to how human workers might feel working closely with different types of robots that utilise cameras and sensors. Solutions proposed include categorising data, blurring non-essential information, and addressing barriers to enhance human-robot interaction and collaboration.

Focus on Sector-Specific Needs

While many discussions focused on similar topics and barriers, the collection of data varies across the different sectors. Each sector (agri-food, healthcare, agile production, inspection, and maintenance) have unique challenges regarding data collection, storage, and cybersecurity that needs to be considered in specific contexts.

Enhancing Trust and Acceptance

Consciously addressing privacy concerns and implementing transparency practices (e.g., data categorization, face-blurring or other steps towards anonymising data) could enhance trust in robotic solutions and promote their broader acceptance in work environments.

Mitigating the Challenges

Some of the solutions proposed include making data available to workers or to the public, as well as informing them about the collected data. Further, involving workers in the implementation process as well as providing interactive training can be used as strategies to address privacy concerns. Other measures are for companies to build both hardware and software in order to retain control over the collected data.

Further References

Important regulations include **Cybersecurity Act** from 2019, which aims to strengthen the EU's cybersecurity framework, and **eIDAS Regulation**, which is a key enabler for secure cross-border transactions.

The European Cybersecurity Certification Group (ECCG)

Was established to help ensure the consistent implementation and application of the Cybersecurity Act.

European Cybersecurity Competence Centre and Network (ECCC)

Aims to increase Europe's cybersecurity capacities and competitiveness, working together with a Network of National Coordination Centres (NCCs) to build a strong cybersecurity Community.

The European Union Agency for Cybersecurity (ENISA)

Is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe.

The final Assessment List for Trustworthy AI (ALTAI)

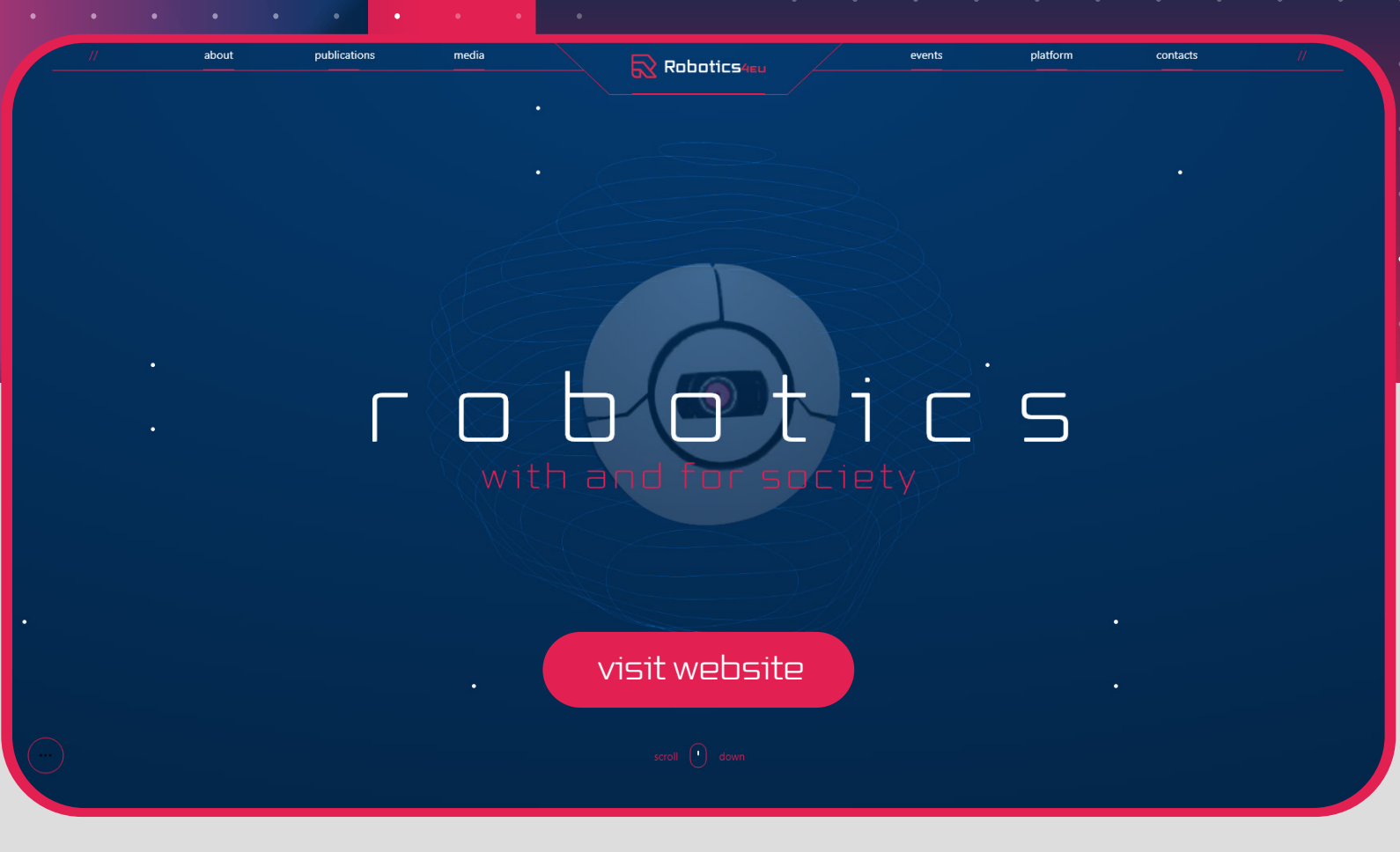
Is a practical tool that translates the Ethics Guidelines into an accessible and dynamic self-assessment checklist. The ALTAI checklist, which was developed by high-level expert group on artificial intelligence named AI HLEG, can be used by developers and deployers of AI who want to implement the key requirements.

Online guidelines on Cybersecurity: how the EU tackles cyber threats

Include various references to ways in which to tackle cyber security challenges and become more resilient to cyberattacks.

Article by

Fosch Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: strengthening the link between cybersecurity and safety in the context of care robots. *Computer Law And Security Review*, 41, 1-13. doi: 10.1016/j.clsr.2021.105528. https://hdl.handle.net/1887/3205253



consortium

CIVITTA
robotex International
LOBA
Laboratoire National de Métrologie et d'Essais LNE
Fonden Teknologirådet
AgriFood DIH Lithuania
NTNU Norwegian University of Science and Technology

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101017283