Trustworthy AAL Design Cards

cost
EUROPEAN COOPERATION
IN SCIENCE & TECHNOLOGY

Funded by
the European Union

Editors

- Gianluigi M. Riva
- Anton Fedosov
- Elif Gürçınar

Contributors

- Gianluigi M. Riva
- Anton Fedosov
- Francisco Florez-Revuelta
- Sara Colantonio
- Christoph Lutz
- Aurelia Tamò-Larrieux
- Maksymilian M. Kuźmicz
- Liane Colonna
- Petre Lameski
- Eftim Zdravevski
- Peter Pocta
- Nicolas Sklavos
- Nathalie G. S. Puaschitz
- Carina Dantas
- Ebru Metin
- Willeke van Staalduinen
- Elif Gürçınar

Acknowledgement

This toolkit is based upon work from COST Action CA19121 (GoodBrother) Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living, supported by COST (European Cooperation in Science and Technology).

COST (European Cooperation in Science and Technology) is a funding agency for research and innovation networks. Our Actions help connect research initiatives across Europe and enable scientists to grow their ideas by sharing them with their peers. This boosts their research, career and innovation.

COST: https://www.cost.eu

COST Action GoodBrother: https://www.cost.eu/actions/CA19121/

Introduction

Active and Assisted Living (AAL) refers to systems and services that support the well-being and independence of older adults and people living with frailty through the use of technology. Ensuring reliability is crucial as these technologies become more integrated into daily life. Although the rise of AAL technologies represents a major advancement in enhancing the quality of life for older adults and other frail individuals, privacy elements must be considered carefully along all stages of the development process. These technologies span a range of systems and services (from monitoring devices to smart home solutions) and aim to support independent living, health management, and overall well-being. However, as AAL technologies become more integrated into the everyday life of the end-users – typically patients or vulnerable subjects – they raise critical ethical, legal, and privacy concerns. These issues have driven the European COST Action CA19121 Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living ("GoodBrother") to explore how AAL systems can be designed and deployed in a manner that prioritizes the rights, dignity, and privacy of end users.

The research network GoodBrother, launched in 2020, seeks to balance technological innovation with societal expectations of fairness, accountability, and compliance with contemporary legal frameworks. Its overarching mission is to ensure that future AAL technologies are developed with transparency and trustworthiness. Within this framework, the Working Group on Social responsibility: Ethical, legal, social, data protection and privacy issues has played a pivotal role, focusing on how developers and designers can incorporate ethical principles and privacy-preserving methods into their work. This working group acknowledges the growing need to bridge the gap between different disciplines -particularly technology, law, and ethics - to ensure that AAL solutions not only function effectively but also respect the fundamental human rights of the end-users while also ensuring that AAL systems are trustworthy, reliable, and user-friendly.

These efforts culminate with this Trustworthy AAL Design Cards collection, which is intended as a practical set of easy-to-read guidelines for AAL practitioners. In particular, these cards provide actionable, understandable,

and specific guidance to developers, designers, and other stakeholders involved in the lifecycle of AAL systems. The key stakeholders are the professionals who need to create and implement trustworthy AAL systems. The purpose of the cards is to serve as a reference tool, providing clear guidelines for stakeholders. By offering structured advice across different stages of research, design, development, and deployment, the cards aim to foster a comprehensive approach to the ethical and compliant creation of trustworthy AAL technologies. Each card is grounded in relevant scholarly works, legal frameworks, and ethical and technological standards and offers a policy recommendation, giving stakeholders the tools they need to make informed decisions at every step of the process.

The primary goal of the Cards is to support the stakeholders through the complex process of creating AAL technologies that can be functional, fair, ethical, and compliant with legal standards. This effort drew upon collaborative design approaches (e.g., co-conceptualization and co-creation) and resulted in actionable guidelines for AAL practitioners in order to improve feasibility and compliance with technical and legal requirements and effectively preserve the privacy of end-users. In particular, the cards focus on privacy as a fundamental consideration, ensuring that the systems respect users' personal data and autonomy. Privacy violations or ethical oversights can lead to a breakdown of trust in both end-users and other stakeholders involved in the care provision, rendering even the most innovative AAL solutions unviable. Therefore, this collection emphasizes the design of trustworthy systems that users and practitioners feel confident adopting.

The primary stakeholders of the Trustworthy AAL Design Cards are developers and designers; however, project managers and decision-makers who work within the AAL domain will benefit from the cards as well. While the technical expertise of these individuals may vary, the cards aim to provide accessible and comprehensible guidelines that cut across disciplines. For these reasons, contributors who designed the cards span across a variety of fields and scientific disciplines. Developers and designers who are directly responsible for the technical and user interface aspects of AAL systems will find the cards useful for embedding ethical and privacy-conscious practices from the early stages of the development process. At the same time, policymakers, legal experts, and ethicists can use the cards to ensure that their insights are integrated into the technological process, fostering interdisciplinary collaboration.

The Trustworthy AAL Design Cards are organized to reflect the four critical stages in the development of AAL systems: Research, Design, Development, and Deployment/Maintenance. Each stage introduces unique challenges related to privacy, ethics, and compliance. The cards offer tailored advice for navigating

these challenges. The research phase is foundational to the development of AAL systems. It involves gathering data, defining user needs, and analyzing the technological and ethical implications of potential solutions. During this phase, it is essential to ensure that research methodologies respect privacy laws, such as the General Data Protection Regulation (GDPR) or the Medical Device Regulation, among others, and maintain the dignity and rights of participants. The Cards offer specific guidelines on how to conduct research ethically, including recommendations on obtaining informed consent, anonymizing data, and ensuring transparency in data collection and use. The design phase involves conceptualizing the AAL system's functionality, user interface, and interactions. This stage requires a careful balance between user experience and privacy. The Cards encourage developers and designers to adopt privacy-by-design approaches and data minimization principles to ensure that privacy considerations are integrated into the system's architecture from the outset. The Cards, thus, provide insights into designing systems that are intuitive, secure, and capable of handling sensitive data responsibly. The development stage translates design concepts into tangible interactive products or services. This phase requires adherence to technical standards and legal regulations, particularly those related to data protection and information security. The Cards offer advice on selecting appropriate security methods, implementing secure data storage, and ensuring that user data is processed lawfully and ethically in every stage of its lifecycle. Additionally, the Cards offer pointers to developers on conducting security assessments and integrating feedback loops to address potential ethical and privacy issues as they arise. Finally, once an AAL system is deployed, continuous monitoring and maintenance are necessary to ensure it remains functional, secure, and compliant with evolving legal standards. The Cards emphasize the importance of post-deployment assessments and monitoring, focusing on timely updates of privacy policies, conducting regular security audits, and engaging with users to gather feedback. This stage also involves managing data retention and ensuring that users have control over their data, including options for data deletion or modification in compliance with legal rights.

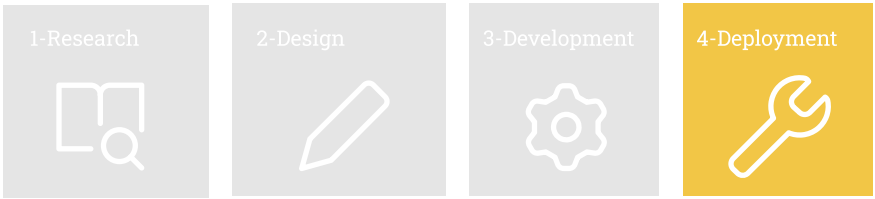
The Trustworthy AAL Design Cards are designed to be flexible and easy to integrate into the workflow of stakeholders at various stages of AAL system development. Each card is structured around a specific issue or challenge, identifying the different stages in which it applies and providing actionable recommendations for addressing it. The structure is aimed at enhancing rapid understanding of the main elements of the topic addressed; for this reason, they provide questions and answers, keywords, examples, or scenarios that may clarify the context. For instance, one card may focus on obtaining informed consent in the research phase, while another might provide advice on implementing data encryption during development. The cards are concise and

self-contained, allowing stakeholders to reference them quickly as they progress through the stages of their project. Likewise, they all contain actionable policy recommendations to guide the development process, and, when applicable, they offer a legal recommendation with an explicit reference to the specific legal requirements for that scenario. This approach intends to provide stakeholders with a brief explanation of the legal or ethical rationale behind each issue addressed, ensuring that they not only know what to do but also understand why it is important. This feature helps bridge the gap between disciplines, allowing developers and designers to engage with legal and ethical considerations without requiring deep expertise in those fields. However, they are not meant to remove or replace legal experts throughout these phases. Additionally, the cards are designed for an iterative development process, meaning stakeholders can revisit them as new challenges or questions arise.

In conclusion, within a rapidly evolving field like AAL, where technological advances should be balanced with ethical and legal considerations, the Trustworthy AAL Design Cards provide an essential tool for developers, designers, and other stakeholders to readily access multidisciplinary know-how concerning AAL technology and service design. By offering clear, actionable, and reliable guidance across the lifecycle of AAL systems - from research to deployment - the Cards enable stakeholders to design innovative technologies that are trustworthy and compliant with privacy and ethical standards. Ultimately, the cards bridge the technical, legal, and ethical domains, ensuring that AAL technologies can be developed fairly, respecting users' rights and needs, and fostering trust in their adoption.

AI Model Performance

Phases:



Recommendation:

The performance of the AI model must be monitored over time to ensure reliability.

As the state of the art changes, so do circumstances and humans. It is important to ensure that AI models are up to date by constantly monitoring their performance and updating them when necessary.

Stakeholders:

Caregivers Caretakers Developers

#Management #Infrastructure

#model drift #concept drift #machine learning

Example/Scenario Description

Over time, the older adults' behavior patterns may change due to health conditions, changes in routine, or new medications. The model monitoring system tracks the model's prediction accuracy and flags any drift when it notices that the model's predictions deviate significantly from the actual observed data. For example, if the model frequently misclassifies normal nighttime bathroom visits as potential falls, it indicates model drift.

Q&A

Q. Is the AI model's performance consistent over time?
A. No: models' performance changes due to data and concept drifts, as well as people's behavior and needs changing over time.

Policy Recommendation

Establish a procedure and methodology to keep monitoring over time AAL systems (e.g. audit the system every two months, or less if needed).

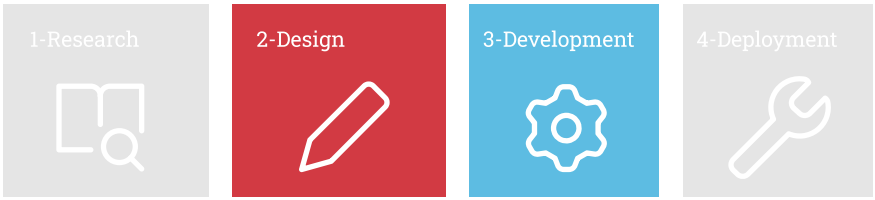
Legal Recommendation

According to Article 25(1) of the GDPR, the data controller (and so developers) must, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures in an effective manner and to integrate the necessary safeguards into the processing. specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. These measures ensure data minimization and also AAL systems reliability and efficacy.

Source: B. Dong, Y. Li, Y. Gao, A. Haque, L. Khan and M. M. Masud, "Multistream regression with asynchronous concept drift detection," 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 2017, pp. 596-605, https://doi.org/10.1109/BigData.2017.8257975

Mental Health & Culture

Phases:



Recommendation:

Incorporate cultural context in the design and dvelopment of AAL systems aimed at mental health monitoring.

Cultural context is an important part of the mental health caring and monitoring, as from it may depend the patient's response and behaviour. These elements need to be carefully studied and incorporated in any AAL mental health monitoring system development.

Stakeholders:

Patients Caregivers Caretakers End Users

#Context

#mental health #culture #privacy #design

Example/Scenario Description

Some cultures might associate mental health issues with personal weakness or family dishonor, leading to reluctance in seeking help. The monitoring system incorporates educational modules that address these beliefs sensitively, providing information about mental health as a medical issue rather than a moral failing.

Q&A

Q1. Do cultures treat mental health issues in the same manner?
A1. Mental health issues may depend on culture and they are treated differently depending on it.
Q2. Are mental health issues stigmatized?
A2. Yes, some cultures stigmatize mental health problems and treat them as evil occurrences and deviations.
Q3. How can developers address these differences?
A3. They should incorporate contextual and cultural-related elements within the design of their model to be able to address properly these differences.

Policy Recommendation

Proper tools to evaluate, address, and incorporate cultural and behavioural elements that may reflect on mental health or privacy should be developed in an early stage of the design process. Internal training and general education for mental health and contextual privacy should be implemented. Awareness of mental health issues will refine the design and development of AAL systems eventually benefitting the quality of data and usability of the service.

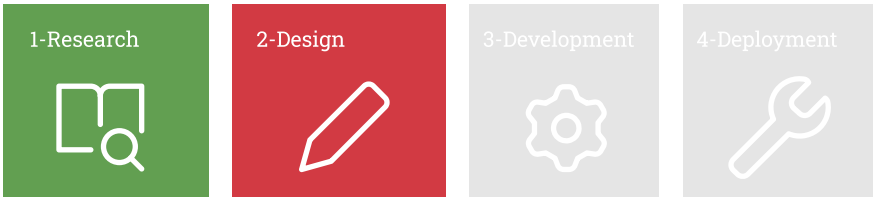
Legal Recommendation

When considering Article 25(2) of the GDPR provisions concerning "data protection by default" in the design process of an AAL system or service, the contextual elements that may impact individuals' privacy perception should be properly assessed and incorporated. Design requirements must also align with the EU Regulation 2017/745 on Medical Devices: specifically, where applicable, Article 61(3) provides that a clinical evaluation shall follow a defined and methodologically sound procedure based on "(a) a critical evaluation of the relevant scientific literature currently available relating to the safety, performance, design characteristics and intended purpose of the device".

Source: Faregh, N., Lencucha, R., Ventevogel, P. et al. Considering culture, context and community in mhGAP implementation and training: challenges and recommendations from the field. Int J Ment Health Syst 13, 58 (2019). https://doi.org/10.1186/s13033-019-0312-9

Users' Involvement

Phases:



Recommendation:

Spend time with end users and all the groups of stakeholders that are interested by the intended AAL system to elicit their needs, concerns, and expectations about the system functioning.

To ensure your AAL system is truly useful and beneficial for end users, it is essential to provide them with a voice and a stake in the solutions they will be using or that will involve them. This may necessitate multiple sessions of interactive requirements elicitation, as well as co-design or co-creation with the relevant end users.

Stakeholders:

Designers Developers End Users

#Requirement

#co-design #co-creation #transparency #efficacy

Example/Scenario Description

Services, programs, devices, or systems developed without considering end-users' perspectives and actual needs may result inefficient, with end-users not using it because unfriendly, not useful, or not adapt for their actual needs. This undermines the very purpose of the development process.

Q&A

Q. How can a developer guarantee that the system will be used by end users?
A. Allowing end users to contribute to the design of your AAL system enables developers to gain insight into their expectations and specific requirements or concerns, also allowing them to tailor response to their needs more effectively.

Policy Recommendation

Define a designing procedure to involve end-users in the design process, by assessing, evaluate, test, and validate their needs in different stages of the dseigning process to ensure the efficacy and usability of the final product.

Legal Recommendation

The correct design of a system, process, device, or service ensures the respect of the principles of purpose, data minimization, and accuracy as per the GDPR Article 6(1) b), c), and d). Implementing an adeguate engagement of the end-users into the design process may ensure that the principle of fairness and transparency (Article 6(1) a) and Article 12 of the GDPR) and the overall duty of information towards data subjects (end-users), according to Articles 13 and 14 of the GDPR may be fully respected.

Source: Sanders, E.B.N. and Stappers, P.J. (2008), Co-creation and the new landscapes of design. Co-design, International Journal of CoCreation in Design and the Arts 4, 1, pp.5-18. https://doi.org/10.1080/15710880701875068

Users' Engagement

Example/Scenario: Designing "Elder Home Assist"

Objective: Develop a smart home system that responds to the needs of older individuals, enhancing their safety, comfort, and independence.

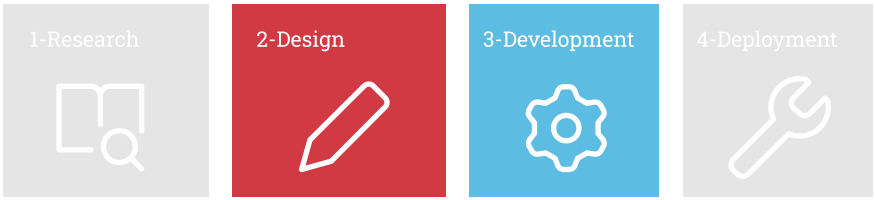
1. Initial Conceptualization:
   - A tech company, Innovate Home Solutions, decides to create "Home Assist," a smart system with features like fall detection, voice-controlled lighting, and medication reminders.
2. Engagement with End Users:
   - Understanding the critical need for end-user input, the company invites a group of older individuals, their family members, and caregivers to participate in co-design workshops. These workshops aim to gain insights into their daily routines, challenges, and suggestions.
3. Key Insights Gathered:
   - Older-adult participants express concerns about privacy with camera-based fall detection. They prefer non-intrusive sensors.
   - Family members highlight the need for real-time alerts for serious incidents directly to their smartphones. Caregivers suggest integrating a simple communication feature like a voice-activated emergency contact system.
4. Iterative Design Phase: Based on feedback, Innovate Home Solutions adjusts the design:
   - Uses motion and pressure sensors instead of cameras for fall detection.
   - Implements a secure, privacy-focused data management system.
   - Enhances the user interface to ensure large buttons and voice commands for easy interaction.
5. Prototyping and Testing:
   - Prototypes are developed and installed in the homes of several participants for a trial period.
   - Users provide continuous feedback on system usability and any operational challenges faced.

6. Refinements Based on User Feedback:
   - Adjustments made include simplifying the voice command system and improving the battery life of wearable components.
   - More personalized medication reminders are added, which can adapt based on user routines and preferences.
7. Launch and Ongoing Co-design:
   - With the refined design, "Home Assist" launches to positive reception, praised for its user-friendliness and alignment with user preferences.
   - Continuous feedback channels are established, allowing users to suggest improvements or report issues, ensuring the system evolves with user needs.

Outcome: Through co-designing "Home Assist" with end users, Innovate Home Solutions created a system that truly meets the needs of its users. This approach resulted in a more effective product and also enhanced user trust and satisfaction, thus leading to better adoption rates and improved life quality for its users. This scenario underscores the importance of integrating end-user perspectives in the design of active and assisted living systems.

Edge Computing

Phases:



Recommendation:

Use embedded, edge or fog computing instead of cloud services.

Some actions require speed. In cases of AAL where a system should respond quickly, the communication loop should be as short as possible and as stable as possible.

Stakeholders:

Patients Caretakers Telecoms Product producers

#Risk #Infrastructure #Sustainability

#fog computing #embedded computing

Example/Scenario Description

Rural areas might have unreliable internet connectivity, with frequent disruptions and low bandwidth. Relying on cloud-based services for real-time monitoring and data processing would result in delays and gaps in service. To address this, the AAL system uses edge computing, where data processing occurs locally on devices such as smart hubs or gateways installed in the home. This ensures that critical data, like fall detection alerts or emergency health information, can be processed and acted upon immediately, even if the internet connection is lost.

Q&A

Q1. Is internet connectivity always available?
A1. No, it might be unreliable, especially in rural areas.

Q2. Do all people have access to high bandwidth network?
A2. Not always people may access stable broadband.

Policy Recommendation

Subsidies internet connectivity in rural areas. Enforce response times from critical systems. Provide better digital infrastructure (e.g., high-speed broadband internet).

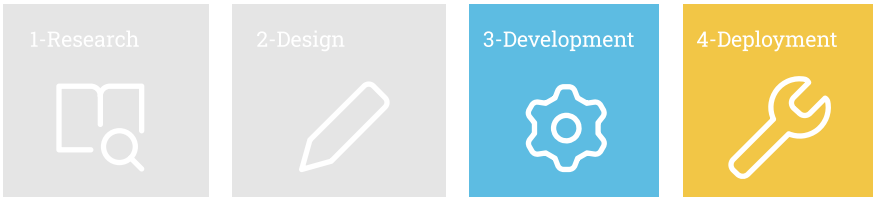
Legal Recommendation

Provide clear explanation in the contract, or Terms & Conditions of the service, regarding the potential interruption of the service due to bandwith issues non depending on the AAL service provider. Manage recurrent incremental back-up and business continuity solutions in accordance with the general provisions laid out by Article 32(1) c) of the GDPR.

Source: Neel Mani, Akhil Singh, Shastri L Nimmagadda,An IoT Guided Healthcare Monitoring System for Managing Real-Time Notifications by Fog Computing Services, Procedia Computer Science,Volume 167,2020,Pages 850-859,ISSN 1877-0509,https://doi.org/10.1016/j.procs.2020.03.424.

Local Processing

Phases:



Recommendation:

End device should be powerful enough to process all the necessary user data related to the service locally (without relying on cloud services).

If the data are transfered to and processed at the cloud, end users may have privacy concerns. To increase their trust in AAL systems and applications in terms of user data handling is important to minimize the data exposure.

Stakeholders:

Developers

#Infrastructure

#end device #device power #user data

Example/Scenario Description

First, consider contemporary edge-computing devices (e.g., Luxonis OAK-D cameras) for sensing and processing user data locally. Second, ensure that local infrastructure is organized in a way that processing is happening without the use of the cloud facilities, unless necessary. Third, consider secure protocols when communicating between sensing and data processing devices.

Q&A

Q. Are the personal data transferred and processed out of my end device?
A. Most of the data should, by design, processed at end-users' end device in order to better protect their privacy and personal data.

Policy Recommendation

Educate decision-makers on best practices in privacy protection and appointing a data controller.

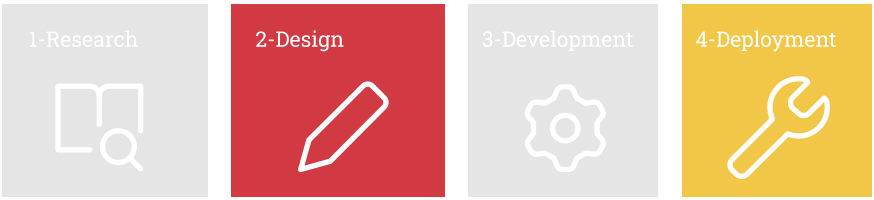
Legal Recommendation

The principle of data minimization (Article 5(1) c)) must be implemented according to data protection by design and by default requirements (Article 25) and the provisions concerning system security laid out by Article 32.

Source: Mujirishvili, T., Fedosov, A., Hashemifard, K., Climent-Pérez, P., & Florez-Revuelta, F. (2024). "I don't want to become a number": Examining different stakeholder perspectives on a Video-Based Monitoring System for Senior Care with inherent privacy protection (by design). In CHI '24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (Vol. 16, pp. 1–19). https://doi.org/10.1145/3613904.3642164

Data Breaches

Phases:



Recommendation:

Create mechanisms to recover from security breaches (e.g., data breaches) Take into account the GDPR requirements.

Minimize the possibility of security breaches (both internal and external) concernign the data processing during the operation of the products and services.

Stakeholders:

Developers | Ethics and Compliance Officers | Users | Security Experts | Product Managers

#Risk #Security #Infrastructure

#exploit attacks #weak passwords #drive-by downloads

Example/Scenario Description

The provisions should be made for a possible data breach during system's operation, or data breach with personal data leakage, outside the product/service environment.

Q&A

Q. How it is possible to improve system security maintenance?
A. System security must be implemented both offline and online from the design stage, enhancing possible additional detection and recover mechanisms.

Policy Recommendation

Provide additional formal guidelines to make interpreting the law easier for developers of AAL technologies and promote compliance technologies that encode important aspects of the GDPR into products and services. Increase awareness of the fact that pseudonymisation and anonymisation are not 'one-off exercises' and that appropriate security measures are required even when data are pseudonymised or anonymised. Increase awareness about edge computing and local-only storing or processing as mechanisms to keep information processing as close to the source as possible in the context of AAL technologies.

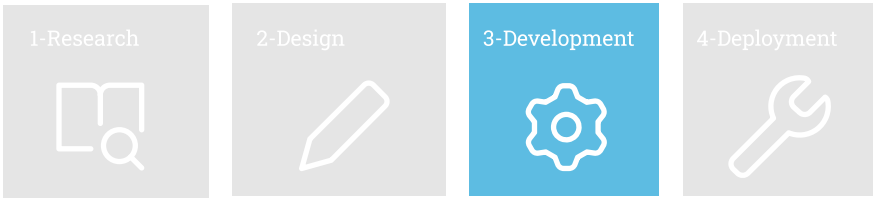
Legal Recommendation

Any potential data breach should be handled according to the provisions of Article 33 of the GDPR. The competent Data Protection Authority must be notified of the data breach within 72 hours unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (e.g. when data are anonymized, treated with strong cryptography, or consist of synthetic data).

Source: Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews Data Mining and Knowledge Discovery, 7(5). https://doi.org/10.1002/widm.1211

Energy Consumption

Phases:



Recommendation:

End device should be optimized as much as possible to decrease its energy consumption.

End users may be concerned about energy consumption of devices, which impact on their autonomy and reliance on an AAl service. To address this issue, energy consumption of device should be considered while developing AAL systems/applications.

Stakeholders:

Developers

#Sustainability

#energy consumption #optimization #end device

Example/Scenario Description

End-users might be using the device to actively perform healthcare activity or passively exploit AAL monitoring, without considering the battery consumption and, so, being aware of the device running out of battery, so compromising the service utility.

Q&A

Q. Is this AAL system/application energy efficient?
A. It must be paid attention to this issue while developing the system/application.
Q. Was sustainability considered while developing this system or application?
A. The system or application should be designed to optimize energy consumption during the developing phase.

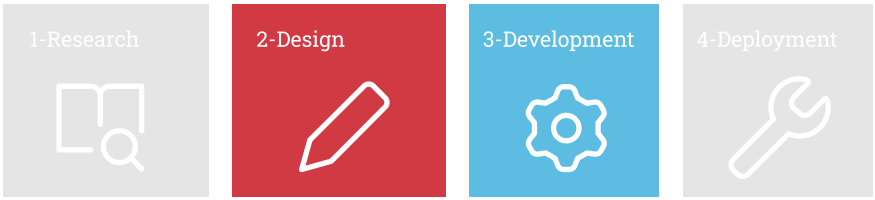
Policy Recommendation

Keep non-digital alternatives in addition to digitised healthcare provision. Users should always be able to access the service and thus service-continuity must be ensured in all stages, particularly in critical treatments. Adopt precautions to ensure constant recharge or substitution of the batteries.

Source: Bassoli M., Bianchi V., et al. (2017), An IoT Approach for an AAL Wi-Fi-Based Monitoring System, IEEE Transactions on Instrumentation and Measurement 66, 12, 10.1109/TIM.2017.2753458

Audio/Video Data Minimization

Phases:



Recommendation:

Introduce methods that protect personal or sensitive information at the user-interface level from captured videos or audios.

Cameras capture data that may include relevant information for AAL applications, as well as private details, such as faces or exposed body parts, which must be protected. Visual obfuscation methods, like pixelation, blurring, face de-identification, or body abstraction, should be considered.

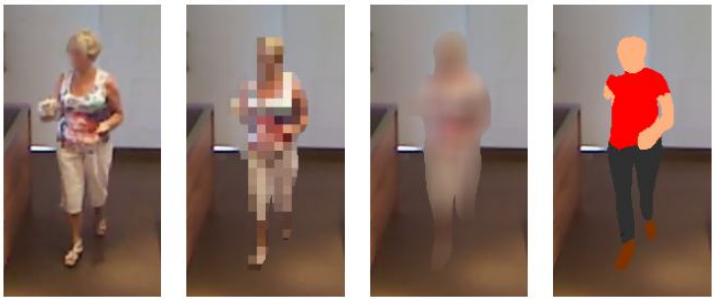
Stakeholders:

Designers Developers End Users

#Privacy

#visual privacy #obfuscation #de-identification #data minimization

Example/Scenario



(a) Original (b) Pixelated (c) Blurred (d) Avatar

Image source: Aleksic, S., Colonna, L., Dantas, C., Fedosov, A., Florez-Revuelta, F., Fosch-Villaronga, E., Jevremovic, A., Msakniç, H. G., Ravi, S., Rexha, B., & Tamò-Larrieux, A. (2022). State of the art in privacy preservation in video data. Zenodo. https://doi.org/10.5281/zenodo.6806207

Q&A

Q1. How can I de-identify people in acquired images?
A1. Simple techniques include pixelating or blurring faces. More advanced AI-based methods involve swapping faces or generating fake ones to replace those in the image.
Q2. How can I protect the visual appearance of monitored people, such as if they are naked?
A2. One option is to use visual obfuscation methods, like replacing people with silhouettes or avatars. However, it is important to balance privacy protection with ensuring the AAL service remains effective and useful.

Policy Recommendation

Public bodies and technology developers need to assess and review the user needs and values concerning design and implementation of video-based monitoring systems.

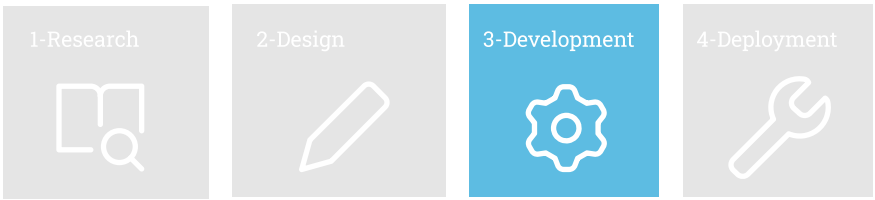
Legal Recommendation

Data minimization (Article 5(1) c) of the GDPR) and privacy by default (Article 25) imply the implementation of all the necessary safeguards to preserve not only the integrity of personal data, but also the privacy aspects of the subjects as related to their dignity and intimacy. When dealing with highly sensitive personal data or biometric data, Article 9 also applies.

Source: Ravi, S., Climent-Pérez, P. & Florez-Revuelta, F. A review on visual privacy preservation techniques for active and assisted living. Multimed Tools Appl 83, 14715–14755 (2024). https://doi.org/10.1007/s11042-023-15775-2

Algorithmic Transparency

Phases:



Recommendation:

Ensure transparency in Machine Learning algorithms, so that users and caregivers can gain trust in AAL systems by understanding decisions.

Ensuring transparency in machine learning algorithms allows users and caregivers to understand how decisions are made, building trust in the AAL system. This enhances accountability and enables users to question decisions or intervene when necessary.

Stakeholders:

End Users Caregivers Developers

#Governance

#explainability #accountability #decision-making

Example/Scenario Description

An AAL system detects unusual nighttime activity and raises an alert for the caregiver. The system also provides a log explaining that it based this decision on the user's recent pattern of irregular sleep and nighttime wandering, allowing the caregiver to understand the reasoning behind the alert.

Q&A

Q. Why is transparency important in AAL systems?
A. Transparency ensures that users and caregivers can understand the decisions being made, enhancing trust.

Policy Recommendation

Require all AAL system developers to utilize explainable AI methods, provide expectations and examples of the explainability. Additionally, require that they provide detailed, user-friendly explanations for algorithm decisions and processes. Develop practical guidelines for the end-user and the carer, potentially aided by audio-visual material that is easy to understand (e.g., instructional videos). (position paper p.4)

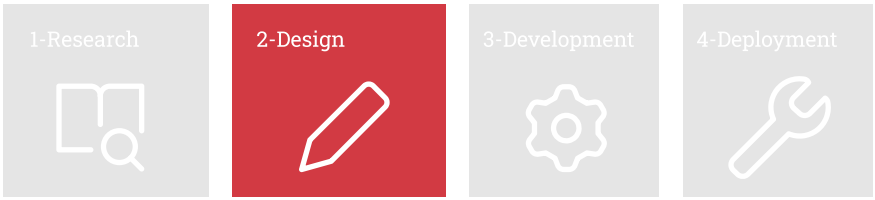
Legal Recommendation

Article 22 of the GDPR provides for automated individual decision-making, including profiling activities, which may impact significantly on the person's sphere. In these cases, it is necessary to provide for the so-called "human-in-the-loop" to validate the decision, or to acquire preventive valid and lawful consent from the end-user.

Source: Cheung J.C.-W., Tam E.W.-C., et al. (2021), Night-Time Monitoring System (eNightLog) for Elderly Wandering Behavior. Sensors, 21, 704. https://doi.org/10.3390/s21030704
Rowe M.A., Kelly A, et al. (2009), Reducing dangerous nighttime events in persons with dementia by using a nighttime monitoring system, Alzheimer's & Dementia, 5, 5, pp.419-426, https://doi.org/10.1016/j.jalz.2008.08.005

Intended Purpose

Phases:



Recommendation:

Clearly define the intended use of your product.

Having a clarity on the intended use of the AAL technologies may help you to decide on numerous aspects of design, and inform the end-users about the benefits and limitations of your product. Intended use is also crucial for legal classification of your product.

Stakeholders:

AAL Providers AAL Developers

#Legal

#medical device #privacy #compliance

Example/Scenario Description

Device A generates new information by analysing data received from external sources (e.g., a blood pressure meter, a wearable, an electronic health record). That device would be classified as medical device software. Meanwhile, a device B which performs storage, communication or simple search of medical data is not considered a medical device.

Q&A

Q1: Is the legal classification of my product that important?
A1: Yes, it is important. Depending on the classification of your product as medical device, you may have different requirements under the Medical Device Regulation. Moreover, if your product is a medical device, it will most probably be a high-risk system under the AI Act, which mean another obligations.

Q2: How should I know if my device would not be used for other purposes?
A2: For the legal classification, the intended purpose is relevant, i.e., what you advertised as the aim of your product.

Policy Recommendation

Prepare a set of policy for guiding the providers in understanding the legal requirements concerning medical devices. Legal/privacy training of the involved professionals is also a pivotal aspect to considered for ensuring compliance and minimizing the risks.

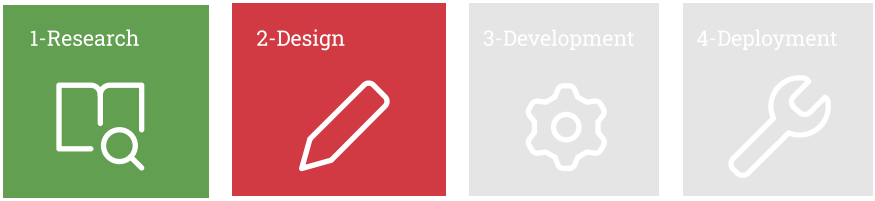
Legal Recommendation

Align with the provisions of the Medical Device Regulation for what concern the definition of medical device and the purpose of its usage, to check conformity and applicability of the requirements.

Source: http://www.aal-europe.eu/wp-content/uploads/2021/04/AAL-and-the-new-EC-Medical-Devices-regulation-final.pdf

Data Protection Impact Assessment

Phases:



Recommendation:

Step by step, assess each potential risk, grade it (high, medium, low), and evaluate its corresponding impact on specific rights or individual interests (e.g. data portability, automated decisions, transparency). Create a strategy how to mitigate it.

Data Protection Impact Assessment (DPIA) must be performed in advance, before and within the design process. The goal of a DPIA is to anticipate any potential data processing risk that the system/ service may create and to find a way to temper them. It allows to map the data processing, their effects and estimated results and, thus, to have a clear overview of the whole data flow that will occur.

Stakeholders:

Developers Practitioners Client (Data Controller)

#Governance #Privacy #Legal

#compliance #data protection

Example/Scenario Description

A developer must create an interface to interact with users. The developer needs to understand how to design the interactive features to align the purpose of the service with the users' needs in a friendly and easy way, while remaining compliant with the GDPR. The interactive feature may imply automated decision that could impact some user's rights, such as access to medical treatments. The developers needs to know in advance how to design these features to mitigate the risks of biased or incorrect decisions.

Q&A

Q. How a Data Protection Impact Assessment (DPIA) should be performed?
A. Before designing and implementing any item (technology, device, interface, or software) that gather personal data whose processing nature, scope, or purpose is likely to result in a high risk to the rights and freedoms of natural persons, the data controller should analyse the characteristics of the item and specific data processing and listing and evaluating the potential risks they may generate, while also consider mitigation strategies.

Policy Recommendation

Identifying and mitigating risks arising from a new project may affect positively your organisation or the individuals it engages with by ensuring compliance and ethical data processing. Provide a clear methodological guidance to developers on how to perform a DPIA in coordination with the legal team. The legal team should not just say "no" to everything, but proactively find a solution to mitigate risks while ensuring the feasibility of the service.

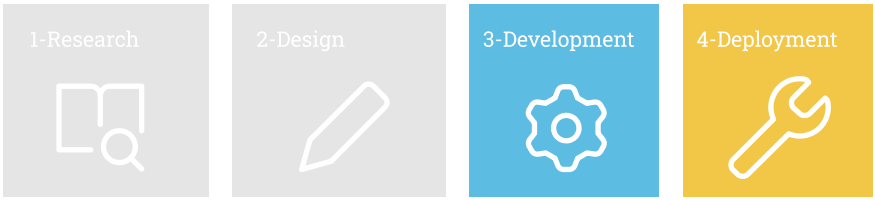
Legal Recommendation

Refer to Article 35 and 25 of the GDPR and to the Article 29 Working Group (WP29) Guidelines 248 rev. 01 2017 on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. Seek advice from a Data Protection Officer or a privacy specialist: you would not use a software designed by a lawyer, then do not implement a legal DPIA if you are an IT! money spent in advance for compliance, are money saved from legal, technical, and reputational costs afterwards.

Source: Ico.UK "How do we do a DPIA?": https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/DPC IE "Data Protection Impact Assessment": https://dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments

System Passport

Phases:



Recommendation:

Create a system passport or system card for your AAL system and share it with end users and interested stakeholders

It is essential to provide end users and interested stakeholders with comprehensive information about the system's functionality and development process, including data sources if the system is data-driven. This ensures that they can make informed decisions and have confidence in the system's benefits. A system passport or system card can be used to integrate all of this information in a structured format. It would also be advisable to invest time in describing the system to end users and recipients.

Stakeholders:

Designers Developers

#Governance #Sustainability #Legal

#system passport #system card #transparency

Q&A

Q. What strategies can be implemented to increase the adoption of the developed AAL system and enhance the trust in it?
A. Providing detailed information about the functioning and development process of your AAL system to end users and interested stakeholders may prove highly beneficial in increasing its adoption in the real world. Transparency is a crucial element in fostering trust.

Policy Recommendation

Promote the introduction of short, standardised, user-friendly forms for informational documents and consider engaging with developers to create icons that accurately and effectively present all the relevant features of products with respect to data processing.

Legal Recommendation

Information for users (data subjects) is a pivotal element in the GDPR architecture (article 13 and 14 provides for all the specific elements required) and it affects the validity of the consent (which must be informed, among other requirements, to be valid).

Source: Fadrique LX, Rahman D, et al. (2020), Overview of Policies, Guidelines, and Standards for Active Assisted Living Data Exchange: Thematic Analysis. JMIR Mhealth Uhealth, 8, 6:e15923. doi: 10.2196/15923. PMID: 32568090; PMCID: PMC7338926.

System Passport

Example / Scenario: Launching "CareCompanion"

Objective: To introduce "CareCompanion," an AAL system designed to assist elderly users with daily activities and ensure their safety, while earning their trust through transparent development practices.

1. Introduction to the Community:
   - A tech company, Community Innovations, develops "CareCompanion," which includes features like activity monitoring, medication reminders, and emergency alerts.
   - Before release, they organize information sessions in local community centers and invite potential users, family members, and caregivers.

2. Explaining the Development Process:
   - At each session, developers and designers present how "CareCompanion" was created:
     - **Co-design and co-creation**: Describe how input from elderly individuals was gathered through focus groups to shape the core features.
     - **Prototype Testing**: Share stories from beta testers who contributed to refining the product, emphasizing real-life examples and testimonials.
     - **Feedback Integration**: Explain how user suggestions directly led to system improvements, such as simplified interfaces and customizable alerts.

3. Addressing Concerns and Questions:
   - Developers distribute to each participant the so-called system passport, a leaflet containing all the relevant pieces of information, about development choices and data used.
   - Developers provide detailed explanations of privacy measures, like encrypted data transmission and limited data sharing, addressing potential concerns about security and confidentiality.
   - A question-and-answer session allows attendees to voice concerns, such as technical support availability and how data is stored and used.

4. Demonstrating Benefits and Features:
   - Live demonstrations are conducted, showing how CareCompanion responds to various scenarios, such as detecting a fall or providing medication reminders.
   - Highlighting real-world benefits encourages users to visualize how the system will fit into and enhance their daily lives.

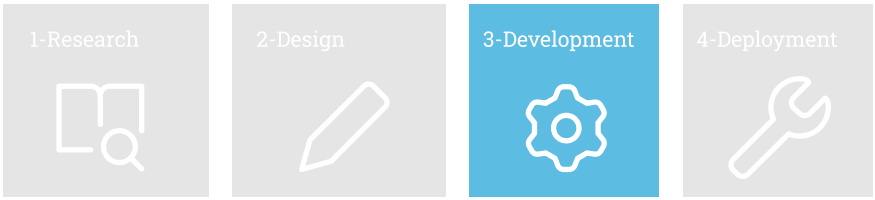
5. Building Continuous Engagement:
   - Community Innovations invites ongoing user involvement through dedicated hotlines and user feedback portals.
   - Regular newsletters keep users informed about updates and improvements based on community feedback.

6. Facilitating Hands-On Experience:
   - Interested users are offered free trials with installation assistance and personalized tutorials to ensure they are comfortable using the system.
   - Support staff are available to visit homes to assist with setup and answer any lingering questions.

7. Results:
   - Through transparency and engagement, users gain a clear understanding of the system's development and functionality.
   - Testimonials from pilot users emphasize increased trust and enthusiasm for the product, leading to higher adoption rates as word-of-mouth recommendations spread.

Integration with Smart Devices

Phases:



Recommendation:

Integrate AAL systems with healthcare and smart home technologies to create a unified support system

Ensuring AAL systems integrate smoothly with existing healthcare and smart home technologies enhances their usefulness and trustworthiness. This creates a unified support system for users without the need for multiple, isolated devices.

Stakeholders:

Developers | Healthcare Providers | Caregivers | End Users

#Infrastructure

#integration, #seamless connectivity #smart home technology

Example/Scenario Description

An AAL system that monitors an older adult's physical activity is connected with the user's existing smart home setup. When the system detects that the user has fallen, it immediately turns on the lights, sends an alert to the caregiver, and adjusts the smart thermostat to maintain a comfortable temperature while help arrives.

Q&A

Q. Why is interoperability important in AAL systems?
A. Interoperability ensures the system can work seamlessly with existing technology and provide complementary support to users.

Policy Recommendation

Encourage the development of open standards for AAL system interoperability with healthcare and home automation technologies.

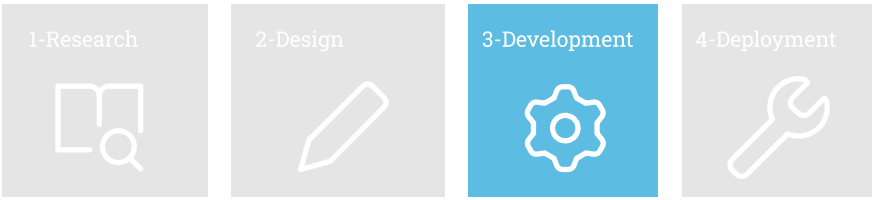
Legal Recommendation

The use of standards (e.g. ISO) and specific guidelines (e.g. EDPB, EDPS, ENISA) cant simplify the implementation of disparate systems that can still be interoperable and easily integrated. Interoperability is not specifically addressed by the GDPR, but it involves the plain and effective right to portability (Article 20).

Source: Neel Mani, Akhil Singh, Shastri L Nimmagadda, An IoT Guided Healthcare Monitoring System for Managing Real-Time Notifications by Fog Computing Services, Procedia Computer Science, Volume 167, 2020, Pages 850-859, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.03.424.

Fail-safe Mechanisms

Phases:



Recommendation:

Implement fail-safe mechanisms to protect users during errors and implement automatic fallback system behavior

Implementing fail-safes in ML-powered AAL systems ensures that users remain safe even if the system encounters an error. These mechanisms can prevent harm by automatically triggering a safe fallback response or system behavior during unexpected failures.

Stakeholders:

Developers | Healthcare Providers | Caregivers | End Users

#Security #Infrastructure

#reliability #error handling #safety protocols

Example/Scenario Description

During a power outage, an AAL system that relies on machine learning to monitor and assist the elderly user automatically switches to a basic mode that continues tracking critical events, such as falls, by using backup sensors and battery power. This ensures continued safety until the system fully restores.

Q&A

Q. What role do fail-safes play in AAL systems?
A. Fail-safes ensure that the system can handle unexpected errors without compromising user safety.

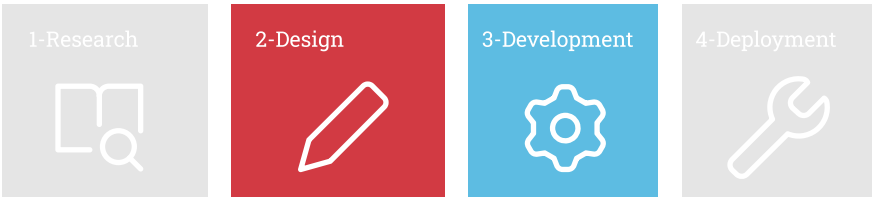
Policy Recommendation

Mandate the inclusion of fail-safe mechanisms in AAL systems to ensure user safety during unexpected errors or failures. Ensure maximal involvement of facility residents, their family members and facility employees in the technology adoption process.

Source: Neel Mani, Akhil Singh, Shastri L Nimmagadda, An IoT Guided Healthcare Monitoring System for Managing Real-Time Notifications by Fog Computing Services, Procedia Computer Science, Volume 167, 2020, Pages 850-859, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.03.424.

Data Quality

Phases:



Recommendation:

If the AAL system relies on data-driven techniques, make sure to collect enough data representing the possible real-world conditions your system will have to face.

Data-driven techniques strongly rely on the type and diversity of data they are trained on. It is important to ensure that your training dataset is diverse enough to consider the largest set of end user's characteristics, environmental conditions and acquisition settings.

Stakeholders:

Developers Designers

#Risk #Requirement #Sustainability

#data quality #data diversity

Q&A

Q. How can it be ensured that the system performs as anticipated in a range of conditions?
A. It is essential to ensure that the system performs as expected by starting with data collection and ensuring that data set is diverse enough to allow the system to be trained on varying conditions.

Policy Recommendation

Ensure that data sources and datasets are selected carefully and define in advance the criteria to select the data. This will ensure the quality of the data for your model, while also respecting data minimization requirements.

Legal Recommendation

While data minimization (Article 5(1) c) of the GDPR) may seem to contrast the need to acquire diverse set of data, it actually stressed the need to acquire more qualitative data and less quantitative data. This means that when the data collection is justified by the specific need to design and implement properly the service, data minimization is met by selecting properly the best quality of data possible for that specific purpose, so to minimize the need to acquire a vast amount of row data.

Source: Zowghi, D., Bano, M. AI for all: Diversity and Inclusion in AI. AI Ethics (2024). https://doi.org/10.1007/s43681-024-00485-8
Rose, L. T., & Fischer, K. W. (2011). Garbage In, Garbage Out: Having Useful Data Is Everything. Measurement: Interdisciplinary Research and Perspectives, 9(4), 222–226. https://doi.org/10.1080/15366367.2011.632338

Data Quality

Example/Scenario Description

Scenario: Developing "HealthWatch AI"

Objective: To create "HealthWatch AI," an advanced AAL system designed to monitor elderly users' daily activities and health metrics, providing alerts for unusual patterns that might indicate health issues.

1. Initial Development Phase:
   - The HealthTech company, Vital Innovations, begins developing "HealthWatch AI" using a dataset primarily collected from urban senior living facilities.
   - The initial training data includes sensor readings, health metrics, and daily activity logs from a relatively homogenous group of users.

2. Initial Deployment and Challenges:
   - During initial deployment, "HealthWatch AI" effectively tracks basic activities like walking and resting among urban seniors but struggles in diverse settings, such as:
     - Misinterpreting normal rural activities like gardening or farming as anomalies.
     - Inadequately responding to users from multicultural backgrounds due to different lifestyle habits and interaction patterns.
     - Errors in detecting health issues in individuals with non-standard biometric baselines (e.g., those with chronic conditions not represented in the data).

3. Understanding the Diversity Gap:
   - Feedback from healthcare providers and varied user groups reveals limitations and highlights the importance of a dataset that reflects broad usage conditions.
   - These insights prompt a deeper investigation, confirming that the training data did not account for the varied lifestyles and health profiles of a broader population.

4. Expanding the Training Dataset:
- Vital Innovations commits to collecting a more inclusive dataset by:
    - Partnering with senior communities across different geographic, cultural, and socioeconomic backgrounds, from rural areas to urban centers.
    - Gathering data reflecting diverse types of physical activities, health metrics, and living arrangements.
    - Including varied health conditions data, capturing a range of baselines and medical histories.

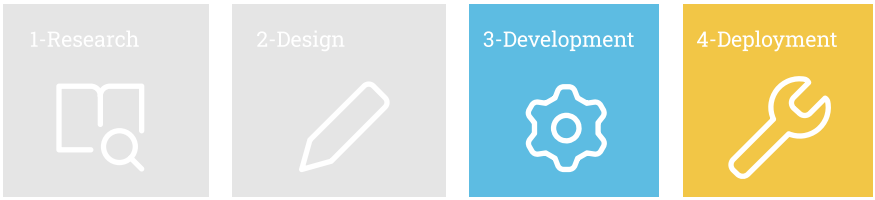
5. Retraining and Validation:
- With the expanded dataset, "HealthWatch AI" is retrained to improve accuracy and adaptability to a wider array of conditions.
- Extensive validation tests simulate diverse real-world scenarios to ensure the system's robustness across all environments.

6. Improved System Launch:
- The revamped "HealthWatch AI" demonstrates significant improvements in accurately monitoring activities and health metrics across different demographics and environments.
- Users report higher satisfaction, noting the system's enhanced personalization and reduced false alarms due to its increased understanding of diverse lifestyles.

7. Ongoing Data Collection Strategy:
- The revamped "HealthWatch AI" demonstrates significant improvements in accurately monitoring activities and health metrics across different demographics and environments.
- Vital Innovations establishes a feedback loop with continuous data collection and system updates, ensuring "HealthWatch AI" evolves with changing user needs and environments.

AI Model Updates

Phases:



Recommendation:

Regularly update and monitor ML models to maintain accuracy, effectiveness, and presonalization to user needs

Regularly updating and monitoring machine learning models ensures they remain effective, accurate, and responsive to changes in user behavior or environment. This keeps the system reliable over time and adaptable to evolving situations.

Stakeholders:

System Administrators | Caretakers | Developers | End Users

#Security #Infrastructure

#adaptability #real-time analysis #model accuracy

Example/Scenario Description

The AAL system for an older adult living with early-stage dementia regularly adjusts its behavior by analyzing changes in the user's daily routines. For example, when the system detects a slower walking speed over time, it updates its fall-risk prediction model to reflect the user's current mobility.

Q&A

Q. Why should AAL systems be continuously updated?
A. Continuous updates ensure that the system remains accurate and adapts to the changing needs of users over time.

Policy Recommendation

Establish a requirement for continuous monitoring and updates to ML models in AAL systems, with regular evaluations for accuracy and safety.

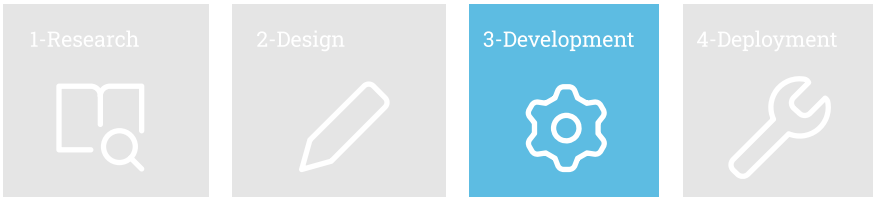
Legal Recommendation

Article 25 of the GDPR, concerning data protection by design implies a constant monitoring of the data processing to ensure reliability and the possibility to intervene properly to minimize risks for the end users.

Source: Mehmood, H.; Kostakos, P.; Cortes, M.; Anagnostopoulos, T.; Pirttikangas, S.; Gilman, E. Concept Drift Adaptation Techniques in Distributed Environment for Real-World Data Streams. Smart Cities 2021, 4, 349-371. https://doi.org/10.3390/smartcities4010021

Security Tests

Phases:



Recommendation:

Conduct regular security testing to identify and address vulnerabilities, protecting AAL systems from breaches and cyberattacks.

Regular security testing helps identify vulnerabilities in the system's machine learning components before they can be exploited. This protects users from potential breaches or attacks, which is crucial for maintaining trust in the system's safety.

Stakeholders:

Cybersecurity Experts | Developers | Regulators | System Administrators

#Risk #Security

#cybersecurity #vulnerability assessment #penetration testing

Example/Scenario Description

Before deploying an AAL system that controls home access and emergency alerts, developers conduct penetration tests and vulnerability assessments. This ensures that the system is resistant to hacking attempts and unauthorized access, protecting the user's sensitive data and physical security.

Q&A

Q. How does security testing protect AAL systems?
A. It identifies vulnerabilities and protects against cyberattacks, ensuring the system is secure and reliable.

Policy Recommendation

Require regular security audits and penetration testing for all AAL systems to ensure they meet high cybersecurity standards.

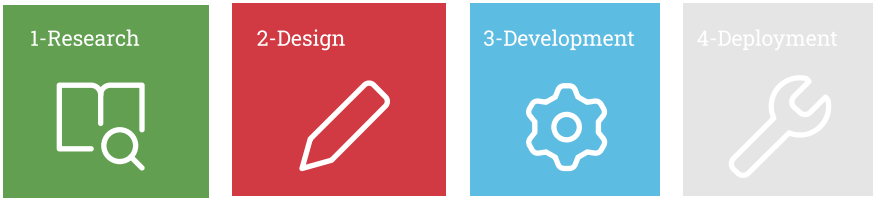
Legal Recommendation

System security is one of the main aspects to ensure the respect of data protection provisions, as per Article 32 and following of the GDPR. Security must be designed properly since from the early stage of the development process. It is important to perform a DPIA (Article 35) to assess what kind of security measure as appropriate, taking into account (Article 32) " the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons".

Source: Touqeer, H., Zaman, S., Amin, R. et al. Smart home security: challenges, issues and solutions at different IoT layers. J Supercomput 77, 14053–14089 (2021). https://doi.org/10.1007/s11227-021-03825-1

Legal Basis

Phases:



Recommendation:

The most suitable legal basis for a data processing must be assessed according to the specific qualities of the service provided, data gathered, contextual framework, and endusers.

When designing any data processing, the correct legal basis should be used to frame this processing. The legal basis must be selected according to the particular data gathering and service provided, meaning that the context is essential to assess the correct legal basis. The key criterion to select the legal basis is to ensure the best protection for the enduser personal data and rights.

Stakeholders:

Developers End Users

#Management #Privacy #Requirement #Context #Legal

#consent

Example/Scenario Description

A developer is creating an interface that requires to gather video image of a private room. The end-user is an older person with dementia. The developer is not sure if the correct legal basis must be consent of the end user or, possibly, relatives. After the assessment of the context, the developer decides that the legitimate interest is the best way to protect the end user because it implies a deeper evaluation of the impacts of the data processing and accountability elements.

Q&A

Q. How can I select the correct legal basis for my data processing among all those listed in Article 6 of the GDPR?
A. Consent should be used when users are actually and substantially empowered and correctly informed with all the necessary elements of the data processing and data lifecycle. If the service involves corollary elements that are not strictly necessary for the basic service, or imply extra-feature requested by the enduser, the contractual legal basis or the legitimate interest may suit. If the service implies mandatory duties (e.g. in medical services), the legal basis may be 6(1) c) (legal obligation), d) (vital interest), or e) (public interest).

Policy Recommendation

Implement recurring tests to constantly varying the robustness of the system and the maintenance of its qualities and features.

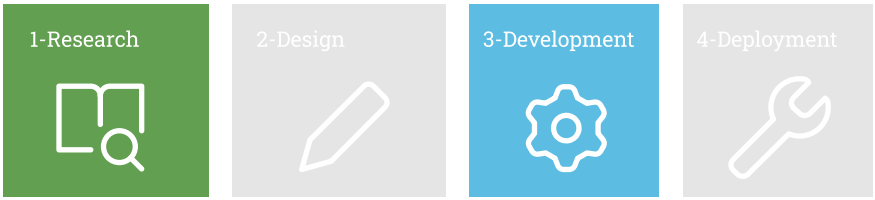
Legal Recommendation

In some instances, legitimate interest (Article 6(1) f) of the GDPR) may better protect both the endusers needs and rights and the data controller's goals because it implies a deeper scrutiny on the impact that the data processing may involve and the mitigation strategies to implement to ensure security and compliance.

Source: European Data Protection Board, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Sensitivity Analysis

Phases:



Recommendation:

Run sensitivity analyses to check the behaviour of the AAL systems.

Before deploying your AAL system, one should check its robustness and reliability in varying conditions. This will ensure the system will perform as expected in real world situations.

Stakeholders:

Developers

#Risk #Sustainability

#sensitivity analysis #robustness #reliability

Q&A

Q. How one can make sure the system is robust enough for real-world deployment?
A. It is essential to assess the robustness of the system under varying usage conditions. Sensitivity analyses and sandbox testing can be effective methods for identifying potential scenarios in which your system may not perform as anticipated.

Policy Recommendation

Implement recurring tests to constantly verying the robustness of the system and the mantainance of its qualities and features.

Legal Recommendation

System security (Article 32 of the GDPR) also imply robustness and proper functioning in all normal, reasonable and plausible conditions. This must be ensured constantly.

Source: Neel Mani, Akhil Singh, Shastri L Nimmagadda, An IoT Guided Healthcare Monitoring System for Managing Real-Time Notifications by Fog Computing Services, Procedia Computer Science, Volume 167, 2020, Pages 850-859, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.03.424.

Sensitivity Analysis

Example / Scenario: Implementing "LifeEase AAL"

Objective: Develop and deploy "LifeEase", an AAL application designed to help elderly individuals manage daily activities, track health indicators, and provide emergency assistance when needed.

1. Development and Initial Deployment:
   - Senior Tech Innovations develops "LifeEase," incorporating features like fall detection, medication reminders, and emergency contact alerts.
   - The system is initially programmed based on general assumptions about user behavior and environment.

2. Deployment Challenges:
   - Following deployment in a senior living community, several issues become apparent:
     - High false alarm rates in fall detection when users perform vigorous activities like physical therapy exercises.
     - Medication reminders occasionally trigger unnecessarily due to slight variations in users' routine schedules.
     - Emergency contact alerts activate inconsistently, depending on minor device placement changes or environmental factors like room lighting.

3. Recognizing the Need for Sensitivity Analysis:
   - Feedback from users, caregivers, and healthcare providers highlights inconsistencies and inaccuracies that decrease the system's reliability and user confidence.
   - The developers recognize that each feature's sensitivity needs to be adjusted to cater to individual variations and environmental factors.

2. Conducting Sensitivity Analyses:

- Senior Tech Innovations performs sensitivity analyses on the system components, including:
  - **Fall Detection**: Evaluating how sensor placement and activity types influence fall detection, identifying factors that lead to false positives and negatives.
  - **Medication Reminders** : Analyzing user behavior patterns to understand how variations in routine affect the timing and frequency of reminders.
  - **Emergency Alerts**: Testing how different environmental conditions and device placements affect the reliability of emergency contact features.

5. Adjustments Based on Sensitivity Findings:

- Based on the analyses:
  - Thresholds for fall detection are adjusted to accommodate various activity levels,
  - minimizing false alarms without compromising safety.
  - Medication reminders are refined to account for allowable deviations in schedules,
  - Emergency alert systems are recalibrated to ensure consistent performance across diverse environmental conditions..

6. Re-Deployment and User Feedback:

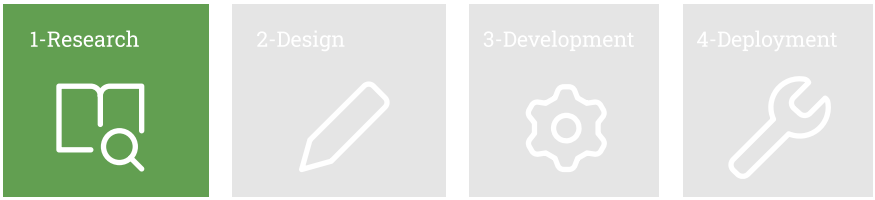
- The refined "LifeEase" system is re-deployed with improved algorithms adjusted to consider varied user and environmental contexts.
- Users report increased trust in the system, citing fewer false alarms, more relevant reminders, and consistent emergency notifications.

7. Ongoing Optimization:

- A continuous loop of feedback and analysis is established, allowing for ongoing calibration and updating of system features based on real-world usage data.

Open Science

Phases:



Recommendation:

Follow open science principles when researching AAL systems

Adhering to open science principles such as open data (FAIR - findable, accessible, interoperable, reusable), code sharing and open access in AAL research increases the quality and reproducibaility of the outputs. It also maximizes knowledge transfer.

Stakeholders:

Developers | End Users | General Public

#Management #Context

#open science #reproducibility #AAL research

Example/Scenario

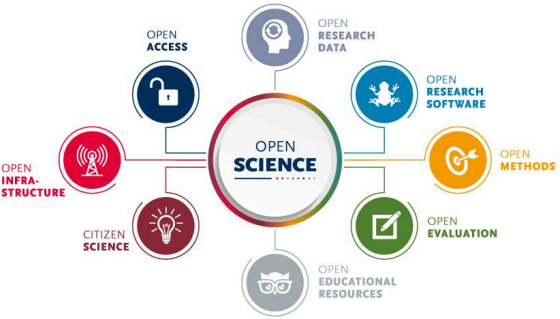


Image source: https://www.uni-potsdam.de/en/openscience/index

Q&A

Q. How can AAL research be more open and reproducible? How can I maximize the outreach of my research?
A. Follow open science and responsible research and innovation practices such as code and data sharing, preregistration, open access publication, multi-stakeholder engagement and public dissemination through social media, podcasts and news venues.

Policy Recommendation

Research funders and university bodies should encourage the application of open science practices in AAL research through incentives, both financial and non-financial. Suitable open science practices include data and code sharing, open access, preregistration and dissemination through public channels such as social media and the news. Coaching of open science in interdisciplinary collaborations should be provided.

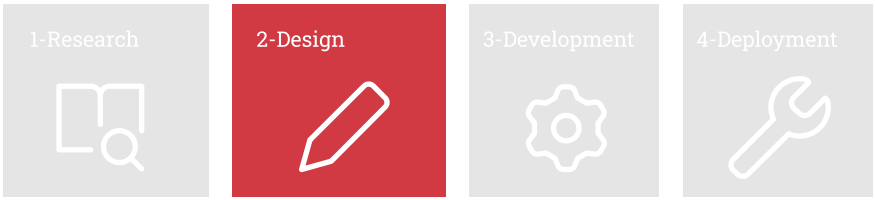
Legal Recommendation

AAL research projects may be performed with benefits of open science and open data, but both personal data protection and intellectual right property must be handled properly, e.g. via synthethic data and creative commons, respectively. Fully anonymized data sharing can occur within existing legal frameworks as long as the highest security and by-design frameworks are respected and implemented.

Source: Isaacowitz, D. M., & Lind, M. (2019). Open science is for aging research, too. Innovation in Aging, 3(4), igz028.10.1093/geroni/igz028.

Users' Consent

Phases:



Recommendation:

Implement clear and user-friendly consent mechanisms that allow users to easily control and understand what data is collected and shared within AAL systems

Designing consent forms that are easy to understand and interactive helps users make informed decisions about their data. This includes providing real-time feedback on which data is being collected and offering easy opt-in/opt-out options for different data types. Dark patterns (e.g., deceptive and complicated consent forms) should be avoided.

Stakeholders:

Designers | Developers | End Users

#Privacy #Context #Legal

#consent #data protection #transparency

Example/Scenario

Description

An AAL system provides an interactive consent dashboard where users can see real-time data collection, categorized by type (e.g., health data, location data) and adjust their consent preferences with simple toggles. Users receive periodic reminders to review and update their settings. The screenshot provides an example from the NHS with accessible visuals.

Image source: https://slideplayer.com/slide/8667585/

Q&A

Q. How can I make user consent management more transparent in AAL systems? Why is consent important in AAL system design?
A. Design a consent management interface that breaks down data categories, explains how each data type will be used, and offers a simple opt-in/opt-out functionality for each.

Policy Recommendation

Incorporate consent dashboards as standard features, enabling users to easily manage their privacy preferences throughout their interaction with AAL systems. Promote awareness of the fact that the binary and one-off consent model is not suitable in the AAL context, and encourage the development of more flexible, customisable, gradual and progressive control systems (e.g., consider engaging with developers to establish (and validate) new consent tools, such as affirmations of consent through gestures).

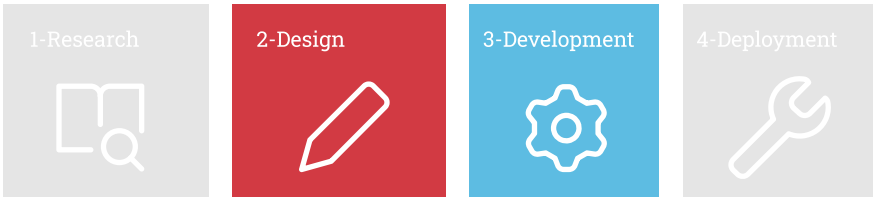
Legal Recommendation

Ensure compliance with consent regulations such as GDPR's explicit consent requirement (Articles 6(1) a) and 7) by making sure users can easily understand and control what data they are sharing and for what purpose.

Source: Ruiz-Casares, M., & Thompson, J. (2016). Obtaining meaningful informed consent: Preliminary results of a study to develop visual informed consent forms with children. Children's Geographies, 14(1), 35-45.

Data Minimizazion Mechanisms

Phases:



Recommendation:

Adopt a data minimization approach by collecting and processing only the data necessary for the AAL system's functionality.

Data minimization helps reduce the risks associated with data breaches and unauthorized access by limiting the amount of personal information collected and processed. This principle - also enshrined in the GDPR - protects user privacy and reduces the burden on system resources, improving performance and compliance with privacy laws.

Stakeholders:

Developers | System Architects | Data Protection Officers

#Security #Requirement #Legal

#data minimization #data protection #compliance

Example/Scenario

Example/Scenario

An AAL system designed to monitor elderly patients' mobility limits data collection to activity levels and location, avoiding unnecessary collection of biometric data or personal identifiers. This ensures that the system functions effectively while maintaining privacy.

Image Source: Image was produced by DALL-E.

Q&A

Q. How does data minimization benefit the development of AAL systems?
A. By collecting only essential data, ideally on a decentralized basis, the system reduces exposure to privacy risks, improves legal compliance (e.g., GDPR), and optimizes system performance.

Policy Recommendation

Developers should follow the principle of data minimization by designing systems that collect and process only the essential data needed for the intended functionality, avoiding the over-collection of personal information.

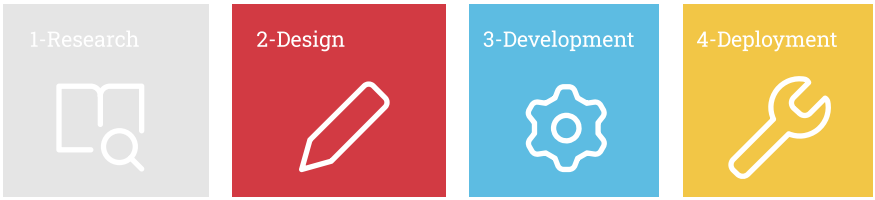
Legal Recommendation

Ensure compliance with data protection regulations (e.g., GDPR Article 5) by implementing data minimization strategies, which help limit liability and reduce the risk of data breaches.

Source: Staab, R., Jovanović, N., Balunović, M., & Vechev, M. (2024, May). From principle to practice: Vertical data minimization for machine learning. In 2024 IEEE Symposium on Security and Privacy (SP) (pp. 4733-4752). IEEE.

Cultural Sensitivity

Phases:



Recommendation:

Adapt AAL systems to the cultural and social preferences of users to enhance usability and social inclusion in real-life settings.

Cultural sensitivity and social factors play a crucial role in the success of AAL systems in everyday environments such as care homes or private homes. Tailoring the interface, communication style, and features of the system to local cultural norms and individual social preferences increases user acceptance, promotes long-term engagement, and reduces feelings of isolation for elderly users.

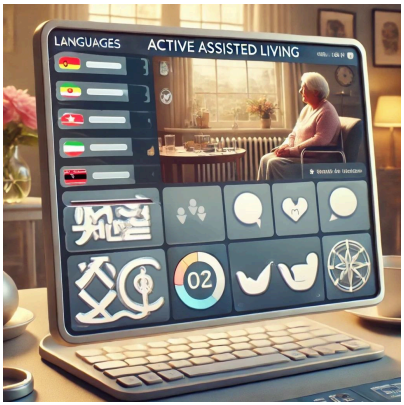
Stakeholders:

Healthcare Staff | Cultural Consultants | End Users

#Governance # Context

#culture #cultural adaptation #social inclusion

Example/Scenario



Example/Scenario Description

An AAL system deployed in a multicultural senior living facility offers customizable language settings, social interaction features, and culturally relevant reminders (e.g., religious events, local holidays). It also connects users with local community groups for shared activities, helping foster a sense of belonging.

Image source: Image was produced by DALL-E.

Q&A

Q. How is it possible to ensure an AAL system adapts to the cultural needs of users? Why is cultural adaptation important in AAL systems?
A. Include customizable settings that reflect cultural preferences, such as language, social communication styles, and culturally relevant content like holidays and events. Engage local cultural consultants to ensure sensitivity.

Policy Recommendation

Ensure that AAL systems are regularly updated to reflect the evolving cultural and social needs of users, incorporating feedback from diverse user groups and local communities.

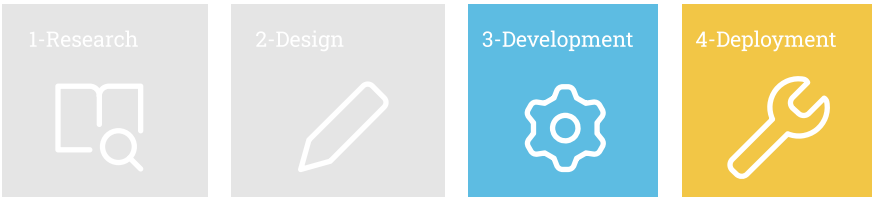
Legal Recommendation

Compliance with accessibility and anti-discrimination laws requires AAL systems to cater to the diverse cultural backgrounds and needs of all users, ensuring fair and equal access to technology.

Source: Lutz C., Miguel C., et al. (2024), Social and societal Issues in AAL. In A. A. Salah, L. Colonna, & F. Florez-Revuelta (Eds.), Privacy-aware monitoring for assisted living: Ethical, legal, and technological aspects of audio- and video-based AAL solutions (chapter 13). Springer.

Bias Audits

Phases:



Recommendation:

Regularly audit and adjust AAL systems to minimize bias in data collection and decision-making processes, ensuring fair treatment for all users.

Bias in AAL systems can arise from the data used or the models and algorithms that process the data, potentially leading to unequal treatment of different user groups (e.g., based on age, gender, ethnicity). Continuous audits and user feedback help address these biases, making the technology more inclusive and ensuring it meets the needs of diverse populations.

Stakeholders:

Data scientists | Developers | End Users

#Governance # Context #Risk

#bias #discrimination #fairness

Example/Scenario Description

An AAL system deployed in a retirement community predominantly recognizes mobility patterns of individuals with certain physical characteristics, leading to less accurate monitoring for individuals with disabilities or atypical movement patterns. Regular bias audits identify and correct this issue, ensuring that the system can more accurately serve all users.

Q&A

Q. How can bias in AAL systems affect users during deployment? What can be done to address bias in AAL systems?
A. Bias can result in unequal treatment of different user groups, leading to errors in monitoring or care and potential downstream harms. This disproportionately affects minorities or those with non-standard physical characteristics. Bias can be reduced through value-sensitive and participatory design.

Policy Recommendation

Mandate the use of periodic audits for bias detection in AAL systems, requiring transparency about the fairness of algorithms and decision-making processes to ensure equitable care for all users.

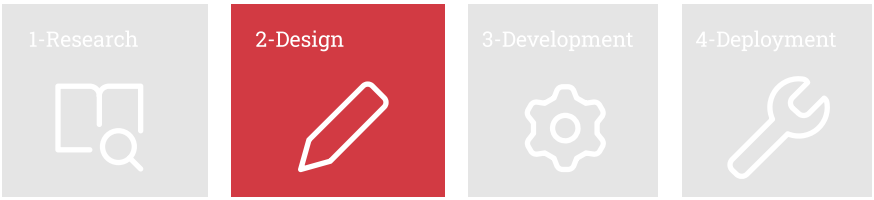
Legal Recommendation

Ensure compliance with anti-discrimination and data protection laws by actively addressing and reducing bias in algorithmic decision-making, holding developers and system operators accountable for fairness in AAL system deployment.

Source: Lutz C., Miguel C., et al. (2024), Social and societal Issues in AAL. In A. A. Salah, L. Colonna, & F. Florez-Revuelta (Eds.), Privacy-aware monitoring for assisted living: Ethical, legal, and technological aspects of audio- and video-based AAL solutions (chapter 13). Springer.

Interoperability and Cooperation

Phases:



Recommendation:

Design products to allow interoperability and cooperation with other devices.

Interoperability and compatibility of devices allow combining them into more tailored smart systems. Thanks to that, users may build a supportive environment they need, and be more satisfied also from your products.

Stakeholders:

AAL Service Providers | Caregivers | End Users

#Requirement # Sustainability

#interoperability #smart environment

Example/Scenario Description

An older person considers buying a fall-detection device. Device of company A is cheaper but cannot be integrated with the devices of the other producers. Device B is more expensive but compatible with various products that the older person may want to buy. Hence, the buyer may prefer a more expensive device B that they can integrate into their smart environment.

Q&A

Q1. What interoperability means?
A1. Interoperability means the ability of different systems and devices to work together seamlessly and exchange data.

Q2. How to ensure interoperability?
A2. Identify what devices could potentially cooperate with the product, and design it in a way enhancing such cooperation.

Policy Recommendation

Require interoperability of devices founded through public programmes.

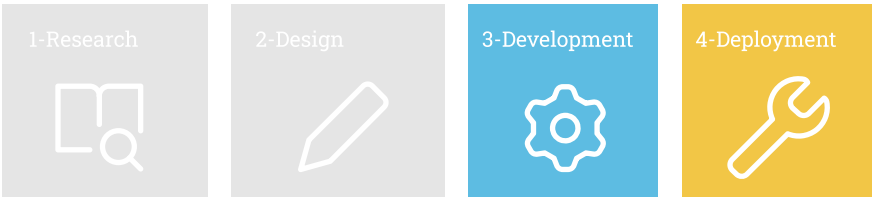
Legal Recommendation

Set up standards of data encryption that would allow seamless exchange of data between of devices used in care and smart homes.

Source: Kuźmicz M. M., (2024), What Should we Care About in AAL? Unveiling the Main Interests of the Users in the Legal Context, 2024 IEEE 18th International Conference on Automatic Face and Gesture Recognition (FG), Istanbul, Turkiye, pp. 1-9, doi: 10.1109/FG59268.2024.10582034.

Liability

Phases:



Recommendation:

Have a clear liability policy.

In case of harm or damage, it is vital to have a clear liability policy stating who is liable, to which extend, and what is the procedure of claiming damages. That can build trust in a provider and their products.

Stakeholders:

Healthcare Staff | Caregivers | End Users

#Risk # Legal

#liability #safety

Example/Scenario Description

An older person considers buying AAL system. Company A offer a product with more functions, and for a slightly lower price. However, company B explains clearly in which circumstances the company will pay damages, and they have easily accessible system of claiming damages. An older person may prefer company B because they will feel reassured by the clear rules.

Q&A

Q1. Should one have liability policy when there is law regulating that aspect?
A1. Law is not always easily accessible to clients. If legal rules are properly translated into a clear liability policy, clients will be more aware of the rules.

Q2. Should one accepting more liability than required by the law?
A2. Accepting more liability may build trust in the service and the product, especially in case of new products like AAL. That can increase profits which will be higher the potential liability costs.

Policy Recommendation

Promote code of conducts that include clear liability rules phrased in a user-friendly manner.

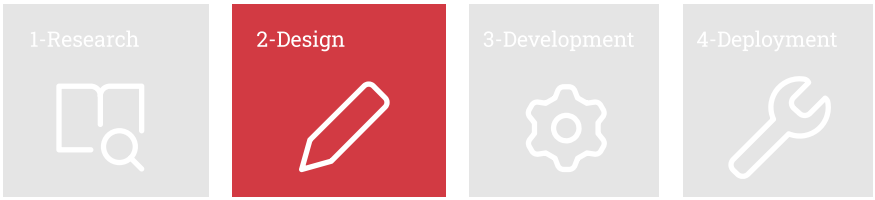
Legal Recommendation

Introduce clear liability rules in the Terms & Conditions, which are crucial for AAL users as they enable them to identify from whom they can claim remedies.

Source: Kuźmicz M. M., (2024), What Should we Care About in AAL? Unveiling the Main Interests of the Users in the Legal Context, 2024 IEEE 18th International Conference on Automatic Face and Gesture Recognition (FG), Istanbul, Turkiye, pp. 1-9, doi: 10.1109/FG59268.2024.10582034.

Customization

Phases:



Recommendation:

Enable customized privacy protection.

AAL systems should allow for privacy-relevant modalities to be changed easily by the user. For instance, the recording should be adopted to specific hours, one should be able to change types of data that recorded and whether the recording occurs locally or remotely, and one should be able to alter how data analysis is run.

Stakeholders:

AAL Providers | Designers | Developers

#Privacy #Context

#personalization #privacy assistance #tailored protection

Example/Scenario Description

Identify what variants or options can be provided (e.g., data storage on local device rather than external). Explain to the user the changes in modalities depending on how they chose that their data is being recorded and analyzed. Enable interoperability to change among different options easily. Test the system with users.

Q&A

Q. What design choices does one have to make products and services of AAL more customizable?
A. It can be adopted the duration of the recording and timing of it; one can adopt where data is stored and who has access to it, or can adopt the means that users are provided with e.g., to delete their data.

Policy Recommendation

Consider how to ensure a data economy that is human-centric and breaks from take it or leave it situation that many users are facing when interacting with smart devices. The debate must focus on how a right to customization of products and a right to repairing privacy-invasive services could benefit regulatory goals.

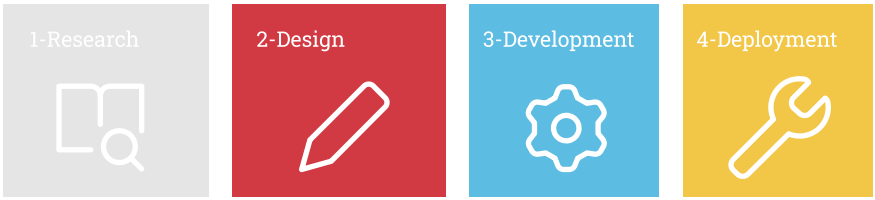
Legal Recommendation

Build upon the concept to privacy by design and GPDR norms of data protection by design and default to further empower individuals to enable an AAL environment that is respectful of individual and contextual privacy needs.

Source: Tamò-Larrieux A., Zihlmann Z.,et al. (2021), The right to customization: conceptualizing the right to repair for informational privacy. In Annual Privacy Forum, pp. 3-22. Cham: Springer International Publishing https://2021.privacyforum.eu/images/2021-06-17-aureliazairakimsimon-apf-righttocustomization_final.pdf
Kollnig K., Datta S., et al. (2023). We are adults and deserve control of our phones': Examining the risks and opportunities of a right to repair for mobile apps, Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, pp. 22-34, https://doi.org/10.1145/3593013.3593973

System's Competency

Phases:



Recommendation:

Consider the data input for AAL systems to maximize competent decision-making.

AAL systems may be biased against certain demographics and user groups, either due to data biases (i.e. biases in model training), or due to algorithmic biases (i.e. usage of algorithms not suited for certain groups). Examples are systems are those that do not work well with specific ethnicities, or with people who are missing limbs, or have certain bodily characteristics. To avoid such issues, the data input should be analyzed thoroughly to ensure competent decisions to be made.

Stakeholders:

Designers Developers

#Governance #Requirement

#competency #accuracy #input data

Example/Scenario Description

In interdisciplinary groups think about the underlying functions of AAL product/service and the data input needed for the functioning. Evaluate the input data and its accuracy not only in terms of correctnes but in terms of whether competent decisions are rendered. Test the AAL according to defined objectives.

Q&A

Q. What is the relationship between the input data and the output that is triggered (AAL decision making)?
A. The answer to this question should enable developers and designers to critically reflect about what data is being processed and how this data is needed for a specific AAL service. How can it be ensured that the data is accurate (i.e., correct) and useful for the system to perform its service, (i.e. competent)

Policy Recommendation

Focus on the overall competency of an AAL system.

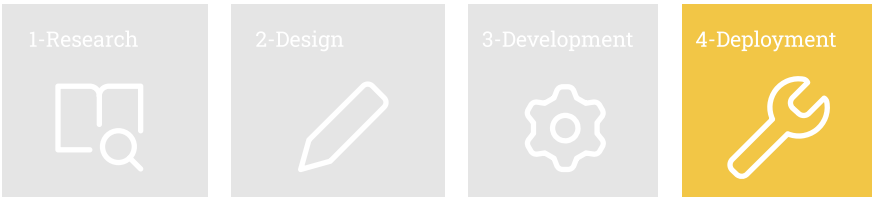
Legal Recommendation

The legal principle of data accuracy could be interpreted more broadly to reflect the competency of a system.

Source: Tamò-Larrieux A. (2021), Decision-making by machines: Is the 'Law of Everything'enough?. Computer Law & Security Review, 41, https://doi.org/10.1016/j.clsr.2021.105541

Data Accessibility

Phases:



Recommendation:

Ensure ability to provide real-time access to data processed by the AAL system.

With new data regulations emerging in the European Union (e.g. the Data Act), more data access rights will emerge that AAL developers will need to take into account. Best practices should include giving more transparency about the volume of data processed, the ability of storing said data locally, and ensuring real-time access rights to data where possible.

Stakeholders:

End-users | Manufacturers | Service Providers

#Governance #Requirement

#data access

Example/Scenario Description

The Data Act is a new regulation and part of the broader EU Data Strategy. This regulation defines data access rights between businesses (B2B) and between businesses and consumers (B2C), outlines guidelines for fair data contracts, and addresses business-to-government (B2G) data sharing in exceptional cases.

Q&A

Q. Are AAL systems ready to be compliant with the new Data Act?
A. Ensure that transparency provisions get updated to include new information on data volume, data granularity, processing operations, and real-time access to data for users.

Policy Recommendation

Ensure that the system enables customisations, i.e., different services. Raise awareness about the consequences of non-compliance and pinpoint how compliance can be enforced and where to lodge formal complaints.

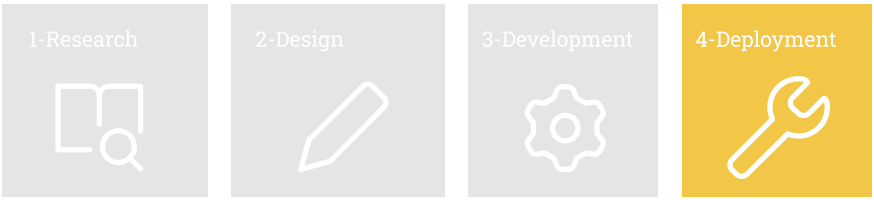
Legal Recommendation

Ensure compliance with upcoming regulations; screen for upcoming regulations and consider their impact on AAL.

Source: Hennemann M., Ebner G. K. Et al., (2024), Data Act: An Introduction, Nomos E-Library, doi.org/10.5771/9783748918691

Policy Implementation

Phases:



Recommendation:

Develop a policy brief for implementing trustworthy AAL systems.

Trustworthy AAL leads to more usage of ICT which can benefit the active and healthy lives of citizens and supports evidence-based policymaking.

Stakeholders:

Policymakers | Decision Makers

#Management

#technology #evidence-based #policymaking

Example/Scenario Description

A specific evidence-related area in policy is policy-making on science- or technology-related issues, such as artificial intelligence. Technology that is entrenched in daily lives gives rise to a wide range of policy issues, including on safety, privacy, security, ethics and the environment.

Q&A

Q. How does one know if information from technology is trustworthy?
A. If the offered information includes a link to the original source or provides additional (science-backed) evidence, it is worth following up on these resources to make an informed decision.

Policy Recommendation

Facilitate the development of trustworthy ICT via the implementation of specific policies for the different stages of the service.

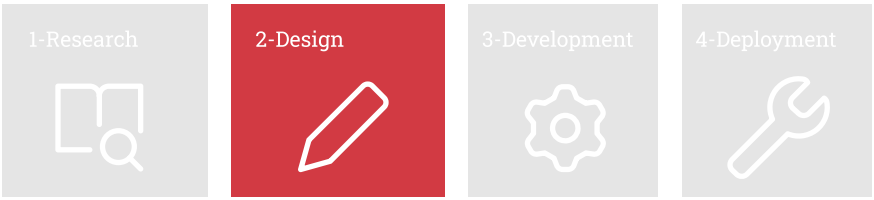
Legal Recommendation

Arrange that the source of information is always transparent and accessible, in accordance with the general GDPR provisions and the duty of information towards end users.

Source: Euopean Parliament. Briefing: Evidence for policy-making Foresight-based scientific advice. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690529/EPRS_BRI(2021)690529_EN.pdf

Organisation and Management

Phases:



Recommendation:

Promote an organisational culture of ethical design and development of AAL products and services.

R&I organisations should implement processes and procedures that ensure ethical issues related to the design and development of AAL products and services are fully analysed, debated and addressed on the daily working flows. To such aim, IT companies and research organisations' managers should have access to comprehensive guidelines and tools.

Stakeholders:

IT Companies | R&I Organisations

#Context

#ethical management #organisational processes #ICT ethics

Example/Scenario

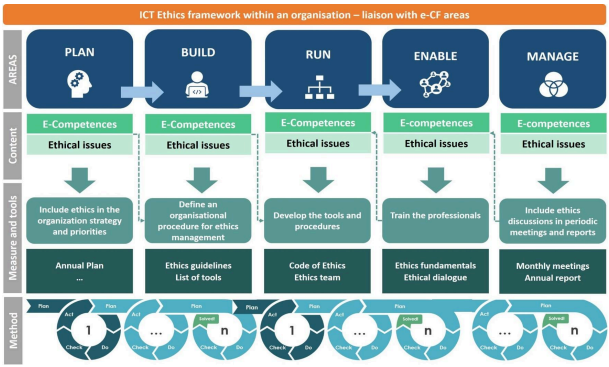


Image source: https://www.ict-ethics.eu/

Q&A

Q. Why the ethical challenges related to a specific solution must be considered before developing it?
A. The AI Act requires to perform a "Fundamental Rights Impact Assessment" (FRIA) before developing AI systems in order to evaluate both the potential legal and ethical impacts on end-users. This must be done along with the Data protection Impact Assessment. These assessments eventually benefit the design and the trustworthiness of the system.

Policy Recommendation

Provide IT companies and organisations with tools that allow developers and researchers to acknowledge and understand older adult's concerns and, in multidisciplinary teams, find ways to overcome those challenges.

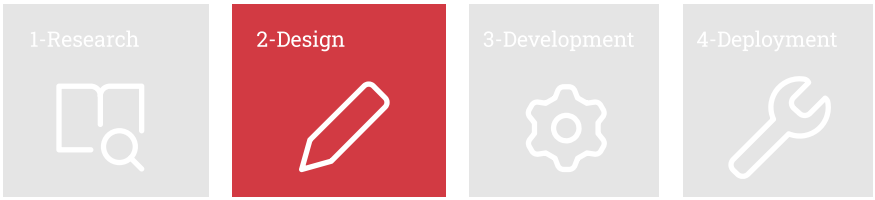
Legal Recommendation

Implement Code of Conducts for ethics in the development of AAL products and services for the request of specific certifications, such as for the Medical Device Regulation.

Source: Cen/TS 17834:2022 - European professional ethics framework for the ICT Profession (EU ICT Ethics). iTeh Standards. https://standards.iteh.ai/catalog/standards/cen/8fac874b-55c9-419d-b6f2-ac0b79e193eb/cen-ts-17834-2022

Procedural Compliance

Phases:



Recommendation:

Prepare Software Bill of Materials.

A Software Bill of Materials (SBOM) is a formal record containing details and supply chain relationships of components included in the software. It aids developers, manufacturers and users in identifying, tracking, and mitigating existing and emerging vulnerabilities and risks.

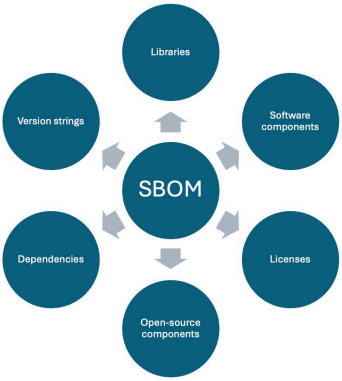
Stakeholders:

Developers | Manufacturers

#Security

#SBOM #security by design #cyber resilience act

Example/Scenario



Example/Scenario Description

Under the Cyber Resilience Act, manufacturers must identify and document product components and vulnerabilities, creating an SBOM that includes at least the top-level dependencies. While the SBOM does not need to be publicly available, it should be included in the technical documentation and provided to market surveillance authorities upon request.

Q&A

Q. Is an SBOM a legal requirements?
A. Yes, the EU Cyber Resilience Act mandates the adoption of SBOMs to improve cybersecurity and ensure transparency in software and hardware supply chains, requiring manufacturers to create SBOMs for their products.

Policy Recommendation

Provide recommendations about how the software build process can be adapted to streamline the generation of SBOMs.

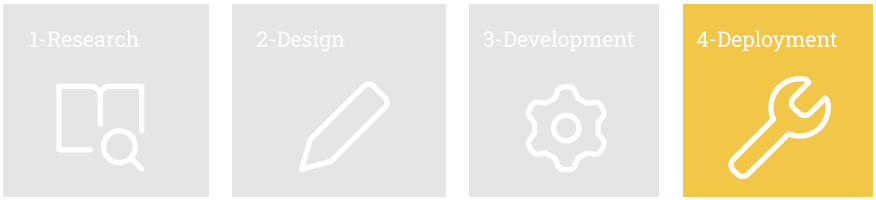
Legal Recommendation

Provide support and resources for OSS contributors and SMEs to comply with SBOM requirements.

Source: Carmody S., Coravos A., et al. (2021), Building resilient medical technology supply chains with a software bill of materials, npj Digit. Med. 4, 34, 10.1038/s41746-021-00403-w

Processing User Data

Phases:



Recommendation:

Inform AAL users about their data processing in understandable way.

Users prefer short documents with clearly divided sections that include narrative explanations, examples, numerical labels and graphics. Furthermore, Articles 13 and 14 of the GDPR require to provide users with comprehensive information regarding data proccesing.

Stakeholders:

End-users | AAL Service Providers | Healthcare Staff | Caregivers | Designers | Policymakers

#Privacy

#data processing #GDPR, video-based AAL #information obligation

Example/Scenario

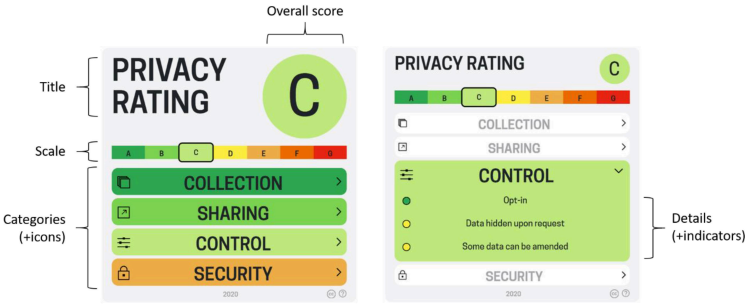


Image source: Barth S., Ionita D., et al. (2021)

Q&A

Q1. How can understandability be improved?
A1. Use plain language, avoid technical or legal terms. Give examples, use tables and other visuals. Provide comprehensive information about the data processing and how specific data are processed.
Q2. Are graphic forms GDPR complaint?
A2. Yes, Article 12(7) of the GDPR allows use of icons.

Policy Recommendation

Reduce legal jargon and write legislation in clear, logical sentences. Follow and pursue guidelines that are pushing for more precise legislation, such as initiatives that look into making legislation 'digitally ready'. When communicating with the end-user, use visualisations or audio-visual tools to explain rights and obligations.

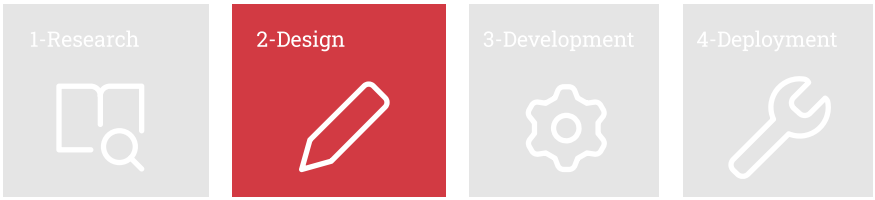
Legal Recommendation

Promote use of numerical labels and graphics by introduction of standardised icons that would meet the requirement of Article 12(7) of the GDPR. End-users should be able to access, in a clear and understandable way, information regarding the collection of data, the type of data the purpose(s) of the data processing, the storage and life-cycle (how long data are stored), and if there exist automated deicisons based on those data processing.

Source: Barth S., Ionita D., et al. (2021), Privacy Rating: A User-Centered Approach for Visualizing Data Handling Practices of Online Services, IEEE Transactions on Professional Communication, 64, 4, pp. 354-373, 10.1109/TPC.2021.3110617 - London Economics, and Ipsos. 2015. Consumer testing study of the possible new format and content for retail disclosures of packaged retail and insurance-based investment products – Final Report. MARKT/2014/060/G for the implementation of the Framework Contract no EAHC-2011-CP-01 https://ec.europa.eu/info/sites/default/files/consumer-testing-study-2015_en.pdf. Kuźmicz, M. M. (2023). Multilayer Information Obligation, and Why We Need It. The Journal on Technology and Persons with Disabilities, 43..

Audit and Control

Phases:



Recommendation:

Perform adequate controls, safeguards and audit trails for data and images gathered / stored / shared.

Ensuring privacy and confidentiality are maintained. Helping build trust among people who are the 'beneficiaries' of surveillance technologies.

Stakeholders:

End-users | AAL Service Providers | Patients | Designers | Developers

#Privacy

#privacy #trust #data

Example/Scenario Description

In the case of using camera devices to monitor activity (e.g., to look at mobility, gait, etc), consider using edge computing to store information (unless specific circumstances arise) and ensure the information deletion after a set period.

Q&A

Q. How can be ensured the necessary 'wrap around' care for the most vulnerable of people?
A. This is actually a choice that end users must have: they must be empowered and involved within the development process.

Policy Recommendation

Technology developers need to involve users in the design and implementation of audio- and video-based smart monitoring systems.

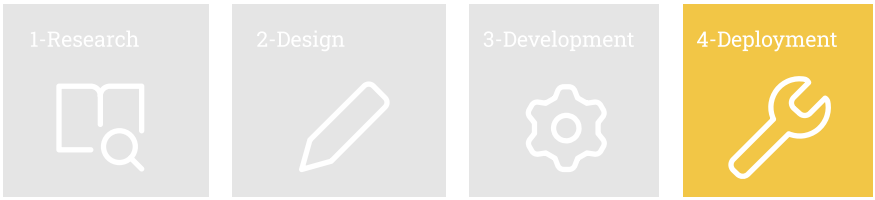
Legal Recommendation

Ensure that the proper legal basis (e.g. consent) is acquired properly and validly: consent must be informed, specific, unambiguous and free. All these elements are required to have a valid and lawful consent.

Source: Makri, EL., Lambrinoudakis, C. (2015). Privacy Principles: Towards a Common Privacy Audit Methodology. In: Fischer-Hübner, S., Lambrinoudakis, C., López, J. (eds) Trust, Privacy and Security in Digital Business. TrustBus 2015. Lecture Notes in Computer Science(), vol 9264. Springer, Cham. https://doi.org/10.1007/978-3-319-22906-5_17

Digital Education and Training

Phases:



Recommendation:

Develop an online training session for stakeholders to recognise, analyse and apply AAL.

Developing an online training session for stakeholders helps equip them with the skills to identify, and utilize AAL technologies. This ensures that individuals can make informed decisions about the reliability and ethical implications of AAL solutions, improving both adoption and user safety.

Stakeholders:

End-users | Educators | Citizens

#Context

#training #digital skills

Example/Scenario

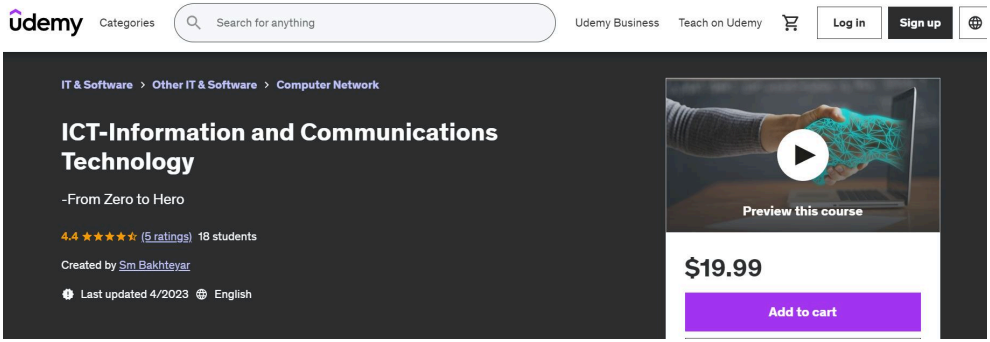


Image source: https://www.udemy.com/course/ict-armf/?couponCode=MTST7102224B2

Q&A

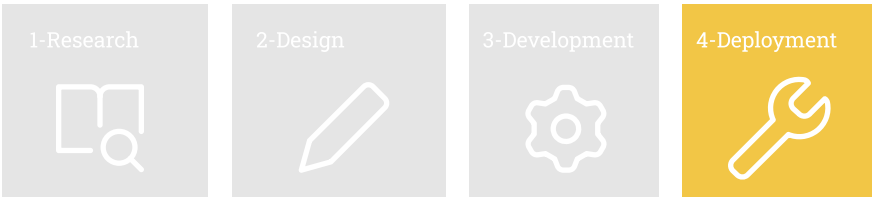
Q. How can trust in AAL be enhanced?
A. By improving awareness and digital education via dedicated training sessions specifically directed to AAL stakeholders.

Policy Recommendation

Provide both technical and pedagogical training to caregivers, so they can explain how to use the AAL technology to the end-users, simply and effectively. Raise awareness about online privacy implications and regulations. Implement long-term and regular digital education.

Datasheets for AI Models

Phases:



Recommendation:

Create datasheets to enhance transparency, accountability, and trust in AI systems by guaranteeing that detailed and clear documentation supports every stage of AI model development and deployment.

Creating datasheets for AI datasets helps address the lack of industry standards by documenting key aspects such as motivation, composition, and recommended uses. This practice enhances transparency, reduces bias, and improves reproducibility, allowing researchers to make more informed decisions when selecting datasets.

Stakeholders:

End-users | Legal Teams | Product Managers | Security Experts | Project Managers | Data Scientists | Ethics and Compliance Officers | Developers

#Risk

#datasheets #data cards #dataset nutrition labels #data statements

Example/Scenario

Image source: Adapted from Timnit G., Morgenstern J., et al. (2021)

Q&A

Q. How do datasheets ensure transparency and accountability?
A. Datasheets ensure transparency and accountability by providing, for example, comprehensive, clear documentation on the AI model's development, data sources, performance metrics, bias mitigation, ethical considerations, and usage guidelines.

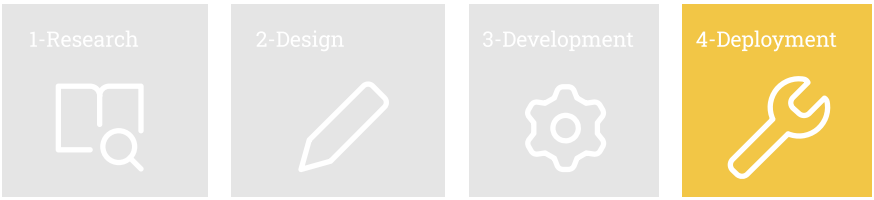
Policy Recommendation

Mandate the inclusion of standardized datasheets for all AI models. Implement ISO standards.

Source: Timnit G., Morgenstern J., et al. (2021), Datasheets for Datasets, Communications of the ACM, 64,12 https://doi.org/10.1145/3458723

Security Risks

Phases:



Recommendation:

Developers should address the security risks that can rise in every life stage of AAL components and systems (e.g. Beginning-of-Life, Middle-of-Life and End-of-Life stages).

Developers must proactively address security risks at each lifecycle stage of AAL components and systems—Beginning-of-Life, Middle-of-Life, and End-of-Life—to ensure the ongoing integrity, confidentiality, and availability of sensitive data and functionalities. This comprehensive approach minimizes vulnerabilities and enhances the overall resilience of AAL systems against potential threats throughout their operational lifespan.

Stakeholders:

Component Manufacturers | System Vendors | Developers | Policymakers

#Security

#security measurements #entire life cycle #security by design #privacy by design #secret and personal data management

Example/Scenario

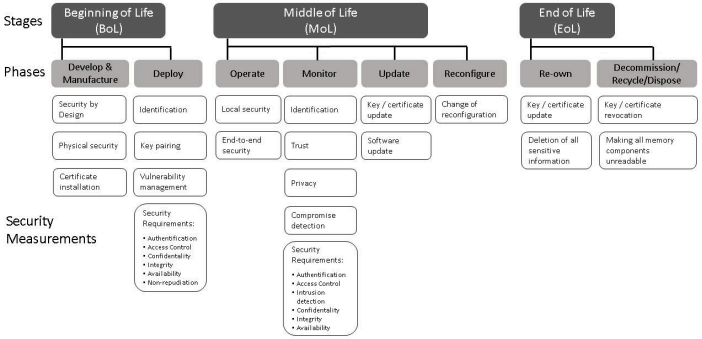


Image source: Adapted from https://doi.org/10.1016/j.jnca.2020.102779

Example/Scenario Description

During the development process, the security-by-design principle should be followed. Within the entire Middle-of-Life (MoL) stage that includes the operation and maintenance, an efficient monitoring of the entire system should be used to detect, identify and resist any attack that could compromise the security of the system or influence the privacy and trust of users. Once the system reaches the end-of-life (EoL) stage all sensitive information such as secret or personal data should be effectively erased or overwritten from the devices.

Q&A

Q. How to ensure a certain level of security and privacy protection over the entire life cycle of AAL systems?
A. Security must be properly planned for every stage of the design, development, and management process and life-cycle of the data and models involved.

Policy Recommendation

Implement and adopt recommendations, guidelines, and standards for security and privacy protection over the entire system's life cycle.

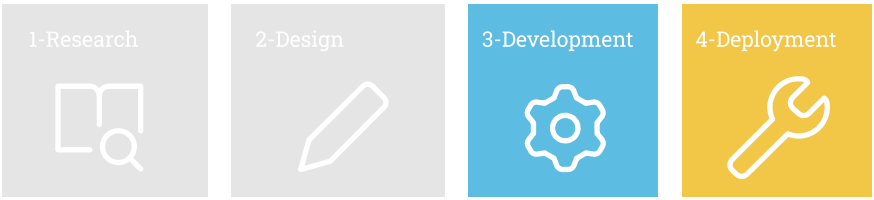
Legal Recommendation

System security (Article 32 of the GDPR) must be implemented in any stage of the data processing and all the staff should be trained to comply with the security requirements.

Source: Yousefnezhad N., Malhi A., et al. (2020), Security in product lifecycle of IoT devices: A survey. Journal of Network and Computer Applications, 171, 102, 779. https://doi.org/10.1016/j.jnca.2020.102779.

AI Model Deployment Records

Phases:



Recommendation:

The performance of any AI-powered application should be monitored after deployment in production. Periodic benchmarking and retraining steps may be useful.

After deploying an AI-powered system, continuous performance tracking is essential because models may degrade or encounter "concept drift" when data patterns evolve over time. Periodic benchmarking and retraining on fresh data allow the system to maintain optimal accuracy and adapt to changing real-world conditions, ensuring long-term reliability.

Stakeholders:

Developers Maintainers

#Risk

#in-production monitoring #concept drift #data drift #AI traceability

Example/Scenario

Example/Scenario Description

The performance of a machine learning model can decline over time without regular intervention, making model monitoring a crucial aspect of any production ML system. When a model's predictions begin to falter, it's important to identify the cause, which often stems from data quality issues, data drift, or concept drift.

Image Source: https://www.iguazio.com/questions/what-is-the-difference-between-data-drift-and-concept-drift/

Q&A

Q. Have tools to monitor the performance of AI-powered system been put in place?
A. The performance of the system and its applications must be carefully monitored along the whole process and life stage.

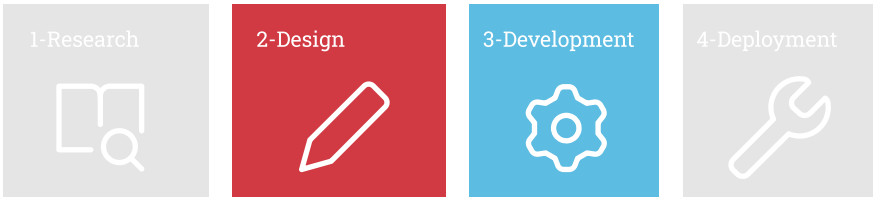
Policy Recommendation

Provide ICT companies and healthcare organisation managers with access to comprehensive guidelines and tools that allow them to implement ethical excellence processes and procedures adapted to their specific needs (e.g., CEN/TS17834:2022 European Professional Ethics Framework for the ICT Profession). Training should be complemented with communication materials written in accessible terms.

Source: Webb G.I., Hyde R., et al. (2016), Characterizing concept drift. Data Min Knowl Disc 30, 964–994. https://doi.org/10.1007/s10618-015-0448-4

Older Adults

Phases:



Recommendation:

Ensure that the user interface is usable and useful to older adults, especially considering potential cognitive declining or dementia.

By prioritizing accessibility and simplicity, developers can enhance the user experience and support the needs of this demographic effectively.

Stakeholders:

Caregivers | Patients | Developers | Healthcare Staff | End-users

#Requirement #Sustainability

#low digital skills #dementia #cognitive decline #user-friendly

Example/Scenario Description

Make sure that the product is user-friendly also for the aging population with cognitive decline. Consider possible challenges of using a touch screen (mobile application) or several buttons to push, and develop a product that does not depend on technical skills of the end-user (passive technology).

Q&A

Q. What to be aware of when designing technology for people with cognitive decline/dementia?
A. Avoid complicated technology that includes the use of mobile applications, other touch screen and buttons to push.

Policy Recommendation

Higher consideration of the aging population and people with cognitive decline/dementia with low digital and technical knowledge. Healthcare units overseeing management of ethical medical principles, such as autonomy, should produce means ofcommunication (e.g., short videos or brochures) to reach relatives of older people, and managers of facilities. These means need to describe, in accessible terms, the importance of safeguarding the relevant principles when implementing and using audio- and video-based AAL systems. This can include showing how the technology works, how privacy by-design approaches have been incorporated into the technology and how one can stop using the technology.

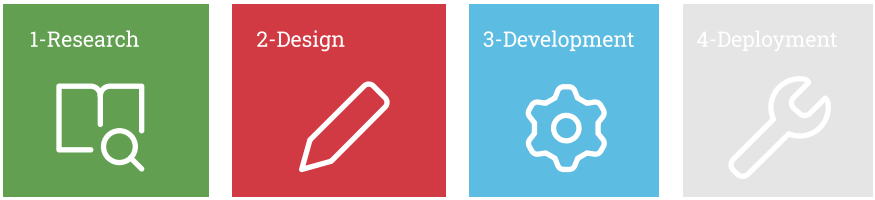
Legal Recommendation

In order to be valid, consent must be gathered from people that are capable of intend and act. When dealing with people with potential dementia or diminished cognitive abilities, it is important to assess (ex-ante) the proper legal basis to perform a valid data processing and if user consent can be an option or not. It may be considered to use an alternative legal basis (Article 6 of the GDPR) and/or to involve relatives.

Source: Puaschitz N.G., Jacobsen F.F., et al. (2021), Factors associated with access to assistive technology and telecare in home-dwelling people with dementia: baseline data from the LIVE@Home.Path trial. BMC Med Inform Decis Mak 21, 264. https://doi.org/10.1186/s12911-021-01627-2
Puaschitz N.G., Jacobsen F.F., et al. (2023), Access to, use of, and experiences with social alarms in home-living people with dementia: results from the LIVE@Home.Path trial, Front. Aging Neurosci., Sec. Alzheimer's Disease and Related Dementias, 15. https://doi.org/10.3389/fnagi.2023.1167616

Dealing with Biases

Phases:



Recommendation:

Anticipate and investigate sources of bias.

AAL systems may be biased against certain demographics and user groups, either due to data biases (i.e. biases in model training), or due to algorithmic biases (i.e. usage of algorithms not suited for certain groups). Examples are systems are those that do not work well with specific ethnicities, or with people who are missing limbs, or have certain bodily characteristics.

Stakeholders:

Developers

#Programming Bias

#data processing #algorithmic bias #data bias #demographics

Example/Scenario Description

1. Identify subpopulations at risk in the available data.

2. For each subpopulation, and in isolation, determine the best performance that can be achieved with the machine learning model of choice. Decide whether it is acceptable or not.

3. Investigate why the model performs so poorly on the adverse distributions (insufficient data, inadequate model, etc.) until obtaining an acceptable performance.

4. Deploy the system on an experimental basis in order to collect more data. Sample the examples with the lowest accuracy in order to determine whether we missed a subpopulation at risk. If one is found, add the vulnerable subpopulation to the initial data and repeat all the steps.

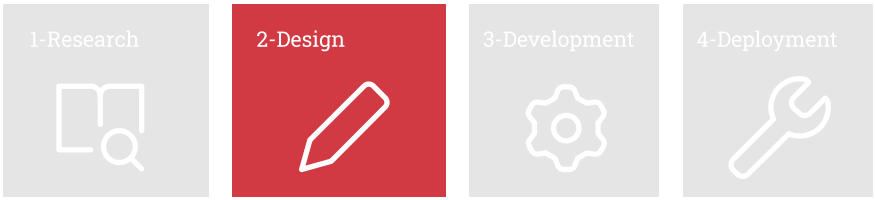
Policy Recommendation

Bias can be tempered by selecting data carefully, considering their quality, relevance, and distribution. Having an external audit to assess the potential emergence of critical biases may help to avoid biased results.

Source: Słowik A., Bottouhttps L. (2021), Algorithmic Bias and Data Bias: Understanding the Relation between Distributionally Robust Optimization and Data Curation, arXiv:2106.09467 [cs.LG] https://doi.org/10.48550/arXiv.2106.09467

Privacy Labels

Phases:



Recommendation:

Use clear and accessible user-interface elements and language for reviewing & managing personal data collected by a system.

Make developers consider data protection by design and default techniques at different system levels to achieve data protection goals in an accessible way (e.g., using privacy nutrition labels).

Stakeholders:

Developers | Designers | End-users

#Privacy

#privacy-by-design #privacy labels

Example/Scenario

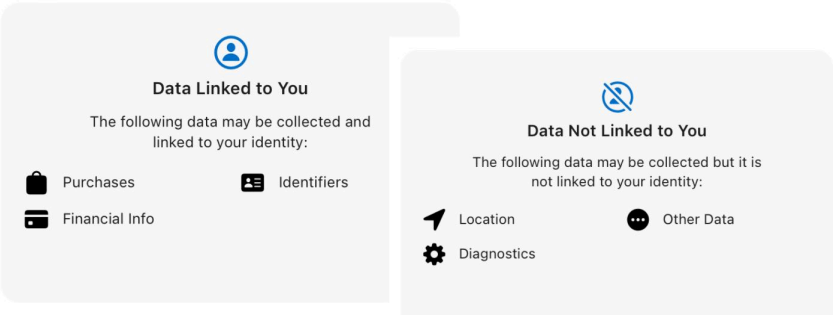


Image source: https://www.apple.com/privacy/labels/

Q&A

Q. What are my options for making privacy accessible for users?
A. Current research recommends using privacy nutrition labels to summarize the collected data by the system.

Policy Recommendation

Encourage developers and designers to divide each system into a meaningful set of design elements (e.g. user interface controls) for reviewing and managing users' personal data within and beyond the scope of the designed system and to use clear and accessible language for information dissemination to understand potential privacy risks and consequences.

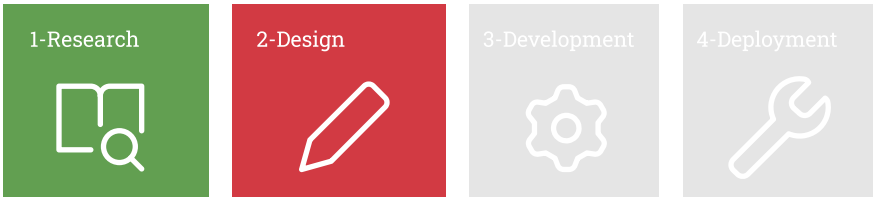
Legal Recommendation

Ensure compliance to the (inter)national data protection regulations: e.g., General Data Protection Regulation (GDPR), e-Privacy Directive, e-Privacy Regulation and established industry practices, e.g., Fair Information Principles.

Source: Kelley, J. Bresee, L.F. (2009), A "nutrition label" for privacy, SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security, Article No.: 4, pp. 1 - 12, https://doi.org/10.1145/1572532.1572538

Stakeholder Identification

Phases:



Recommendation:

Identify all relevant stakeholders of your product.

Proper design and commercial success of AAL product depends on accommodating interests of all relevant stakeholders. To identify these interests and needs, one must recognize the specific stakeholders.

Stakeholders:

AAL providers | Designers

#Requirements

#stakeholders #inclusion #participatory design #needs

Example/Scenario

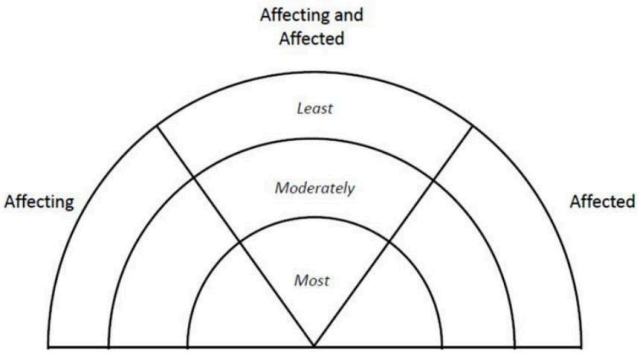


Image source: Chevalier, J. M., & Buckles, D. J. (2008). SAS2: A guide to collaborative inquiry and social engagement https://doi.org/10.4135/9789351507734

Example/Scenario Description

A rainbow diagram for classifying stakeholders according to the degree they can affect or be affected by a problem or action.

Q&A

Q1. Who is stakeholder?
A1. Individuals and organizations that may be affected by your product, or may affect it.

Q2. What are typical AAL stakeholders?
A2. Usually, there are: older adults, formal and informal caregivers, producers of AAL, families of the older adults.

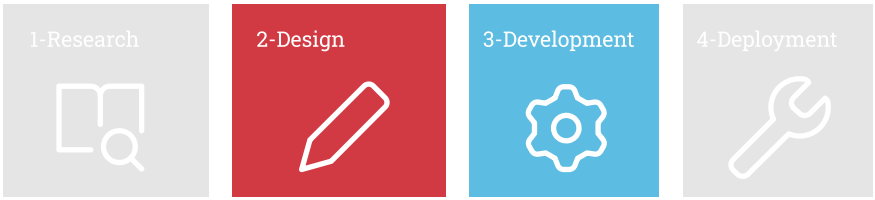
Policy Recommendation

Adopt and promote use of a single AAL stakeholder taxonomy, based on research.

Source: Kuźmicz, M. M. (2024), Who Should We Care About in the Digital World? Challenges of Stakeholders' Identification – The Case Study of AAL. In H. Matsumi, et al. (Eds.), Data Protection and Privacy. Ideas That Drive Our Digital World (Vol. 16). essay, Bloomsbury Publishing.

Sensitive Content

Phases:



Recommendation:

Have clear policy on protection of users' initmacy.

One of the main concerns of the users is that they intimate images would be seen. It is important to have clear policy on what you consider as intimate image, and what means do you apply to protect access to them.

Stakeholders:

End-users

#Intimacy

#nudity #privacy #intimate images #sensitive information

Example/Scenario

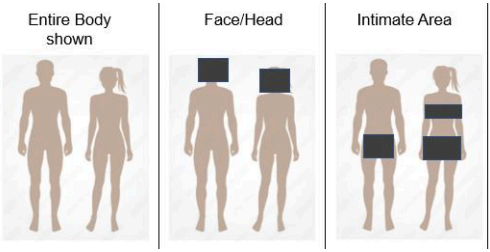


Image source: Maidhof, C., Hashemifard, et al. (2022)

Example/Scenario Description

Different levels of nudity may be considered as resulting in the lost of intimacy. Some people may consider image presenting them naked but with face/head or intimate areas covered as acceptable.

Q&A

Q1. When an image is intimate?
A1. Many situations may be concerned as intimate, for example, when a person is naked, using bathroom, or is engaged in sexual activity.

Q2. Is there a legal definition of intimate picture?
A2. Currently, there is no harmonised legal definition of intimate picture in the EU.

Policy Recommendation

Provide guidelines on what constitute inmate pictures based on the cultural and social norms.

Legal Recommendation

According to the principle of data minimization (Article 5(1) c) GDPR) the data controller must minimize the use of data and, so, the exposure and impact on freedom and liberties of the subject. This implies to apply the most effective tools of protection (e.g. obfuscation, anonymization) for those information that are most sensitive, in balance with the needs related tot he purpose of the data processing (e.g. patients must be recognisable to ensure prompt rescue in emergency cases).

Source: Maidhof, C., Hashemifard, et al. (2022), Underneath your clothes: A social and technological perspective on nudity in the context of Aal Technology, Proceedings of the 15th International Conference on PErvasive Technologies Related to Assistive Environments. https://doi.org/10.1145/3529190.3534733