Identity Valley®

DRG4 FOOD

DRG PLAYBOOK

a digital responsibility guide for software development

Prepared for

DRG4FOOD

v0.3 (2024)

www.identityvalley.org | www.drg4food.eu | Mail : info@identityvalley.org

Funded by the European Union

Introduction

DRG4FOODxIDENTITYVALLEY

This “Digital Responsibility Playbook” (v0.2) is meant to ensure a systematic approach for the implementation of the Digital Responsibility Goals (DRGs) into the DRG4FOOD project. In this “manual”, the prioritisation of the DRG guiding criteria (detailed in D4.1) is translated into guiding questions and recommendations for potential implementations to instruct project participants on how to fulfil DRG4FOOD’s vision of a more trustworthy data-driven food system.

The playbook is divided into one section for each Digital Responsibility Goal. Each section contains: key questions that should guide the design process and operation of digital technologies; a checklist of recommended implementations to develop and operate responsible digital technology; resources to support implementation and an examplary scenario of an optimal implementation.

Components of the checklist are each based on a guiding criterion associated with a DRG. They are divided into four hierachical levels of ascending sophistication, yet descending necessity (inspired by the MoSCoW prioritization technique): fundamental, intermediate, advanced and ideal.

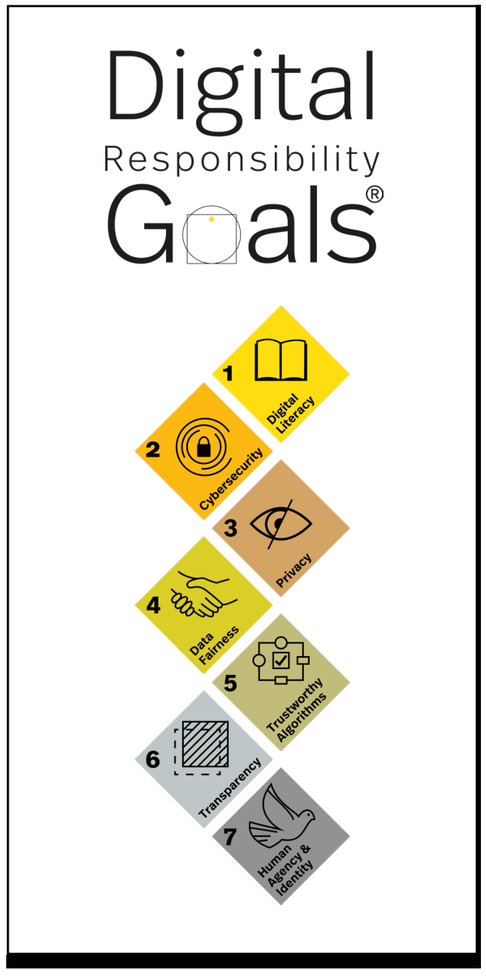

Table of contents

DIGITAL LITERACY

Digital Literacy and unrestricted as well as competent access to digital services and infrastructure are prerequisites for the sovereign and self-determined use of digital technologies.

Key questions

Who is the target group of this digital technology, and who is excluded from using it and why?

How can this digital technology be designed to maximise its acceptance?

How is this digital technology leveraging opportunities and avoiding risks of the digital transformation?

Resources

UX Design Checklists

Web Content Accessibility Guideline (WCAG)

WAVE Web Accessibility Evaluation Tool

Rewordify – Simple language generator

Google Lighthouse (Website quality evaluation)

Checklist

Fundamental

N/A

Intermediate

- ☐ Whenever possible, implement accessibility-enhancing features or design content accessibly (e.g. large fonts, sufficient contrast, optimisation for screen readers)
- ☐ Consider and implement user-friendliness in UX and UI design
- ☐ Use little jargon and language that is familiar to the user

Advanced

N/A

Ideal

- ☐ Provide information about why and how this digital technology was developed using the DRGs (e.g. on your website)
- ☐ Provide information if and how sustainability, diversity or inclusion were implemented

Example

The colours and fonts chosen for an online banking portal were picked with accessibility in mind. The UX / UI, including the understandbility of content, was piloted by test users and feedback was integrated into the design. Information on how and why digital responsibility was a focus of the development process is detailed in a specific section on the project / company website.

CYBERSECURITY

Cybersecurity protects systems against compromise and manipulation by unauthorized actors and ensures the protection of users and their data - from data collection to data utilization. It is a basic prerequisite for the responsible.

Key questions

Who in your team is responsible for cybersecurity and how does your team respond to incidents?

What does “security by design” entail for this digital technology?

What are potential security vulnerabilities of this digital technology and how can it be tested for those vulnerabilities?

How can users report a security issue with this digital technology and how are users notified in the event of a security breach?

Resources

OWASP Application Security Verification Standard (ASVS)
OWASP Mobile Application Security Verification Standard (MASVS)
Common Weakness Enumeration (CWE)
Secure development and deployment guidance (UK National Cyber Security Center)
Secure Software Development Framework (SSDF) – NIST
Coordinated Vulnerability Disclosure policies in the EU

Checklist

Fundamental

- ☐ Member(s) of the team have experience securing digital technologies
- ☐ Assess your cybersecurity threat/attack vectors
- ☐ Depending on the assessment, ensure that proportional secure software development and information security practices and standards are followed
- ☐ Provide information to users on how cybersecurity is ensured

Intermediate

- ☐ Draft a plan/strategy for security considerations throughout the product life cycle

Advanced

- ☐ Offer users a mechanism to report bugs and issues, and be responsive to these reports (responsible disclosure policy)

Ideal

- ☐ Publish risk assessments, information about patched vulnerabilities and disclose any security incidents publicly

Example

A nutrition coaching smartphone app achieves advanced security level (MAS L2) on the OWASP Mobile Application Security Verification Standard (MASVS) and the development team has a dedicated security expert who keeps security requirements up-to-date. Cybersecurity is also seen as a community effort, offering possibilities to report vulnerabilities and disclosing of relevant incidents.

PRIVACY

Privacy is part of our human dignity and a prerequisite for digital self-determination. Protection of privacy allows users to act confidently in the digital world. Privacy by design and by default enable responsible data usage. Users need to

Key questions

Does the digital technology collect personal information from the user? How sensitive is this information?

Does it collect more information than necessary?

How does a user of the digital technology access, correct, delete, or remove personal information?

Is the purpose of personal data processing clear at all times? Will any of the personal information stored be shared with third parties?

Resources

Guidance on Privacy-Enhancing Technologies (PET)

International Association of Privacy Professionals

General Data Protection Regulation (GDPR)

Privacy is an afterthought in the software lifecycle. That needs to change (StackOverflow)

Checklist

Fundamental

- ☐ Implement basic data protection principles (GDPR, Art. 5) proactively, transparently, and user-friendly
- ☐ Ensure that protection of user privacy is the default setting and consider privacy by design choices, where appropriate
- ☐ Publish a concise overview of what personal data is collected and why, how it is used or shared, how it is stored and secured, and how long it is kept

Intermediate

- ☐ Implement innovative privacy-enhancing technologies (PETs) to exceed basic legal requirements of privacy protection, where possible

Advanced

N/A

Ideal

N/A

Example

The privacy policy of an online shopping website is worded in easily understandable language and presented in a user-friendly structure. Personal data is only gathered for providing the services of the website / company. GDPR compliancy is certified by an external party. Methods of differential privacy are used to ensure a high level of privacy of customer data.

DATA FAIRNESS

Non-personal data must also be protected and handled according to its value. At the same time, suitable mechanisms must be defined to make data transferable and applicable between parties. This is the only way to ensure **data fairness** and balanced cooperation between various stakeholders in data ecosystems.

Key questions

Which databases are you using for this digital technology and why did you choose them?

What are potential gaps, inaccuracies, or biases in datasets? If so, how can they be adjusted for or corrected?

How could users or society best benefit from data produced/ used by this digital technology beyond DRG4FOOD?

Resources

FAIR data principles

Datasheets for datasets

Create a dataset card

Data Cards: Purposeful and Transparent Dataset Documentation for Responsible AI

Open Data Handbook

Checklist

Fundamental

- ☐ Determine and document the potential gaps, inaccuracies or biases in datasets (e.g. by using the “dataset card” / “datasheets for datasets” approach, see resources)
- ☐ Implement users’ control over data usage as granular as possible
- ☐ Offer the possibility to export data in an open format

Intermediate

N/A

Advanced

- ☐ Where possible, make datasets available to the public by open data license, implementing FAIR data principles

Ideal

- ☐ Publish an overview of what non-personal data are collected and why, how they are used or shared, how they are stored

Example

The development team of a fitness tracker has diligently validated the datasets used for the digital solution and documented findings in a dataset card that is openly available. The user is offered user-friendly ways to export user data in common formats for sharing with other services (e.g. other apps or health practioners). Access to datasets is made possible for research purposes (e.g. under the EU Data Altruism scheme). All data flows are detailed in an easily understandable data policy.

TRUSTWORTHY ALGORITHMS

Data-processing must be **trustworthy**. This is true for simple **algorithms** as well as for more complex systems, up to autonomously acting systems.

Key questions

How can reliability and consistency of the underlying algorithms of this digital technology be verified?

Are outputs of the algorithmic systems of this digital technology un-biased, fair and inclusive?

What are the social consequences of this digital technology?

How can the decision-making processes of algorithmic systems be verified and reconstructed?

Resources

IEEE Standard Model Process for Addressing Ethical Concerns during System Design

What is Explainable AI (XAI)?

Model Cards for Model Reporting

Model Card Creator Tool

EU Ethics guidelines for trustworthy AI

Checklist

Fundamental

- ☐ Mitigate biases in algorithmic outputs through effective measures
- ☐ Whenever possible and reasonable, provide the option to “explain” the output of algorithmic processing or AI/ML systems

Intermediate

- ☐ Conduct and document an algorithmic impact assessment (“first-party audit”)

Advanced

- ☐ When using AI/ML systems perform a robustness test of your model
- ☐ Publish source code in an online repository to allow for independent review

Ideal

- ☐ Task an independent party with validating your model architecture (“second-party audit”)

Example

Before the implementation of an algorithmic system used in public administration to detect social benefits fraud an impact assessment has been conducted. The finalised system has been independently audited for bias, robustness and reliability. The system offers indicators explaining results to case handlers and the source code is accessible to accredited journalists or researchers.

TRANSPARENCY

Proactive **transparency** for users and all other stakeholders is needed. This includes transparency of the principles that underlie digital products, services, and processes, and transparency of the digital solution and its components.

Key questions

How can transparency in the context of this digital technology foster trust?

How can this transparency be verified independently?

What communication channels are there for users and stakeholders of this digital technology to contact the team or find out more information?

Resources

Open-Source Initiative

Checklist

Fundamental

- ☐ Whenever possible, provide transparency (data flows, technology, potential conflicts of interest, business model…)

Intermediate

N/A

Advanced

- ☐ Implement verifiable transparency (e.g. footnotes, certificates, blockchain…)

Ideal

- ☐ Publish source code & all components of the project in an online repository under an open-source license
- ☐ Offer communication channels to get in contact with users (social media, chat function, community forum, feedback form…)

Example

A social media company provides transparent information on their business model and revenue streams (e.g. contextual advertising & ad partners, outsourced content moderation,...) and technology used (e.g. facial recognition, algorithmic content recommendation). Some of the underlying code is open-sourced to allow for external evaluation. Sufficient resources and channels are available to allow for effective customer service.

HUMAN AGENCY & IDENTITY

Especially in the digital space, we must protect our **identity** and preserve human responsibility. Preserving the multifaceted human identity must be a prerequisite for any digital development. The resulting digital products, services, and processes are human-centered, inclusive, ethically sensitive, and sustainable, maintaining **human agency** at all times.

Key questions

How can the user concretely benefit from this digital technology?

Does the use of this digital technology impact important aspects of the life of individuals, like health, job, family, or privacy?

Has this digital technology the potential to change the behaviour of the user?

Does this digital technology have a positive/negative impact on sustainability and climate?

Resources

UN Sustainable Development Goals
Consequence Scanning

Checklist

Fundamental

- ☐ Ensure that design choices and capabilities are first and foremost tailored to benefit the user
- ☐ Ensure that any commodification does not impact autonomy or dignity of the user

Intermediate

- ☐ Refrain from using nudging methods or similar techniques to subliminally influence the behaviour of the user

Advanced

- ☐ Where appropriate, allow for human agency instead of autonomous decision-making
- ☐ Choose technology, suppliers, business model based on sustainability criteria

Ideal

- ☐ Contribute to solving a societal problem with this digital technology

Example

A travel booking website does not employ dark patterns (e.g hidden costs, pressure selling, preselection etc.) to manipulate or deceive users. For customer relations interaction with a human is actively offered. Sustainability is a factor driving business decisions, e.g. the website is hosted on a “green” data center.