Federal Ministry
of Justice and
Consumer Protection

Methodology of scenario planning

The method explained

2 April 2019

Methodology of scenario planning

In the CDR Initiative run by the Federal Ministry of Justice and Consumer Protection (BMJV), an approach using scenario planning was developed, enabling the consequences of the digital transformation process to be identified using realistic case examples. Further details and documents about the CDR Initiative are available on the website: www.bmjv.de/CDR-Initiative.

[Please note that this link is outdated. More information on www.cdr-initiative.de]

Brief overview

Digitalisation is radically altering the interfaces between business, society and politics. Within society, what was once a *desire* for a responsible approach towards innovation has now become a *demand*. In order to develop generally acceptable ideas of what positive digital progress could look like, it is necessary to engage in collective thinking above and beyond the confines of specific interest groups.

This is why the BMJV set up the 'Corporate Digital Responsibility (CDR) Initiative' in 2018. The Initiative is tasked with finding out what it means to assume corporate responsibility in the digital world. As part of the Initiative, a Working Group was established comprising representatives of business and politics. The team set out with the goal of developing a method for identifying and clearly illustrating the impact of digitalisation on society. This method – known as 'scenario planning' – is based on realistic case examples which can be discussed by anyone with readily accessible technical knowledge, without requiring academic expertise. One strength of scenario planning is how it enables things to be seen from the consumer's viewpoint. This makes it possible to find out what measures are required and what interests need to be taken into account in order to strengthen the general public's trust in the digital transformation process. Another strength is that it enables consumers to reappraise their own expectations with regard to technological innovations. Using the example of a 'smart front door', the group was quick to recognise the benefits of being able to grant flexible access, while the risks of being denied access due to technical limitations were also identified.

Although the individual case examples show a wide range of different possibilities for simplifying the practical aspects of everyday life on both individual and collective levels, the problems associated with these scenarios are actually quite similar. There is no doubt that the spread of digital technology offers potential in terms of freedom and/or inclusion. However, certain issues relating to liability, responsibility and security (of data, networks and IT infrastructure) still need to be clarified. Furthermore, digital innovation also creates new problems related to the protection of privacy and the short lifespan of increasingly complex digital products and services.

On a higher level of abstraction than the case examples, a need for clarification became apparent with regard to the principles of voluntary action, self-determination and the right not to be connected to the digital world, as well as regarding fundamental structural issues.

The results presented by the Working Group in this document provide some initial pointers towards the new framework conditions that need to be established so that the digitalisation process can develop in a positive direction. The insights gathered in this report should not be regarded as exhaustive but are rather intended to serve as a basis for further work within the CDR Initiative.

Introduction

This document presents the Working Group's results. The CDR Working Group opted for an approach based on the discussion of case examples. 'Scenario planning' is also used (in different variations) in the development of technological innovations and is similar to the concept of 'design thinking'.

The goal was to develop and test an open-ended method that is intuitive to work with and can be used with relatively little practice by stakeholders outside the BMJV's initial circle of participants. The method – which was refined and consolidated over a period of multiple test phases carried out by the CDR Working Group – is presented in the following sections. Some early insights for responsible digitalisation are also described. These resulted from the trial application of the 'scenario planning' technique.

This document is also intended to serve as an instruction manual on how to identify and discuss the implications of a technological innovation using concrete examples. It is divided into the following sections:

Corporate Digital Responsibility (CDR):	Definition
Scenario planning:	Methods for identifying gaps in responsibility
Case example:	The smart front door
Aspects of digital responsibility:	Results from several case examples
Principles of responsibility in practice:	Content of responsible digitalisation
Limitations:	Open issues
Recommendations:	Suggestions for next steps

Corporate Digital Responsibility (CDR) – What is at stake?

The overall concept of Corporate Digital Responsibility (CDR) is based on the idea of Corporate Social Responsibility (CSR) which describes the way in which companies assume responsibility for their impact on society. CSR deals with various social, ecological and economic aspects such as those covered in the standard internationally-recognised documents on corporate responsibility. These documents include the ILO Declaration of Principles on Enterprises and Social Policy, the OECD Guidelines for Multinational Enterprises, the UN Guiding Principles on Business and Human Rights, the UN Global Compact, the International Standard ISO 26000 and the applicable reporting standards for companies.

This broad-ranging concept of CSR would seem to cover every area of corporate responsibility. But the digitalisation process and the associated surge in innovation – particularly involving the connection of all kinds of new products and services to the internet – have generated social phenomena which have yet to be addressed within the existing CSR framework.

For example, new issues of self-determination arise when using digital technologies that involve not only data (including the analysis and networking of that data) but also algorithms, and which are digitally connected with physical products across several different spheres of responsibility.

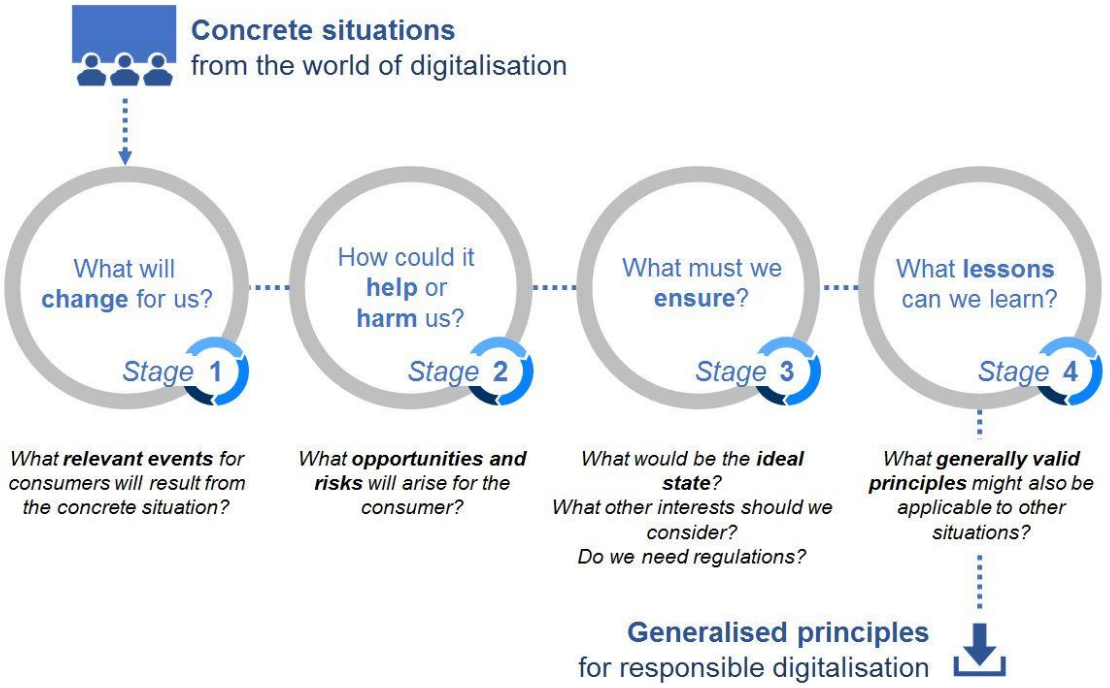
Contrary to what might be expected, the difference between CDR and CSR is not based on the difference between ‘social’ and ‘digital’ but rather on the way the underlying responsibility is interpreted. This appears in a new light due to the spread of digital technology: in the rapidly advancing field of digital innovation, who is responsible to whom and for what? As regards the future consequences of the technology being produced today, conflicts of interest could emerge. It is important to examine and discuss the legitimacy of new developments in the light of competing economic, social and ecological interests. Such assessments can and must be measured in terms of our contemporary Western values and ideals, several aspects of which differ from the value systems in other countries (e.g. the social scoring system in China). It is too early to say whether CDR and CSR will become entirely separate paradigms. In this early phase of examining CDR, the focus is on developing a new understanding of responsibility under the conditions generated by the dynamics of digital innovation.

The method

Scenario planning provides a way of getting away from the abstract level and shedding light on the responsibility issue in everyday digital situations. First of all, hypothetical situations are described in concrete detail and then closely analysed in a sequence of four different stages. For example, the implications of consumers having a smart front door are identified in terms of the potential opportunities and risks for the general public. This leads to the formulation of hypothetical steps to be taken by economic actors (e.g. companies). These hypothetical proposals are informed by the known consequences of digital progress.

Scenario planning thus makes it possible to assume and/or consider the viewpoints of different stakeholders. Applying the technique to a broad range of different situations enables a more accurate picture of the key questions in a digitalisation process to emerge and brings possible answers to the surface. Scenario planning is particularly suitable for group work because it allows various different perspectives to be incorporated into the process. It is helpful to set clear time limits because – even within diverse groups – the main arguments can often be identified within a short space of time based on initial and spontaneous responses.

Scenario planning is carried out in four iterative stages as illustrated in the diagram below:


Concrete situations
from the world of digitalisation
What will change for us?
Stage 1
How could it help or harm us?
Stage 2
What must we ensure?
Stage 3
What lessons can we learn?
Stage 4
What relevant events for consumers will result from the concrete situation?
What opportunities and risks will arise for the consumer?
What would be the ideal state?
What other interests should we consider?
Do we need regulations?
What generally valid principles might also be applicable to other situations?
Generalised principles
for responsible digitalisation

Stage 1: Scenario development

The participants or organisers select a field of application within the digital transformation process and then describe a scenario in as much detail as possible (e.g. how some new technology affects or could affect our everyday lives). Ideally, everyone should have a relatively similar and (above all) concrete idea of the field of application. In the first stage, the participants must therefore address the following key question: 'What consumer-relevant events or effects will arise in the field of application?' The participants note down everything that immediately springs to mind. There are no right or wrong answers. No evaluation needs to be carried out during this stage because the main emphasis is on factual consequences.

Stage 2: Scenario evaluation

In the second stage, the group evaluates the previously selected event by asking what the opportunities and challenges are for consumers. In the chosen example of a smart front door, this involves evaluating the usage and storage of access information. In other words, what impact will the technological scenario have on their lives? Once again the participants consider the pros and cons in terms of the opportunities and risks arising from this more specifically defined situation.

Stage 3: Need for action

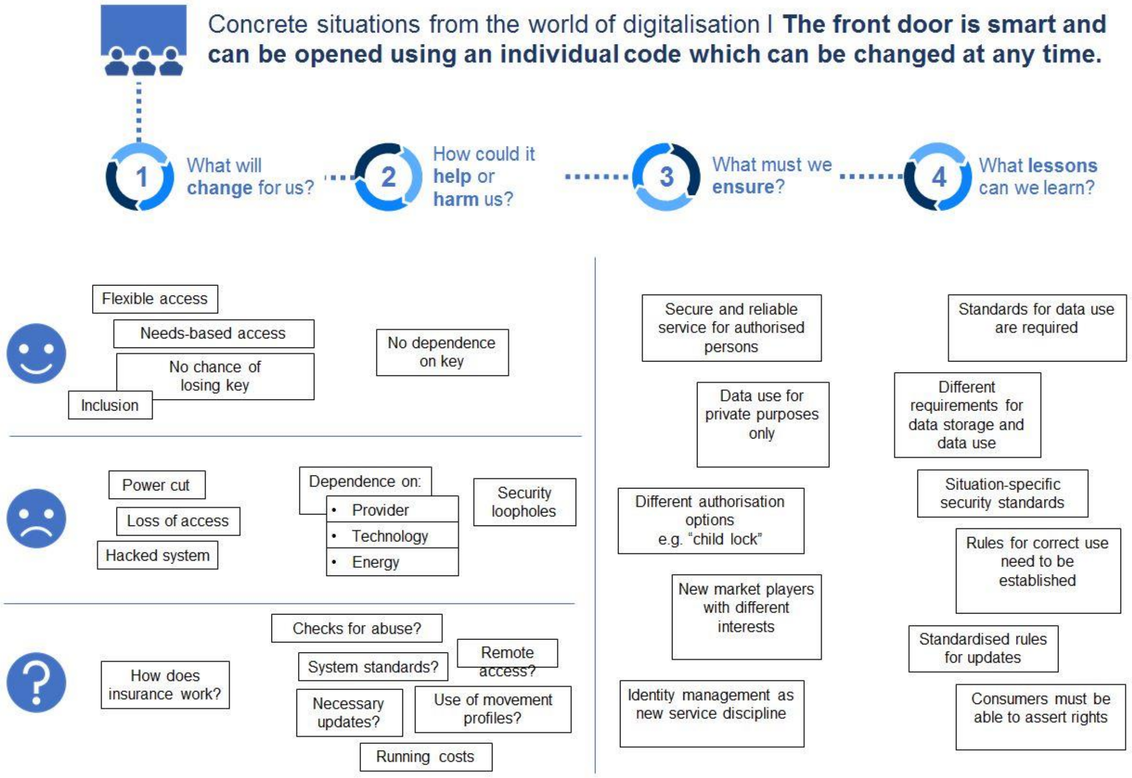
If the group is confident that it has identified all the relevant implications, it proceeds to the third stage where it moves from the concrete to the meta level. What action is required based on the evaluated event? What is the ideal state? What other interests exist? What stakeholders were involved in the selected event? If necessary, the existing statutory regulations or the regulatory gaps for this concrete example can also be addressed.

Stage 4: Recommendation for action

On another level of abstraction, situations are identified that appear to demand some kind of fundamental clarification. These situations can often be seen reappearing in several different scenarios. Taking the example of the smart front door, they include the need to disclose personal data, but also the need for protection against unwanted transfer to third parties, freedom from manipulation, and independence from a single provider. If insights are confirmed on this level by several different scenarios, it provides a strong indication (backed up by the case examples) about where responsibility needs to be directed in the digital context. However, it tells us nothing about what measures should be used in order to establish a responsible approach towards digital innovation. But based on the analysis conducted in the fourth stage, an action plan is drawn up describing how a responsible approach could be achieved and who could implement it.

Case example – the smart front door

This example is based on the premise that access mechanisms controlled by digital identification routines are increasingly common in private residential settings. It is irrelevant whether the identification process is performed via biometric recognition or by entering a code. In order to simplify the scenario, it was decided to focus on a process of entering a code that can be individually selected and changed by the user. To conduct scenario planning, practical aspects were significant. If a key is no longer required, who is granted access? Who decides on and monitors access? What happens if the code gets lost or if there is a power cut? These practical questions and their implications are illustrated in the following diagram:



Concrete situations from the world of digitalisation I **The front door is smart and can be opened using an individual code which can be changed at any time.**

1 What will **change** for us?

2 How could it **help** or **harm** us?

3 What must we **ensure**?

4 What **lessons** can we learn?

Flexible access

Needs-based access

No chance of losing key

Inclusion

No dependence on key

Power cut

Loss of access

Hacked system

Dependence on:
- Provider
- Technology
- Energy

Security loopholes

How does insurance work?

Checks for abuse?

System standards?

Remote access?

Necessary updates?

Use of movement profiles?

Running costs

Secure and reliable service for authorised persons

Data use for private purposes only

Different authorisation options e.g. "child lock"

New market players with different interests

Identity management as new service discipline

Standards for data use are required

Different requirements for data storage and data use

Situation-specific security standards

Rules for correct use need to be established

Standardised rules for updates

Consumers must be able to assert rights

Aspects of digital responsibility

Comparing different scenarios gives rise to a cross-cutting perspective which sheds light on the underlying structural conditions that form an essential part of digital responsibility. Without this analysis and without the necessary framework conditions, the long-term consequences (as opposed to the short-term advantages) can eventually become impossible to control due to the powerful dynamics of innovation.

The following thematic areas were identified by the Working Group as being relevant fields of responsibility requiring clarification. They have not been discussed in detail or substantively elaborated.

They are organised thematically. The idea is for them to be incorporated at a later stage into an overall concept of digital responsibility. The particular selection of different themes reflects a fundamental desire to prevent further social imbalances emerging as a result of digitalisation. These aspects and principles should be taken into consideration when developing and distributing digital technologies:

Ensuring social inclusion via:	• Accessibility • Digital education and awareness-raising • Consumer information and assured consumer understanding • Skills management for employees • Fair digital platforms with non-discriminatory access
Ensuring that digital services enable individual self-determination in terms of:	• Voluntariness • Freedom of choice for consumers • Right not to use social media • Right to be forgotten
Taking account of structural changes in the mass distribution of technology with regard to:	• Transport • Infrastructure • Urban landscapes • Future of work
Avoiding rebound effects	• Demand for sustainability in general • Longevity and modularity of solutions • Permanent update capability for software components
Guaranteeing interoperability with generally applicable standards for:	• Technology • Dealing with competition • Products • Services
Guaranteeing data protection and privacy	• Privacy by design and default • Transparency regarding the data collected and processed • Clear restriction to specified purpose • Consumer access and deletion rights
Guaranteeing digital security through:	• User protection, i.e. preventing anyone from becoming a victim or offender • Generally applicable security guidelines • Precautions against system outages and provision of alternative solutions
Designing liability regulations for digitally networked (i.e. smart) systems:	• Standard procedures for breaches of digital contracts • Assertion of liability claims • Effective monitoring systems and market supervision • Availability of regulatory knowledge • Ability to name the responsible persons • Clarification of product responsibility • Strengthening of self-responsibility

Based on these aspects of digital responsibility, it is possible to derive the principles outlined in the following section.

Principles of digital responsibility

(non-exhaustive)

The digital transformation process is highly dynamic and its future development is impossible to predict. Any approach to Corporate Digital Responsibility must be similarly dynamic and adaptable. The insights presented here are provisional. It is important when dealing with this issue to have the courage to rethink ideas and/or revise assumptions. The core question is how we want the world of tomorrow to be.

The companies should discuss their value hierarchies and clarify the issue of their responsibility towards third parties. The companies are stakeholders in the digital transformation process. They account for the 'C' in CDR. But other stakeholders bear responsibility too. The goal is for the principles to represent an economic advantage in the long term. Based on the concrete aspects of digital responsibility outlined above, it is possible to define a number of initial generalised principles of corporate responsibility which should be embedded within a practical and statutory framework:

1. Companies should enable and encourage consumer self-determination.

2. Companies should regard the digital transformation process as a means for increasing social inclusion and should make it serve the goal of sustainability. This includes asking whether certain technologies are actually necessary (risk/opportunity assessment).

3. Companies should try to ensure that nobody gets left behind in the digital transformation process.

4. Companies should avoid making consumers dependent on technology in the digital transformation process.

5. Companies should encourage social discourse and engage in awareness-raising.

6. Companies should guarantee data protection and privacy (privacy by default/privacy by design).

7. Companies should provide interoperable technologies.

8. Companies should ensure that new technologies are designed with high IT security standards during the development phase and should continue providing the necessary security updates in future.

Limitations

The members of the CDR Working Group met on a monthly basis, running the Initiative alongside their main duties in their respective companies and the Ministry. This explains the highly practice-oriented nature of the results. It also explains why it was impossible to conduct deeper analysis and develop more detailed concepts. The group's high level of efficiency is due to the fact that in their main jobs, the members work on similar issues of responsibility in the digital context. Very little time was required for knowledge transfer.

It also means that the group's knowledge about the consequences of digitalisation is not sufficiently representative and needs to be broadened by adding other social viewpoints. This broadening of the horizon to include other interest groups and representatives of different segments of society will involve a communication process that will serve to improve the resilience of the solutions put forward for digital responsibility.

The 'scenario planning' technique used by the group has proven itself to be stable and scalable. It enables a broader view to be taken of the opportunities and risks involved with innovations, technological products and digital services without requiring any prior expert knowledge. But this on its own is not enough to develop a viable concept of digital responsibility for all stakeholders. It requires more in-depth conceptual work which is planned for a subsequent stage.

The work already conducted was done without any major reference to scientific theories because these have not yet been developed far enough in the area of digital responsibility. In the fields of business ethics and corporate responsibility, however, theories have been developed which could be utilised here. Their applicability for the concept of CDR still needs to be assessed. Likewise, the question of whether CSR and CDR should be treated as integrated or separate concepts has not yet been resolved in this first exploratory phase and will have to be clarified within the scope of academic investigation.

Recommendation

Based on the results outlined in this document, the Working Group recommends proceeding in the following manner in the CDR Initiative:

1. Broadening the scope of scenario planning to include several different interest groups in order to obtain the most diverse possible impression of the concrete and structural consequences of digital innovation.

2. Conceptual work to shape awareness of digital responsibility on the basis of further insights from scenario planning.

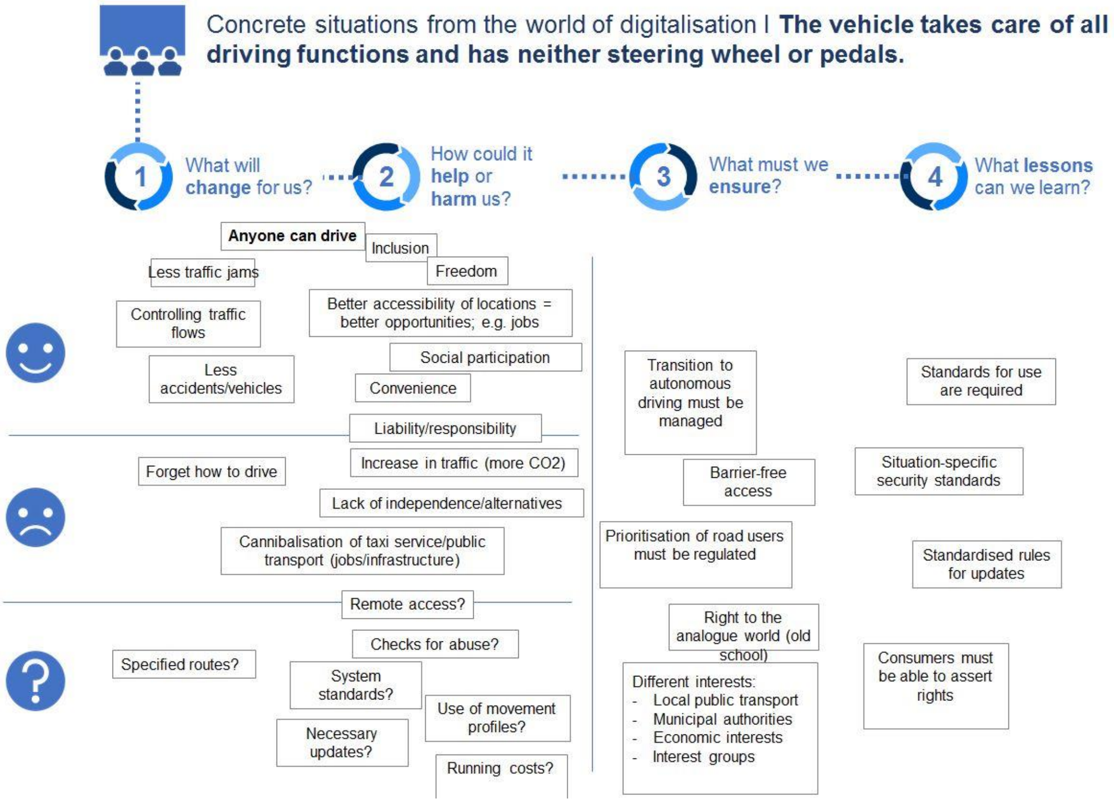
3. Consolidation of the concept of corporate digital responsibility by sharing ideas with the research community and other relevant stakeholders.

Annex: Further case examples

In the following section, additional examples with brief descriptions are provided as a way of further illustrating the scenario planning technique.

Case example – Autonomous driving

In this example, autonomous driving is defined as being where the vehicle takes complete care of all the driving functions, thereby distinguishing it from assisted driving and from semi-automated, highly-automated or fully-automated driving. The user does not require any driving skills or a driving licence and the vehicle has neither steering wheel nor pedals. Everyone in the vehicle is a passenger. At present, there are no autonomous vehicles on the road in Germany, nor are there any autonomous driving functions in use. What is being discussed here is a future scenario.



Concrete situations from the world of digitalisation I **The vehicle takes care of all driving functions and has neither steering wheel or pedals.**

1 What will **change** for us?

2 How could it **help** or **harm** us?

3 What must we **ensure**?

4 What **lessons** can we learn?

Anyone can drive

Inclusion

Less traffic jams

Freedom

Controlling traffic flows

Better accessibility of locations = better opportunities; e.g. jobs

Social participation

Less accidents/vehicles

Convenience

Liability/responsibility

Forget how to drive

Increase in traffic (more CO2)

Lack of independence/alternatives

Cannibalisation of taxi service/public transport (jobs/infrastructure)

Remote access?

Checks for abuse?

Specified routes?

System standards?

Use of movement profiles?

Necessary updates?

Running costs?

Transition to autonomous driving must be managed

Barrier-free access

Prioritisation of road users must be regulated

Right to the analogue world (old school)

Different interests:
- Local public transport
- Municipal authorities
- Economic interests
- Interest groups

Standards for use are required

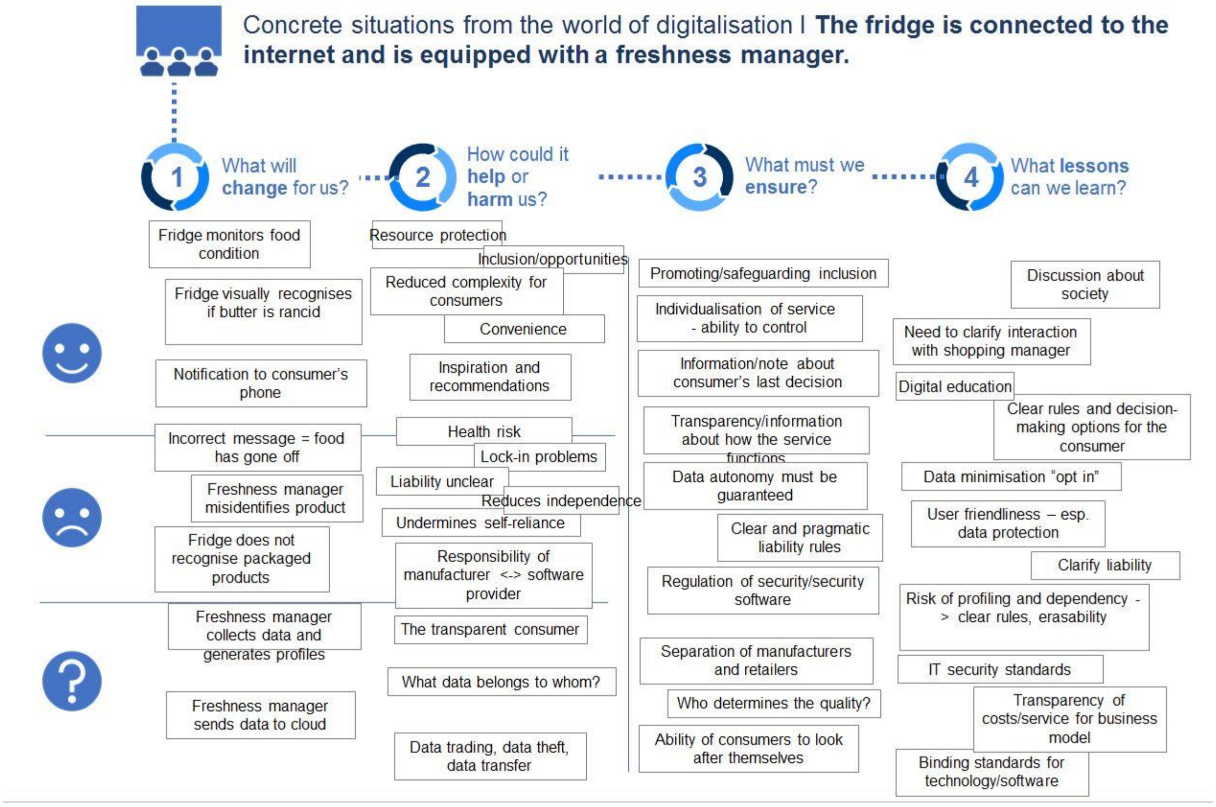
Situation-specific security standards

Standardised rules for updates

Consumers must be able to assert rights

Case example – IoT fridge with freshness manager

This is an example from the Internet of Things (IoT). In the kitchen is a smart IoT fridge equipped with a freshness manager which monitors the condition of the groceries using a third-party algorithm. IoT appliances include all devices and components which are wirelessly connected to a network and which are capable of collecting, storing and processing data.



Concrete situations from the world of digitalisation I **The fridge is connected to the internet and is equipped with a freshness manager.**

1 What will **change** for us?

Fridge monitors food condition

Fridge visually recognises if butter is rancid

Notification to consumer's phone

Incorrect message = food has gone off

Freshness manager misidentifies product

Fridge does not recognise packaged products

Freshness manager collects data and generates profiles

Freshness manager sends data to cloud

2 How could it **help** or **harm** us?

Resource protection

Inclusion/opportunities

Reduced complexity for consumers

Convenience

Inspiration and recommendations

Health risk

Lock-in problems

Liability unclear

Reduces independence

Undermines self-reliance

Responsibility of manufacturer <-> software provider

The transparent consumer

What data belongs to whom?

Data trading, data theft, data transfer

3 What must we **ensure**?

Promoting/safeguarding inclusion

Individualisation of service - ability to control

Information/note about consumer's last decision

Transparency/information about how the service functions

Data autonomy must be guaranteed

Clear and pragmatic liability rules

Regulation of security/security software

Separation of manufacturers and retailers

Who determines the quality?

Ability of consumers to look after themselves

4 What **lessons** can we learn?

Discussion about society

Need to clarify interaction with shopping manager

Digital education

Clear rules and decision-making options for the consumer

Data minimisation "opt in"

User friendliness – esp. data protection

Clarify liability

Risk of profiling and dependency -> clear rules, erasability

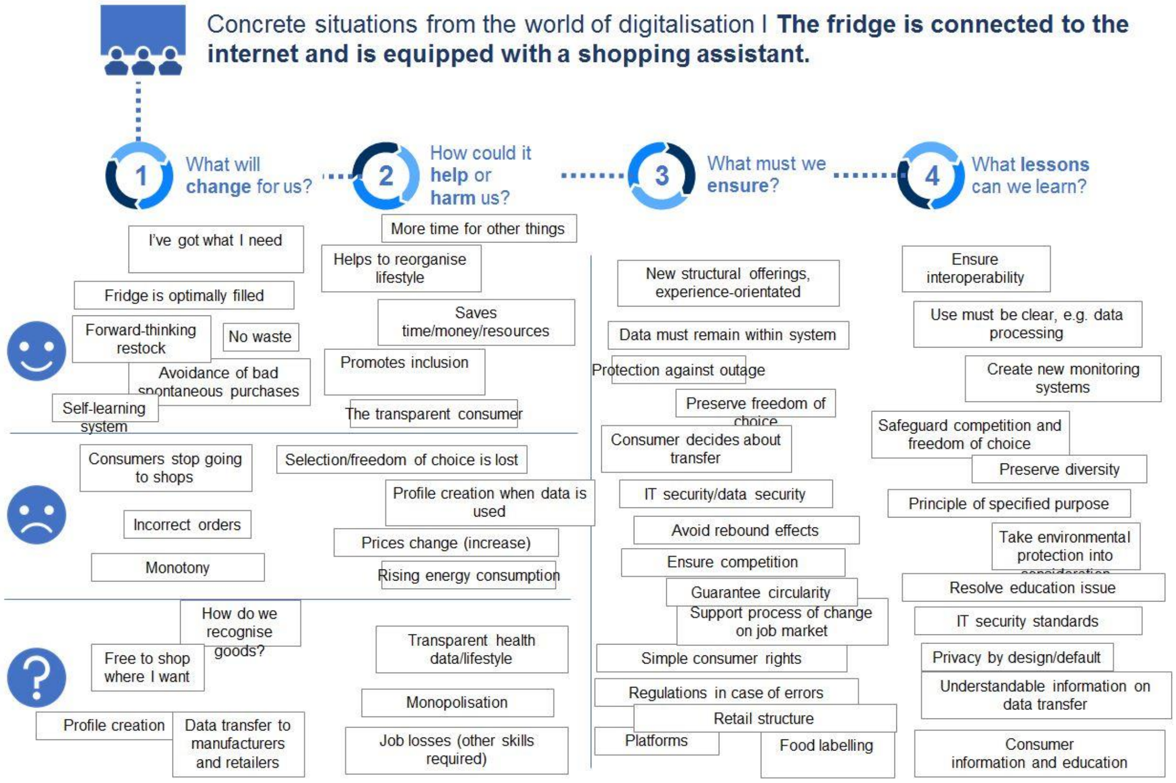
IT security standards

Transparency of costs/service for business model

Binding standards for technology/software

Case example – IoT fridge with shopping assistant

New questions are raised by each (new) feature. Not to mention combinations of features. This time, the selected example was a smart IoT fridge equipped with a shopping assistant.



Concrete situations from the world of digitalisation I **The fridge is connected to the internet and is equipped with a shopping assistant.**

1 What will **change** for us?

2 How could it **help** or **harm** us?

3 What must we **ensure**?

4 What **lessons** can we learn?

I've got what I need

Fridge is optimally filled

Forward-thinking restock

No waste

Avoidance of bad spontaneous purchases

Self-learning system

More time for other things

Helps to reorganise lifestyle

Saves time/money/resources

Promotes inclusion

The transparent consumer

Consumers stop going to shops

Incorrect orders

Monotony

Selection/freedom of choice is lost

Profile creation when data is used

Prices change (increase)

Rising energy consumption

How do we recognise goods?

Free to shop where I want

Profile creation

Data transfer to manufacturers and retailers

Transparent health data/lifestyle

Monopolisation

Job losses (other skills required)

New structural offerings, experience-orientated

Data must remain within system

Protection against outage

Preserve freedom of choice

Consumer decides about transfer

IT security/data security

Avoid rebound effects

Ensure competition

Guarantee circularity

Support process of change on job market

Simple consumer rights

Regulations in case of errors

Retail structure

Platforms

Food labelling

Ensure interoperability

Use must be clear, e.g. data processing

Create new monitoring systems

Safeguard competition and freedom of choice

Preserve diversity

Principle of specified purpose

Take environmental protection into consideration

Resolve education issue

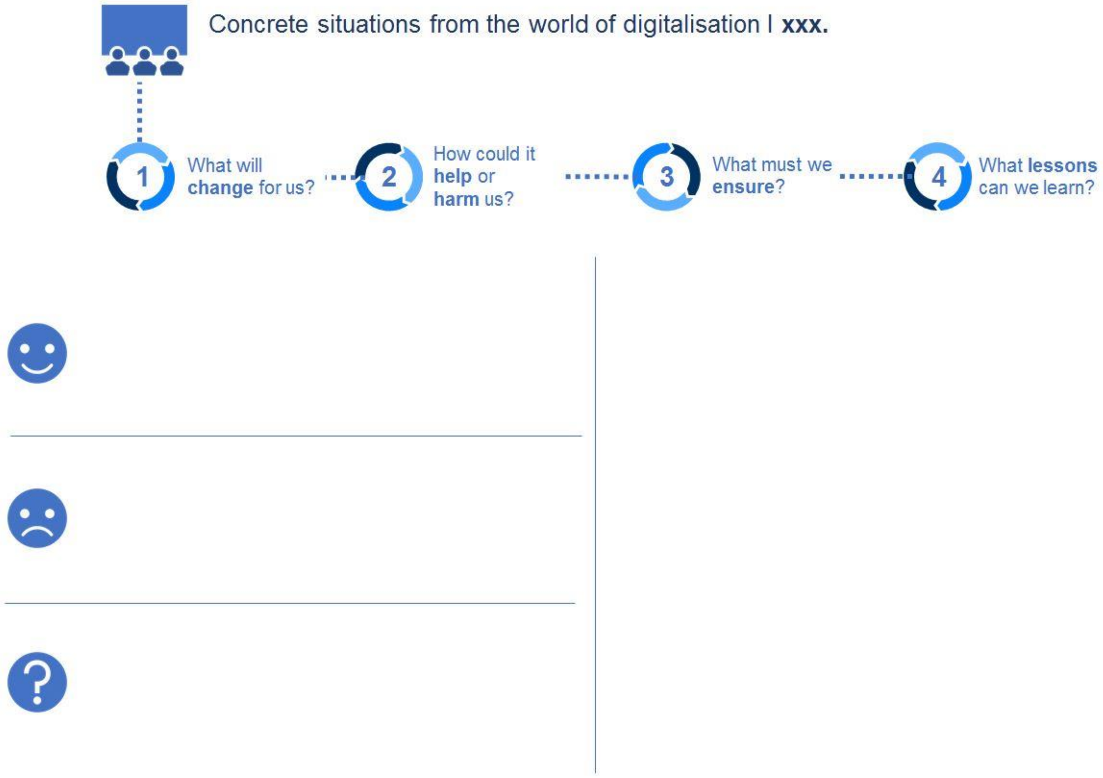
IT security standards

Privacy by design/default

Understandable information on data transfer

Consumer information and education

The more case examples are analysed using scenario planning, the more complete the overall picture becomes. The goal here is to ensure that the group is highly diverse and heterogeneous so that as many viewpoints as possible are incorporated. We have included a template just in case you wish to try it for yourself.



Concrete situations from the world of digitalisation I **xxx.**

1 What will **change** for us?

2 How could it **help** or **harm** us?

3 What must we **ensure**?

4 What **lessons** can we learn?

☺

☹

?

Last revised: March 2019

IMPRINT

Published by:
The German Federal Ministry of Justice and Consumer Protection
11015 Berlin
www.bmjv.de

Cover image:
Image title: Getty Images / Ani_Ka

Last revised:
March 2019