

Appendix

of the Paper

Bridging Digital Transformation in Public Health with
Digital Responsibility

in

Electronic Markets – The International Journal on
Networked Business

Appendix

Part 1

Screenshots of the Presentation and Digital
Whiteboard for Group Work in the Focus Group

Digital Responsibility Focus Group

Part 1 & 2: Welcome, objectives and introduction to the research project

Welcome to the focus group

.

miro

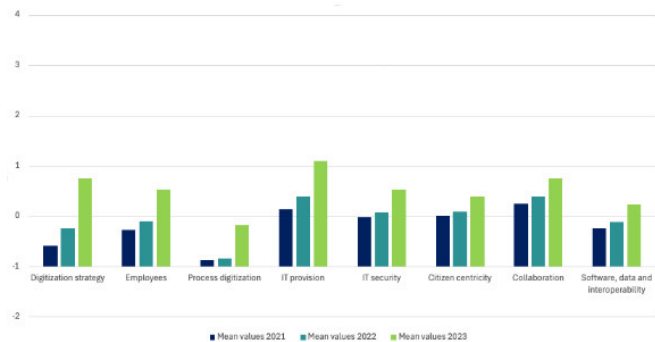
Agenda

1. **Welcome & Objectives (5 min)**
 2. **Introduction to the research project (10 min)**
 3. **Tips for working with Miro (5 min)**
 4. **Discussion: Validation and adaptation of the DR framework (40min)**
-

Digital Responsibility Focus Group

Part 1 & 2: Welcome, objectives and introduction to the research project

Digitalization in the public health sector



Presentation of the DR framework according to Trier et al (2023)



Digital Responsibility Focus Group

Part 1 & 2: Welcome, objectives and introduction to the research project

Results

Code	Total number of criteria with this code	Percentage of all criteria
DR Level: Corporate Level	325	91.8
DR Level: Interorganizational Level	40	11.3
DR Level: Intraorganizational Level	14	4.0
DR Level: Personal Level	59	16.7
DR Level: Societal Level	20	5.6
DR Level: Total	458	/
DR Principle: Security	84	23.7
DR Principle: Data Privacy	12	3.4
DR Principle: Functionality	194	54.8
DR Principle: Accountability	133	37.6
DR Principle: Participation	57	16.1
DR Principle: Transparency	76	21.5
DR Principle: Sustainability	32	9.0
DR Principle: Fairness	4	1.1
DR Principle: Norms & Values	1	0.3
DR Principle: Total	593	/
Total of all Codes	1051	/

Results: DR-Principles

DR-Principles	Short definition
Security	Security as a new DR principle serves to take into account criteria for IT resilience, incident response and cyber security.
Sustainability	Sustainability requires a balance between harnessing the benefits of digital innovation and minimizing environmental damage.
Participation	Participation refers to the involvement in digital processes, e.g. users in software projects or citizens in public decision-making processes.
Data Privacy	Data protection gives individuals the opportunity to control their digital identity.
Transparency	Transparency promotes trust by clarifying how digital services work and ensuring that users understand the value of their data.
Functionality	Functionality ensures that technological advances are in line with societal needs by complying with legal and ethical frameworks such as the General Data Protection Regulation (GDPR).
Fairness	Fairness advocates equal access and equal participation in the digital society and calls on companies to respect intellectual property and ensure the transparency of algorithms.
Norms & Values	Norms and values require individuals, companies and societies to uphold ethical standards such as trust, autonomy and well-being and to focus on integrating these values into product development.
Accountability	The area of accountability calls for clear roles, governance processes, legal frameworks and global efforts to ensure equal opportunities for less privileged nations in the digital world.

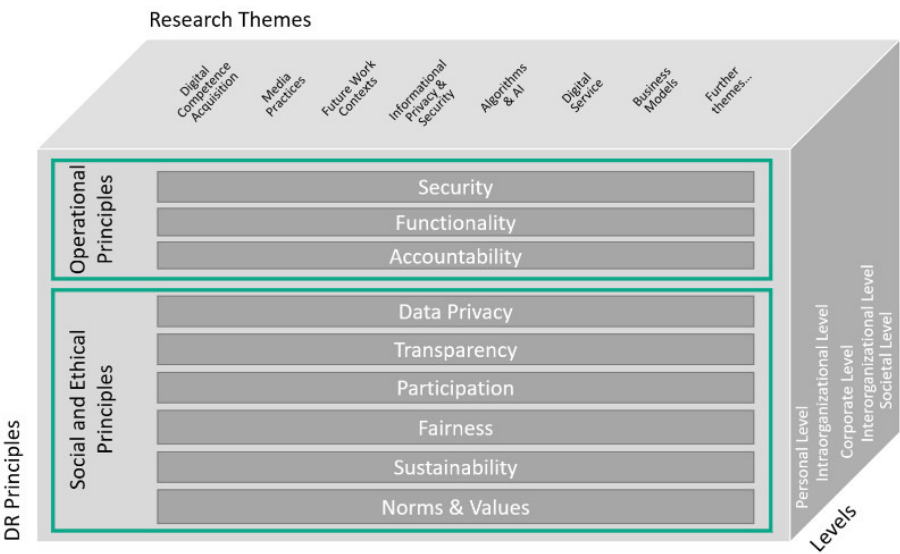
Digital Responsibility Focus Group

Part 1 & 2: Welcome, objectives and introduction to the research project

Results: DR-Levels

DR-Level	Short Definition
Societal Level	The societal level emphasizes the role of the state and supranational institutions in promoting sustainable digitalization through effective political decisions and regulatory frameworks.
Interorganizational Level	At this level, the focus is on cooperation and coordination between public health institutions and external stakeholders.
Corporate Level	The corporate level focuses on the ethical values and operational standards that guide companies in promoting sustainable, transparent and inclusive behaviors when using digital technologies.
Intraorganizational Level	This level focuses on the internal dynamics of digitalization within the health authorities. The focus is on cross-departmental collaboration and coordination between management and employees.
Personal Level	The personal level emphasizes the responsibility of the individual to behave ethically in digital activities.

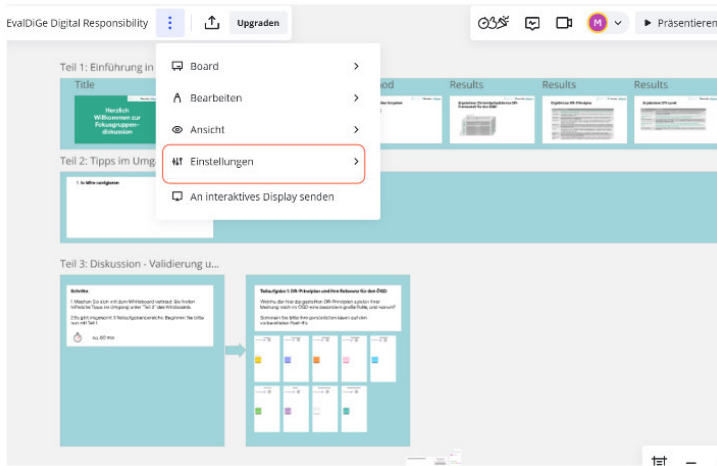
Results: A contextualized DR framework for the public health sector



Digital Responsibility Focus Group

Part 3: Tips for working with Miro

1. navigate in Miro



Right-click and drag to move on the board



Swipe the trackpad with two fingers to move around on the board



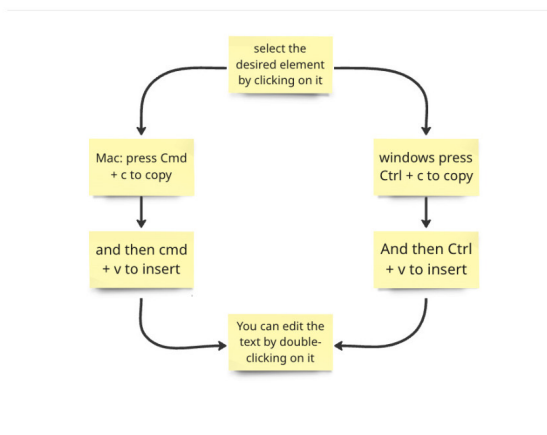
Move the mouse wheel to zoom in or out



To enlarge or reduce with two fingers, pull apart or pull together



2. copy and paste elements



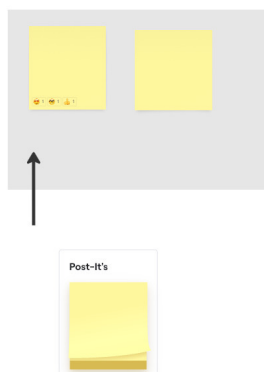
3. create notes

On the left-hand side of the screen you can find a selection of notes



4. move objects

Move objects by clicking & dragging or by copying & pasting. Try moving the Post-It's into the text box.



Digital Responsibility Focus Group

Part 4: Discussion - Validation and adaptation of the DR framework

Now the content part starts!

There are a total of 3 subtasks, which we will guide you through step by step.

Please start with subtask 1.

Subtask 1: DR principles and their relevance for the public health sector

- Please classify the role of the DR principles in the public health sector with a Post-It on the arrow!
- Then give reasons for your assessment on the Post-It.



10 min

Which role does
Security play?

does not
play a role



does play
a big role

Digital Responsibility Focus Group

Part 4: Discussion - Validation and adaptation of the DR framework

Subtask 2: DR levels and their relevance for the public health sector

- Please classify the role of the DR level in the public health sector with a Post-It on the arrow!
- Then give reasons for your assessment on the Post-It.



7 min

Which role does the
Societal Level play?

does not
play role



does play
a big role

Digital Responsibility Focus Group

Part 4: Discussion - Validation and adaptation of the DR framework

Subtask 3: Feedback, practical implications & next steps

- Please collect your personal ideas on the prepared Post-Its for the following four questions.



8 min

- 1: Are there specific practical requirements that should be given greater consideration in the framework? If so, which ones?
- 2: What challenges and opportunities arise for the public health sector from the findings of the framework to date?
- 3: How can the DR principles be integrated into maturity models? What practical implications would this have?
- 4: What are the effects of the addition of the two levels and the new principle to the DR framework? Do they make sense?

Appendix

Part 2

Table 1

All Criteria and Their Applied Levels and Principles

[illegible]

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
DS.3.0.01 For the implementation of digitalization measures, it is at least planned to define a required budget and personnel per measure.	X					X			X					
DS.3.1.01 A digitalization budget is defined for each digitalization measure that is required for the corresponding implementation.	X					X			X					
DS.3.1.02 The prioritisation of digitalization measures is based on criticality as well as the available digitalization budget.	X					X			X			X		
DS.3.2.01 The person responsible for the budget in the public health agency is in close exchange with the responsible department of the district/city and requests the budget (per year) required for the digitalization measures.		x				x								
DS.3.3.01 The digitalization budget is regularly adjusted when digitalization measures are advanced or implemented.	X								X					
DS.3.4.01 The public health agency exchanges information with other public health agencies on planned digitalization measures, digitalization budgets planned for this purpose and adjustments as needed.		x												x
DS.3.4.02 The public health agency supports public health agencies with lower digital maturity in setting a digitalization budget for digitalization measures.		X						X					X	
MA.1.0.01 Employees are aware of individual digitalization measures (e.g. ongoing measures to switch to paperless processes are known).	X			X							X			X
MA.1.1.01 Employees are sensitised to the meaning and purpose of digitalization, the protection of data and the possibilities of digital collaboration (e.g. via email or intranet).	X			X							X			
MA.1.2.01 Staff development is complemented by regular courses on the following topics: digitalization, especially raising employees' awareness of the meaning and purpose of digitalization, data protection and the possibilities of digital collaboration (e.g. via e-mail or intranet).	X			X			X				X			
MA.1.3.01 The sensitization of employees is carried out on a task-related basis and personnel development is supplemented by taskrelated components for further development in the area of digitalization.	X			X							X			
MA.1.4.01 The sensitization of employees is carried out continuously, i.e. new aspects for sensitization are identified and communicated in appropriate measures (e.g. workshops).	X			X							X			
MA.2.0.01 Individual employees are involved in defining the digitalization strategy and implementing the measures.	X			X							X			
MA.2.0.02 Participation opportunities for employees are at least being planned.	X			X							X			
MA.2.1.01 Employees know those responsible for digitalization measures and get involved reactively (e.g. employees contact each other with feedback on digitalization measures).	X			X		X					X			X
MA.2.1.02 The dialogue between those responsible for digitalization measures and co-determination committees (e.g. staff council, representatives of the severely disabled) on the topic of inclusion in digitisation measures is carried out on an ad hoc and irregular basis.	X					X					X			
MA.2.1.03 All affected employees are informed about relevant digitalization measures at an early stage and can participate in working groups or pilot projects (e.g. in requirements surveys or tests).	X			X							X			X
MA.2.1.04 Inclusion is taken into account when involving selected employees in digitalization measures (e.g. with regard to diverse backgrounds and age groups).	X			X							X			
MA.2.2.01 All affected employees are actively involved in relevant digitalization measures (e.g. in defining the strategy, developing new processes, software functions and/or selecting and implementing software/hardware).	X			X							X			
MA.2.2.02 Regular workshops on the digitalization of the public health agency are held (e.g. presentation of current digitalization measures and projects or identification of new digitalization measures).	X								X		X			

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
MA.2.2.03 There are employees in the team who know the functional scope of the specialised applications, can answer user enquiries and communicate requirements to service providers.	X			X					X					X
MA.2.2.04 A dialogue between digitalization managers and codetermination committees (e.g. staff council, representatives of the severely disabled) takes place at least once a year.	X					X					X			
MA.2.2.05 Newly hired employees are introduced to the digitalization measures relevant to their area of responsibility.	X			X					X		X			X
MA.2.3.01 The employees know the digitalization managers to whom they can proactively contribute their ideas regarding new digitalization measures, for example.	x			x		x			x		x			x
MA.2.3.02 Employees are interested in further developing specialised applications and note feedback, which is forwarded to the service providers/manufacturers by the person responsible at the interface.	X			X		X					X			
MA.2.3.03 A dialogue between digitalization managers and codetermination committees (e.g. staff council, representatives of the severely disabled) takes place at least twice a year.	X					X					X			
MA.2.4.01 Systems and processes are strongly user-centred, and usercentredness is continuously analysed and improved (e.g. emphasis is placed on usability and maximum useful digitalization).	X								X				X	
MA.2.4.02 The public health agency (supported by the municipality, if necessary) exchanges information with other public health agencies across federal state borders on participation opportunities for employees in digitalization.		X									X			X
MA.2.4.03 The public health agency supports other public health agencies with lower digital maturity (e.g. by offering crosscutting workshops or counselling services).		X						X					X	
MA.3.0.01 There are individual training courses on communication and collaboration, Office applications (e.g. Word, Outlook), specialist applications, IT security and data protection.	x			x			x				x	x		
MA.3.0.02 Skills are acquired in the use of office applications or specialist applications at least independently.	X			X							X			
MA.3.1.01 Mandatory training courses on communication and cooperation, office applications (e.g. Word, Outlook, Excel), specialised applications, IT security and data protection are held at regular intervals for all employees of the public health agency.	X			X			X				X	X		
MA.3.1.02 Employees can use office and specialist applications for their tasks.	X			X					X		X			
MA.3.1.03 Those responsible for the organisational units of the public health agency regularly determine the training needs of their staff. The training offered is regularly adapted accordingly.	X			X		X					X			
MA.3.1.04 A training concept for all staff has been developed. This contains an overview of (mandatory and recommended) training opportunities for different staff roles, a prioritisation of training and a contact person for training.	X					X					X			
MA.3.1.05 In the event of a crisis, employees can be quickly trained for new tasks (e.g. the handling of specialised applications is well documented and prepared).	X								X		X			
MA.3.2.01 The training concept is accessible to all employees and is actively communicated to them.	X			X							X			X
MA.3.2.02 Training offers are compiled in the training concept in a target group-specific manner and for different skill levels (e.g. specialised applications, basics of process orientation) and offered at least twice a year.	X			X							X			
MA.3.2.03 The training offers are planned and organised in such a way that they can be integrated into the daily work routine.	X			X							X		X	
MA.3.2.04 When hiring new employees, the digital competence of the persons is taken into account.	X			X					X					
MA.3.2.05 Relevant training offers are suggested to the employees according to their tasks.	X			X							X			

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
MA.3.2.06 There are task-specific trainings that can be accessed continuously and without a deadline (e.g. as a presentation, video).	X			X							X		X	
MA.3.3.01 Framework conditions for a digital training culture are created (e.g. through access to a platform with different training offers, self-determined participation in training or free space for employees for training).	x									x	x			
MA.3.3.02 Training is offered at least twice a year as a refresher, based on need.	x			x										
MA.3.3.03 Trainings are evaluated by the public health agency and repeated, improved or discarded depending on the results.	X					X								
MA.3.3.04 Employees pass on their knowledge from the trainings to other employees in the public health agency in a structured exchange format (e.g. through regular appointments, workshops, written documentation).	X			X							X			X
MA.3.3.05 At least some employees receive training on IT-supported documentation of processes using process modelling language and tools.	X			X							X			
MA.3.4.01 There is a training concept for the individual employee that specifies how his/her skills can be continuously and individually developed and refreshed.	X			X					X		X		X	
MA.3.4.02 Employees can not only participate in trainings from a predefined training catalogue, but they are also financed to attend independently selected trainings (e.g. from external platforms).	X			X							X			
MA.3.4.03 Experiences on training are shared with other public health agencies. The training programme is adapted at least twice a year.		X												X
PD.1.0.01 There is a concept of how subject-specific processes are carried out uniformly according to a written specification (e.g. through a self-defined flowchart).	X					X								X
PD.1.1.01 A level of abstraction is defined for the process documentation, e.g. based on responsibilities, input, output, concrete activities.	X													X
PD.1.1.02 Uniform documentation guidelines (e.g. modelling language, possibly also without standardised syntax / semantics such as flowchart-like languages) and contents of the documentation (e.g. tasks, roles, resources, interfaces, integration of IT) are defined.	X					X								X
PD.1.1.03 Individual processes are documented and communicated with IT support in accordance with the documentation guideline.	X					X								X
PD.1.2.01 The majority of the standardised processes are documented and communicated with IT support in accordance with the documentation guideline.	X					X								X
PD.1.2.02 In the case of newly added specialised applications, processes are further developed, i.e. potential for improvement and change is identified, implemented and documented.	X								X					X
PD.1.2.03 Target processes are defined and documented for processes that are to be digitalised.	X					X								X
PD.1.3.01 There is an exchange with other public health agencies regarding process documentation.		X												X
PD.1.3.02 In times of crisis, processes are redefined and documented depending on the needs.	X								X					X
PD.1.3.03 Key processes are modelled using a standardised modelling language (e.g. BPMN).	x												x	x
PD.1.4.01 The majority of standardised processes are automatically documented through IT support.	X													X
PD.2.0.01 The public health agency defines evaluation and assessment criteria for processes that map the digitalization potential of (sub-)processes (e.g. processes with clear process rules, processes with high process frequency, low discretionary scope and data-intensive processes).	X					X								X
PD.2.1.01 Processes are analysed to assess their potential for digitalization and, based on this, a decision is made as to which processes can be digitalised.	X					X								

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
PD.2.2.01 For processes with high digitalization potential, suitable IT systems are identified and integrated into the processes (e.g. to accelerate processes and increase their transparency).	X													X
PD.2.2.02 With the integration of the IT systems into the processes, the process flows are adapted according to the functionality of the IT systems or the IT systems are used according to the process flows.	X								X					
PD.2.3.01 The documentation of standardised processes is largely supported automatically by IT.	X								X					X
PD.2.3.02 Interfaces between the most important specialised applications are supported by IT systems so that data does not have to be maintained twice in different places, for example.	X								X				X	
PD.2.4.01 Individual processes are fully automated by IT systems (e.g. Corona infection: notification until quarantine discharge).	X								X					
PD.3.0.01 There is a concept of how processes are defined across organisational units of the public health agency.	X					X								X
PD.3.1.01 Process documentation exists across at least first organisational units.	X													X
PD.3.1.02 Employees know the processes that are directly related to their own tasks.	X			X										X
PD.3.1.03 Employees are partially aware of the dependencies and interfaces of upstream and downstream processes/tasks.	X			X										X
PD.3.2.01 Process documentation exists across all organisational units.	X													X
PD.3.2.02 Employees know the dependencies and interfaces of upstream and downstream processes/tasks and know which input and output must be delivered at the interface.	X			X										X
PD.3.2.03 Processes are well coordinated at the first interfaces so that media discontinuities are minimised and the output can be reused as input.	X								X					
PD.3.3.01 Key processes are well coordinated at all relevant interfaces so that media discontinuities are minimised and the output can be reused as input.	X								X					
PD.3.4.01 Cross-process coordination takes place regularly for the continuous improvement of processes with common interfaces.	X								X					
PD.4.0.01 An evaluation of the processes is at least in the planning stage.	X					X								
PD.4.1.01 An evaluation of the processes with regard to quality criteria (e.g. effectiveness or efficiency) takes place at least in an unstructured way (e.g. the evaluation is purely oral and is not collected centrally).	X					X							X	
PD.4.2.01 A process evaluation with regard to quality criteria (e.g. effectiveness, efficiency) takes place in a structured way with software support (e.g. the evaluation is collected centrally in writing in a predefined mask in e.g. Excel). The evaluation takes place at least once a year.	X					X			X				X	
PD.4.2.02 Specific process improvement measures are derived from the evaluation (e.g. standardisation of processes, reduction of unnecessary interfaces).	X					X			X					
PD.4.2.03 The public health agency continuously evaluates whether the process documentation corresponds to the actual execution of the processes. The process documentation is adjusted accordingly.	X					X								
PD.4.3.01 An evaluation of the processes with regard to quality criteria (e.g. effectiveness, efficiency) takes place in a structured manner with software support using predefined key figures (e.g. process cycle time, customer satisfaction). The evaluation takes place at least once a year.	X					X			X				X	
PD.4.3.02 An evaluation of success/failure of the derived process improvement measures takes place.	X					X			X					
PD.4.3.03 The process documentation is checked twice a year and adapted if necessary (e.g. for completeness, clarity, comprehensibility and structure).	X					X			X					

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
PD.4.4.01 An evaluation of the first processes is carried out automatically with regard to selected key figures.	X								X					
IB.1.0.01 The necessary hardware is accessible to all employees as needed at each workstation (e.g. computer, printer, scanner, telephone)	X			X					X					
IB.1.0.02 An internet connection (LAN or WLAN) is guaranteed at every workstation.	X								X					
IB.1.0.03 Operating systems are up to date and system updates are installed.	X								X					
IB.1.0.04 Individual field staff have access to mobile business devices (e.g. laptops, mobile phones).	X			X					X					
IB.1.1.01 Adequate equipment for videoconferencing and teleconferencing is available. This means that all employees have access to a microphone and a webcam each if needed.	X								X					
IB.1.1.02 A stable and powerful internet connection (LAN or WLAN) is guaranteed at every workplace.	X			X					X					
IB.1.1.03 Mobile working is made possible for selected employees through the use of mobile devices such as laptops.	X			X					X					
IB.1.1.04 Digital faxes are available where required.	X								X					
IB.1.1.05 Ergonomic and efficient work is possible at the request of the employees (e.g. height-adjustable screens, second screen, ergonomic mouse).	X			X					X				X	
IB.1.1.06 Compatibility between the workplaces in the home office and in the field is partly given (e.g. through laptop or mobile phones with data volume, so that data can be transferred between different end devices).	X			X					X					
IB.1.2.01 Presentation facilities are available in the public health agency (e.g. beamer or multi-function board).	X								X					
IB.1.2.02 Mobile working (e.g. home office) is made possible for all employees on a permanent basis by providing suitable hardware while taking IT security and data protection into account (e.g. by providing laptops or tablets).	X								X			X		
IB.1.2.03 The location-independent collaboration of employees is supported by software solutions for digital document storage (e.g. file sharing).	X			X					X					
IB.1.2.04 The location-independent cooperation of employees is supported by software solutions for digital communication (e.g. chat function, forum, etc.).	X			X					X					
IB.1.2.05 There is no media discontinuity between the workplaces on site, in the home office and in the field (e.g. specialised applications can also be used on mobile devices outside the public health agency).	X			X					X					
IB.1.2.06 Individual field staff have access to mobile business devices (e.g. laptops, tablets, smartphones) as needed, which are compatible with the corresponding specialised applications.	X			X					X					
IB.1.3.01 Designated areas for collaborative work with remote collaboration options including conference systems are available (e.g. digital whiteboard and multi-function board).	X								X					
IB.1.3.02 The location-independent collaboration of employees is supported by software solutions that enable the simultaneous editing of documents.	X								X					
IB.1.3.03 All field staff have access to mobile business devices (e.g. laptops, tablets, smartphones) as required, which are compatible with the corresponding specialist applications.	X			X					X					
IB.1.4.01 Designated areas for collaborative work with remote collaboration options including conference systems are available in sufficient numbers (e.g. digital whiteboard and multi-function board).	X			X					X					
IB.1.4.02 The location-independent collaboration of employees is supported by integrative software solutions for digital communication and document storage, so that employees do not have to switch between different software solutions.	X								X					

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
IB.1.4.03 Collaboration in the public health agency is supported by an intuitive and continuously maintained knowledge and collaboration platform.	X								X					
IB.2.0.01 At least individual guidelines exist for the procurement of IT equipment.	X					X								X
IB.2.1.01 IT equipment is procured centrally and according to demand. It takes into account delivery backlogs/bottlenecks.	X	X											X	
IB.2.2.01 The administration has an IT equipment concept.	X					X								X
IB.2.2.02 The procurement and management of IT equipment is carried out centrally, demand-oriented and via a defined office (e.g. via the IT department).	X					X								
IB.2.2.03 The procurement of IT equipment is evaluated so that optimisation potential can be identified.	X	X				X			X					
IB.2.3.01 The need for new hardware for safe stationary work is regularly queried and retrofitted with foresight.	X								X				X	
IB.2.3.02 Employees are involved in the IT procurement process (e.g. employees can choose IT items from a selection).	X			X							X			
IB.2.4.01 The need for new hardware for secure mobile working is regularly queried and retrofitted with foresight.	X								X				X	
IB.2.4.02 Qualified personnel such as occupational physicians assist in the selection of ergonomic IT hardware.	X			X							X			
IB.3.0.01 The definition of a person responsible for IT is at least in planning or has already been done.	X					X								
IB.3.0.02 The person responsible for IT defines the IT sourcing strategy for the infrastructure components.	X					X								
IB.3.0.03 There are isolated basic infrastructure components in the public health agency (network access at the workplace, server and storage).	X								X					
IB.3.0.04 The public health agency uses a stand-alone data centre (without redundancy for a possible failure).	X		X						X			X		
IB.3.1.01 The person responsible for IT is known to the employees.	X			X		X								X
IB.3.1.02 There is structured coordination between the person responsible for IT, the organisational areas of the health department and external IT managers or IT service providers.	x	x	x			x								x
IB.3.1.03 The IT infrastructure supports all specialist applications.	X								X					
IB.3.1.04 The public health agency has a cold standby or even a hot standby.	X	X							X			X		
IB.3.1.05 A concept for evaluating the performance of the IT infrastructure is defined by a person responsible for IT together with the organisational units, but may not yet have been implemented.	X					X								
IB.3.2.01 A close exchange between the person responsible for IT and the organisational areas has been established so that the IT infrastructure is jointly developed in line with the requirements of the organisational areas.	X					X			X					X
IB.3.2.02 The IT infrastructure is planned and implemented holistically across all organisational areas (e.g. through a cross-location IT infrastructure including WLAN for decentralised health departments with several locations).	X					X							X	
IB.3.2.03 The IT infrastructure is modular, so that individual components can be flexibly replaced and expanded.	X								X				X	
IB.3.2.04 The public health agency has a hot standby as emergency protection.	X	X							X			X		
IB.3.2.05 The IT infrastructure is evaluated by the person responsible for IT according to key performance indicators and adjusted accordingly.	X					X			X					
IB.3.2.06 The IT infrastructure (e.g. servers, storage, computing capacity) can be quickly expanded in times of crisis to support employees in their tasks in the best possible way.	X								X				X	

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
IB.3.3.01 The IT infrastructure components are based on the current state of the art and are consolidated for the entire public health agency.	X								X					
IB.3.3.02 A virtualisation strategy for the IT infrastructure is defined. It is specified for the IT infrastructure components whether and when they will be virtualised.	X					X							X	
IB.3.3.03 The number and size of local and virtual components is continuously evaluated and adjusted with regard to the requirements of the organisational areas.	X					X			X					
IB.3.3.04 Virtual servers and storage enable location-independent work capability (software is available, central data storage, data exchange with other organisations).	X								X					
IB.3.3.05 Storage for large amounts of data is kept ready.	X								X					
IB.3.3.06 A cloud concept with IT security and data protection requirements has been prepared as required and is being used.	x					x	x					x		
IB.3.4.01 The IT infrastructure is proactively and continuously further developed by the IT security manager with reference to the latest technology.	X								X			X		
IB.3.4.02 The IT infrastructure enables the best possible cooperation with other organisations (e.g. it is planned and implemented at country level and, where appropriate, across countries).	x	x												
IB.4.0.01 The IT service processes according to the ITIL standard (e.g. support, incident management, change management, procurement processes) are known to the person responsible for IT.	X					X								
IB.4.0.02 There is a backup for system failures and ad hoc problems (e.g. employees can fall back on manual processes in an emergency and are prepared for corresponding crisis situations).	X								X					
IB.4.1.01 The processes for service support and delivery are defined and communicated.	X					X								X
IB.4.1.02 Structured channels exist for employees to request IT services (e.g. hotline, ticket tool).	X			X							X			
IB.4.2.01 The IT service management processes for service delivery and support are established. Responsibilities are defined.	X					X								
IB.4.2.02 Meaningful service level agreements are in place and adhered to.	X					X								
IB.4.3.01 An IT service management system has been established for sustainable root cause analysis and the elimination of faults.	x					x			x			x	x	
IB.4.3.02 The quality of IT service management is measured using criteria (e.g. availability, duration of disruption) and adjusted accordingly.	X					X			X					
IB.4.4.01 IT service management processes are certified according to the applicable ISO standard and the basic protection of the Federal Office for Information Security.	X					X						X		
IB.4.4.02 The IT service management is continuously developed and adapted to the needs of the public health agency.	X								X					
IS.1.0.01 At least initial ideas regarding an IT security concept exist or an IT security concept has already been drafted.	X					X						X		
IS.1.0.02 The role of an IT (security) officer responsible for the public health agency is defined.	X					X						X		
IS.1.0.03 All relevant employees are integrated into the safety process.	X			X							X	X		
IS.1.0.04 An inventory list of all physical devices and the systems and applications used is available.	X					X								
IS.1.1.01 Security measures are systematically documented in an IT security concept.	X	X				X						X		
IS.1.1.02 The IT security process and the role of the IT (security) officer are made known to all employees.	X					X					X			X
IS.1.1.03 An inventory list of all physical devices as well as the systems and applications used is available and is maintained according to a defined process on an ad hoc and periodic basis.	X					X								

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
IS.1.2.01 A central IT security concept including risk management is in place.	X					X						X		
IS.1.2.02 Responsibilities and an appropriate organisational structure for IT security are defined.	X					X						X		
IS.1.2.03 The IT security concept including IT security processes are documented and regularly reviewed for effectiveness and appropriateness.	X					X						X		
IS.1.2.04 Defined reporting mechanisms exist, e.g. in the form of management reports, which contain the essential relevant information about the IT security process, especially about problems, successes and opportunities for improvement.	X					X						X		X
IS.1.3.01 Measures from the IT security concept are fully implemented in practice and their implementation is regularly monitored.	X					X			X			X		
IS.1.3.02 Whenever possible, additional internal or external employees are deployed to deal with peaks in IT security workload.	X								X			X		
IS.1.4.01 The IT security concept is regularly reviewed and adapted to the requirements of the IT baseline protection of the Federal Office for Information Security.	X					X			X			X		
IS.1.4.02 The IT (security) officers exchange information on IT security topics in the public health agency on a regular and demand-oriented basis and try to reduce IT security risks together.		X							X			X		X
IS.2.0.01 E-mail filters, secure browsers and security updates for hardware and software are used regularly.	X											X		
IS.2.0.02 The head of the office is sufficiently sensitised by the IT (security) officer and initiates appropriate measures (e.g. he/she supports the implementation of training programmes on IT security).	X					X					X	X		
IS.2.0.03 The CERT-Bund of the Federal Office for Information Security is known to all persons responsible for IT security in the public health agency and existing IT systems are checked against the CERT-Bund reports of risk level 4-5 at least once every six months.	x					x			x			x		x
IS.2.0.04 Safety guidelines exist for the detection of safety-relevant events.	X					X						X		
IS.2.0.05 Reporting paths for safety-relevant events are defined.	X					X			X			X		
IS.2.0.06 System functions for detecting security-relevant incidents on deployed IT systems are activated and used (e.g. virus scanner).	X					X			X			X		
IS.2.0.07 Guidelines for dealing with some security incidents as well as contact persons have been defined and made known to the employees.	X					X						X		X
IS.2.0.08 Warnings and incidents are responded to and reported to the appropriate authorities.	X					X			X			X		
IS.2.1.01 At least some employees have the ability to support the installation of security updates and software updates.	X								X			X		
IS.2.1.02 All employees and external users are instructed once in the safe use of IT components and sensitised to the extent that this is relevant to their work context.	X			X							X	X		
IS.2.1.03 The existing IT systems are fully checked at least twice a year against the CERT-Bund notifications of the Federal Office for Information Security.	X					X			X			X		
IS.2.1.04 Affected employees are informed ad hoc with alerts about IT security incidents so that data can be "safely" deleted with the system's tools.	X											X		X
IS.2.1.05 The security guidelines for the detection of security-relevant incidents are regularly reviewed and are known to all employees responsible for IT security.	x			x		x			x			x		x
IS.2.1.06 Reporting channels for safety-relevant events are regularly checked, tested and updated.	X					X			X			X		
IS.2.1.07 Additional malware scanners on central IT systems are installed and used as needed.	X								X			X		
IS.2.1.08 The IT security guidelines and contact persons for dealing with security incidents are known to all employees. Contact information is always up-to-date and easily accessible.	x			x		x					x	x		x

[illegible]

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
IS.2.4.03 There is a regular exchange between IT (security) officers and other contact persons relevant to IT security (e.g. data protection, health and safety at work, fire protection) on the efficiency of education and training.	X					X						X		X
IS.2.4.04 The existing IT systems are fully checked daily against the CERT-Bund reports from the Federal Office for Information Security.	X					X						X		
IS.2.4.05 Vulnerability management has been established and is carried out continuously as part of the security processes.	X								X			X		
IS.2.4.06 An exchange with other authorities or the competent state authorities or the Federal Office for Information Security takes place regularly.		X										X		X
IS.2.4.07 A central detection and real-time verification of IT event messages takes place.	X								X			X		
IS.2.4.08 The reporting of IT security-relevant events is automated by the detection systems used and a response is made with suitable protective measures.	X								X			X		
IS.2.4.09 IT systems and solutions, including cloud solutions, comply with the highest security level and are continuously evaluated and adapted with regard to new requirements.	X					X			X			X		
IS.2.4.10 A dedicated security incident reporting point is also available outside normal working hours.	X					X			X			X		
IS.2.4.11 There is a management system in place to deal with IT security incidents, which is regularly reviewed to ensure that it is effective and up to date.	X					X			X			X		
IS.2.4.12 Existing processes are continuously refined based on findings from security incidents and industry developments (also in other public health agencies).	X								X			X		
IS.3.0.01 The allocation of access authorisations, access permissions and access rights is regulated for specific IT systems and employees.	X			X		X						X		
IS.3.0.02 The use of passwords is regulated in a binding manner.	X			X								X		
IS.3.1.01 An identity and authorisation concept is available in written form.	X					X						X		X
IS.3.1.02 In addition to passwords, the use of additional authentication features or procedures is evaluated for resources requiring protection.	X											X		
IS.3.2.01 The identity and authorisation concept is fully implemented in practice.	X											X		
IS.3.2.02 Precisely defined access rules apply for individual users or groups of users to the data of an IT system.	X					X						X		
IS.3.2.03 Multi-factor authentication, e.g. with cryptographic certificates, digital signatures, smart cards or tokens are used.	X											X		
IS.3.3.01 Actions where the dual control principle is to be applied are evaluated (e.g. administrative activities in particularly critical IT systems).	X					X						X		
IS.3.3.02 The effectiveness of user separation on the IT system or application is continuously monitored and adjusted accordingly.	X					X			X					
IS.3.3.03 The authentication mechanisms are selected according to the need for protection and are continuously evaluated.	X					X			X			X		
IS.3.3.04 Emergency preparedness is established so that the public health agency can continue to operate in the event of a failed identity and authorisation management system.	X								X			X		
IS.3.4.01 Identity and access management is regularly adapted to the technical requirements of the IT systems.	X								X			X		
BZ.1.0.01 Communication with citizens also takes place digitally (e.g. email or contact forms).	X				X				X					
BZ.1.0.02 An online availability and web presence of information on policies, services and contact persons is in place.	X				X				X					X
BZ.1.1.01 At least digital one-way communication from the public health agency to citizens exists for appropriate matters (e.g. through the availability of downloadable forms).	X				X				X					

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
BZ.1.1.02 The most frequently asked questions of citizens from the organisational units are available online (e.g. on quarantine regulations or entry requirements).	X				X				X					X
BZ.1.2.01 Digital two-way communication is made possible (e.g. through the possibility for citizens to upload documents, emails, online chat room and online appointments).	X				X				X					
BZ.1.2.02 Citizens are enabled to communicate without media discontinuity. The online presence is geared towards citizens and allows regular communication (e.g. contact persons are easy to find and can also be reached via several alternative channels).	X				X				X					X
BZ.1.2.03 Simple or basic counselling services are offered digitally by the public health agency (e.g. as video material or video conferencing).	X				X				X					
BZ.1.3.01 A mix of online and offline services is offered (e.g. counselling services via video conference and in person).	X				X				X		X			
BZ.1.3.02 Counselling sessions and health promotion and prevention services are also offered completely digitally, if appropriate, in addition to face-to-face services (e.g. educational sessions on prevention, pregnancy conflict counselling, tumour counselling, sexual counselling, risk communication or crisis communication).	X				X				X					
BZ.1.4.01 The individual preferences of citizens are taken into account in interaction and communication (e.g. adaptation of the approach according to previous analogue/digital experience and feedback from citizens, especially according to individual preferences regarding digital channels).	X				X						X		X	
BZ.2.0.01 The information available online is regularly updated by the public health agency.	X				X				X					X
BZ.2.1.01 An alternative channel for "non-digital citizens" allows sufficient communication with the public health agency.	x				x						x			
BZ.2.1.02 Legal requirements regarding barrier-free access have been implemented.	x				x	x		x			x			
BZ.2.2.01 Proactive push notifications and email notifications are sent to citizens (e.g. appointment reminders or deadline reminders).	X				X									X
BZ.2.3.01 The public health agency provides citizens with common online applications that allow citizens to complete transactions, authentications and verifications online, using digital signatures where appropriate.	X				X						X	X		
BZ.2.4.01 Business processes and IT systems are driven by citizens' needs.	X				X						X		X	
ZA.1.0.01 At least one initial IT-supported communication across organisational units takes place (e.g. by email).	X								X					
ZA.1.0.02 The public health agency has its own public health agency specific email address (e.g. GA@LandkreisX.de).	X								X					
ZA.1.1.01 There is at least planning for initial IT-supported cooperation across the first organisational units of a public health agency where cooperation makes sense (e.g. psychosocial service and child and youth health service).			X						X					
ZA.1.1.02 Employees use shared digital calendars for scheduling.	X								X					X
ZA.1.1.03 A digital shift plan exists.	X								X					X
ZA.1.2.01 There is IT-supported cooperation across at least the first organisational units, wherever cooperation makes sense (e.g. psychosocial service and child and youth health service). This is done via defined interfaces for data exchange so that inconsistencies for these organisational units are avoided.			X						X					
ZA.1.2.02 The recommendations on technical and semantic standards, profiles and guidelines of the interoperability specifications (including those of Gematik) are complied with.			X			X								
ZA.1.2.03 The public health agency has an internal network for the internal exchange of data.	X		X						X					

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
ZA.1.3.01 There is IT-supported cooperation across all organisational units for which cooperation makes sense (e.g. psychosocial service and child and youth health service). This is done via defined interfaces for data exchange so that inconsistencies for these organisational units are avoided.	X		X						X					
ZA.1.4.01 Cooperation across all levels is realised through the use of an intuitive and continuously maintained knowledge and cooperation platform. This is a central web platform for cooperation and exchange of experiences.	X		X						X					
ZA.1.4.02 The cooperation is based on digital standardised processes without media discontinuities as standard. These processes are constantly updated and further developed on the basis of new technologies/standards.	X		X						X					
ZA.1.4.03 The communication infrastructure works on the basis of current and jointly defined or centrally standardised data exchange standards (e.g. by means of HL7).	x		x			x			x				x	
ZA.2.0.01 The public health agency exchanges information with other public health agencies and regional offices (e.g. via email).		X							X					
ZA.2.1.01 The public health agency regularly exchanges information with neighbouring public health agencies as well as with relevant state offices via IT-supported channels (e.g. via video conferences).		X							X					
ZA.2.1.02 There is digital communication with public health agencies of other federal states if required (e.g. information about a quarantine case of a holidaymaker).		X							X					
ZA.2.1.03 Employees of the public health agency take part in interdisciplinary working groups within the federal state. They use digital media (e.g. video conferences).		X								X				
ZA.2.2.01 The public health agency regularly exchanges information with other public health agencies and with regional offices. This exchange takes place without media discontinuities via digital channels (e.g. via video conferences).		X							X					
ZA.2.2.02 The recommendations on technical and semantic standards, profiles and guidelines of the interoperability specifications (including those of Gematik) are complied with.			X			X								
ZA.2.3.01 The public health agency regularly exchanges information with other public health agencies and with regional offices. This exchange takes place without media discontinuity via permanently available digital channels (e.g. via shared specialised applications/software).		X							X					
ZA.2.3.02 The public health agency exchanges information with other public health agencies on the procedure and knowledge of digitalization (e.g. joint user board for the exchange of requirements for specialised applications).		X												X
ZA.2.4.01 Cooperation across all levels is realised through the use of an intuitive and continuously maintained knowledge and cooperation platform. This is a central web platform for cooperation and exchange of experiences.	X								X		X			
ZA.2.4.02 The cooperation is based on digital standardised processes without media discontinuities as standard. These processes are constantly updated and further developed on the basis of new technologies/standards.	X								X				X	
ZA.2.4.03 The communication infrastructure works on the basis of current and jointly defined or centrally standardised data exchange standards (e.g. by means of HL7).	X					X			X				X	
ZA.3.0.01 Digital cooperation with external stakeholders is at least in the planning stage or already being implemented (e.g. via email).		X							X					
ZA.3.1.01 Channels for IT-supported communication/cooperation with the first external stakeholders (especially laboratories, RKI) can be realised e.g. via video conferences.	x	x							x					
ZA.3.2.01 Channels for IT-supported communication/cooperation with other external stakeholders (especially hospitals, rehabilitation, GPs, old people's homes) can be created ad hoc via shared specialist applications or are possible via video conferences.		X							X					

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
ZA.3.2.02 The recommendations on technical and semantic standards, profiles and guidelines of the interoperability specifications (including those of Gematik) are complied with.			X			X								
ZA.3.3.01 Channels for IT-supported communication/cooperation with all relevant external stakeholders (courts, police, research partners) are permanently available so that media discontinuity, inconsistent work and duplicate entries can be avoided (e.g. through jointly defined exchange formats).		X							X					
ZA.3.4.01 Cooperation across all levels is realised through the use of an intuitive and continuously maintained knowledge and cooperation platform. This is a central web platform for cooperation and exchange of experiences.	X								X		X			
ZA.3.4.02 The cooperation is based on digital standardised processes without media discontinuities as standard. These processes are constantly updated and further developed on the basis of new technologies/standards.	X								X				X	
ZA.3.4.03 The communication infrastructure works on the basis of current and jointly defined or centrally standardised data exchange standards (e.g. by means of HL7).	X								X				X	
SD.1.0.01 Specialised applications/software and business processes are considered together.	X								X					
SD.1.1.01 Business processes are supported by specialised applications.	X								X					
SD.1.1.02 Specialised applications allow several employees to work on one database at the same time, so that workarounds are unnecessary.	X								X					
SD.1.1.03 Specialised applications are already (also partially) used and accepted along the business processes.	X								X					
SD.1.1.04 Centrally provided specialised applications are used nationwide.	X								X					
SD.1.2.01 Specialist applications cover defined best practices and are integrated with each other along the business processes.	X								X					
SD.1.2.02 New, high-potential software can be tried out and tested (e.g. within the framework of pilot uses).	X								X					
SD.1.2.03 Business applications are resilient in crisis situations. They are performant with high accesses, parallel users and allow version storage.	X								X			X		
SD.1.2.04 Initial e-file-compliant processing by software/specialised applications takes place.	X								X					
SD.1.3.01 The specialised applications/software allow a connection of web-based applications (e.g. symptom diary) and are integrated on a central platform, if applicable.	X								X					
SD.1.3.02 All business processes are supported by specialised applications/software.	X								X					
SD.1.3.03 Business processes and specialised applications are viewed in an integrated manner and optimised together on an ongoing basis. New functionalities/best practices are continuously integrated.	X								X					
SD.1.4.01 Modular possibilities for creating new digital solutions are available (e.g. for the use of chatbots).	X								X				X	
SD.1.4.02 Legally compliant e-file system is in place.	X					X								
SD.2.0.01 First implementation of interfaces takes place between specialised applications.	X								X					
SD.2.1.01 Specialised applications already have basic interfaces to each other, but these are not yet fully utilised.	X								X					
SD.2.1.02 Data is kept in a common database.	X								X					
SD.2.1.03 Duplicates are cleaned up, if necessary manually or semiautomatically.	X								X				X	
SD.2.2.01 Data transfer is at least (partially) automated by means of standardised interfaces.	X								X					
SD.2.2.02 Possibilities for cross-institutional data exchange are available (e.g. for infection control).	X	X							X					

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
SD.2.3.01 Existing interfaces are bidirectional if necessary.	X								X					
SD.2.4.01 Interfaces for the exchange of data between all important stakeholders are continuously adapted to current standards.	X	X							X					
SD.2.4.02 Gateways/platforms exist as a solution for still missing interfaces (if interfaces are still missing).	X								X					
SD.3.0.01 Basic data analysis solutions are available.	X								X					
SD.3.1.01 There is a collection and integration of key figures.	X								X					
SD.3.2.01 Existing systems are taken into account through interfaces in the reporting channels.	X	X							X					X
SD.3.2.02 A manual or automated creation of internal reports based on internal data takes place.	X					X			X					
SD.3.2.03 Individualised reports and data queries are generated.	X					X			X					
SD.3.3.01 Analytical population data, including big data, will be incorporated into the operation.	X								X					
SD.3.3.02 There is a (partially) automated production of daily metrics.	X								X					
SD.3.3.03 Reporting/data is used for forecasting and decision support.	X								X					
SD.3.3.04 Messages can also be sent automatically.	X								X					
SD.3.3.05 Reporting/data is provided for public health research.	X				X				X					X
SD.3.4.01 A complete data quality management including data warehouse with a business intelligence solution has been implemented.	X								X					
SD.3.4.02 There is an alarm management system based on real-time data.	X				X				X			X		
SD.3.4.03 The data analysis is permanently operated and optimised.	X								X					
SD.4.0.01 The technical documentation of specialised applications is being planned or is already being implemented.	X					X			X					X
SD.4.1.01 The requirements for data are defined by different actors.	X	X				X								
SD.4.1.02 There are informal or formal processes to report functions and new ideas for the further development of specialised applications.	X								X					X
SD.4.1.03 The technical documentation of specialised applications has been implemented.	X					X								X
SD.4.2.01 Specialised applications are systematically selected (1. weak points identified from process map; 2. specialised concept with requirements derived, 3. selection of suitable specialised applications).	X								X					
SD.4.2.02 There is a life cycle concept for specialised applications/software.	X												X	
SD.4.2.03 Updates and upgrades are planned and implemented in a structured manner.	X								X					
SD.4.2.04 Data quality indicators are defined and regularly evaluated.	X					X			X					
SD.4.3.01 There is a defined prioritisation process for the implementation of functions.	X					X			X					
SD.4.3.02 Requirements for user interfaces and user experience are in place and enable a high level of user-friendliness of the applications.	X				X				X				X	
SD.4.3.03 The dialogue with software manufacturers is continuously being improved.	X	X							X					X
SD.4.4.01 Specialised applications are continuously evaluated and improved in terms of performance, accessibility and data protection.	X						X		X		X			
SD.4.4.02 The functions of software/specialised applications are continuously expanded based on new technical possibilities (e.g. image recognition, character recognition, process automation).	X								X					
SD.4.4.03 Fast system set-up for new staff is guaranteed.	X				X				X					
SD.5.0.01 The data protection concept measures data protection and IT security processes and describes the level of data protection.	X						X					X		
SD.5.0.02 Specialised applications take into account legal requirements (e.g. retention periods, security requirements).	X					X								

Criteria (translated from German, inclusive criteria ID)	Corporate Level	Interorganizational Level	Intraorganizational Level	Personal Level	Societal Level	Accountability Principle	Data Privacy Principle	Fairness Principle	Functionality Principle	Norms & Values Principle	Participation Principle	Security Principle	Sustainability Principle	Transparency Principle
SD.5.1.01 The data protection concept includes a catalogue of measures with technical and organisational measures.	x					x	x							
SD.5.1.02 The data protection officer shall be involved in actions involving sensitive data.	X					X	X							
SD.5.2.01 Processes relating to data protection are continuously updated based on the current legal regulations.	X						X							
SD.5.2.02 There are regular measures to make employees aware of the aspects of data protection.	X			X			X							
SD.5.3.01 Concepts are in place to protect data (e.g. pseudonymisation and anonymisation).	X						X							
SD.5.3.02 There is an exchange with other public health agencies as well as state offices and federal authorities about the regulations on data protection and their implementation.		X					X							X